FUTURE-PROOFING CLOUD CONNECTIVITY IN AN EXACTING REGULATORY LANDSCAPE

Navigating Technology Risk Management and Compliance in accordance with the Monetary Authority of Singapore's Guidelines

epsilon
a kt company

SUMMARY

1.

FINANCIAL INSTITUTIONS IN A CLOUD WORLD

The Need to Stay Ahead

The tactics of cyber threat actors are growing more sophisticated by the hour. A single weak link in the interconnected financial ecosystem can and will be exploited to carry out fraudulent financial transactions, exfiltrate sensitive financial data, or disrupt support of financial services.

Keeping several steps ahead of threat actors can boost your financial institution's business continuity preparedness and future-proofing — well beyond tomorrow. And the incremental investment involved can yield higher returns on investment when you consider the severe costs of tangible and intangible financial loss due to cyber theft, regulatory penalties and reputational damage.

As a financial institution in Singapore, have you done everything necessary to stay resilient and adaptable amid the tightening data protection and financial compliance laws?

Can you be sure your instituted digital transformation measures meet all the requirements of the Technology Risk Management (TRM) guidelines?

This eBook is designed to give you an overview of the wider implications of the Monetary Authority of Singapore's (MAS) guidelines. It details the options available for keeping many steps ahead of further imminent regulatory changes amid the current global pandemic situation.

2.

MINIMISING CLOUD ANXIETY FOR FINANCIAL INSTITUTIONS

The benefits of moving infrastructure over to cloud-based platforms are clear. The COVID-19 pandemic has made the benefits even clearer and more concrete.

With increased adoption and widespread usage, cloud costs are continuing to be more economical and flexible. Savings from moving away from legacy on-premises architecture are also being factored into the benefits of migration to cloud infrastructure. For the financial sector, digitalisation is even more crucial with the entrance of digital banking, peer-to-peer crowdfunded lending and other agile forms of digital competition.

According to **IDC's Cloud Outlook 2021** and similar reports, there are six trends in the APAC region driving rapid and high levels of digital transformation into cloud computing:

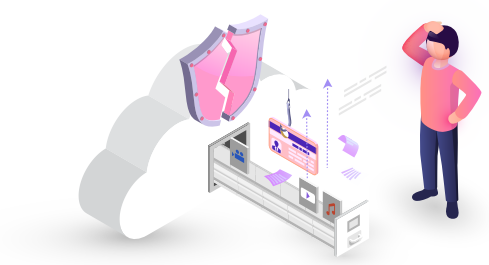
APAC FINANCIAL SECTOR CLOUD STATISTICS

- By 2023, **85%** of tier-1 and tier-2 APEJ banks will have coalesced on-premises/dedicated private clouds and multiple public clouds, along with legacy platforms, to assuage their many infrastructure requirements.
- More than **40%** of APEJ FIs already run workloads and IT jobs (in part or in full) in a multi-tenant public cloud.
- Close to **30%** of banks currently running workloads in the private cloud have plans to move a percentage of these to the public cloud: some having firm plans to move within 24 months.
- IDC predicts that the public cloud spend by APEJ FSIs will grow close to four times to **US$13.9bn in 2023** from a spend of **US$3.6bn in 2018**, growing at a compound annual growth rate of over **30%**.
- This spending reached **US$5bn in 2019**. Despite the pandemic, this growth is projected to continue with a slight uptick.

APAC TRENDS

- The urgency to transition from CAPEX to OPEX amid competitive pressures.
- The wide range of cloud adoption strategies on tap: hybrid cloud, multi-cloud, joint provider-cloud.
- Ultra-lean fourth-generation core banking necessitates cloud as an essential tenet.
- Application development agility advantages including but not limited to enhanced micro-services, containers, and orchestration tools.
- The availability of now-mature cloud marketplaces offering innovations that can boost financial institutions' own innovation and business differentiation strategies.
- The fact that cloud computing has become the principal route towards data science benefits for dynamic enterprise intelligence and data-driven innovation.

Regardless of the level of digital transformation your organisation has embraced so far, compliance and national cybersecurity mandates mean that more safeguards and best practices need to be integrated into the entire banking, financial and insurance system in Singapore.



Causes of cloud anxiety and how to contain them:

Notwithstanding the compelling advantages and non-negotiable regulatory pressure to digitalise via the cloud, the challenges and perceived pain points still exist.

TOP CHALLENGES CITED AND FACED BY FINANCIAL ORGANISATIONS INTIMIDATED BY THE CLOUD INCLUDE:

- ✓ The complexity of managing multiple cloud platforms and cloud partners/vendors.
- ✓ Questions surrounding data sovereignty, network visibility and cloud networking.
- ✓ Security concerns due to storage of sensitive data by third parties and their own cybersecurity hygiene.
- ✓ Cost concerns due to a combination of unpredictable and maybe even unending rounds of mandates for upgrading cloud-related infrastructure and processes.
- ✓ Many of the anxieties are not unfounded, and with traditional approaches to cloud migration, lapses can and do surface.

Taking all the above factors into consideration, what is the intelligent approach to maximise the benefits while minimising the risks and containing the perceived pain points?

3.

THE CLOUD GUIDELINES

Financial institutions are scaling up the utilisation of cloud services to enable innovation and new business models, as well as to meet the exponential need for and use of data.

MAS' Technology Risk Management (TRM) and ABS Cloud Computing guidelines reflect clear industry good practices and recommendations in line with this shift. It will continue to facilitate responsible and secure adoption of cloud services by establishing clear expectations for both banks and cloud service providers.

To align with the rapidly evolving global cybersecurity landscape, the Technology Risk Management guidelines is constantly updated to address:

1. Expanded roles and responsibilities for the Board of Directors and Senior Management to be equipped with the latest skills and information to understand and manage technology risks, including cyber risk.
2. Expansion of existing cybersecurity guidelines to include Cyber Threat Monitoring and Information Sharing, Cyber Incident Response and Management, and Cyber Security Assessments.
3. Expanded cybersecurity ring-fence perimeters to include the assessments of third-party vendors and entities that access the FI's IT system.
4. New area of concern: Assessment of third parties' suitability in connecting to Application Programming Interface (APIs); and the governance of third-party API access.
5. Expanded processes for simulation of cyber-attacks tactics, techniques and procedures.

Also, the **ABS Cloud Computing Implementation Guide 2.0** is a substantial update to the 2016 version to guide the categorisation of material and non-material cloud outsourcing arrangements, guidance for due diligence assessment on cloud service providers (CSPs), and approaches for governing, designing, securing and running the cloud. Recommendations include:

1. A detailed framework that proposes ways for governing, designing, securing and running the cloud infrastructure.

2. Significant features for categorising material and non-material cloud outsourcing arrangements: for example, Financial Risk management systems (material) versus staff data which does not include personal bank or credit card data (non-material).

3. Deeper guidance for ensuring that CSPs are following the ABS Guidelines on Control Objectives and Procedures for Outsourced Service Producers (OSPs) and the OSP Audit Report (OSPAR).

4. In-depth regulations for securing material versus standard (non-material) workloads. These regulations are implemented for critical workloads as well.

5. Detailed suggestions and explanations in due-diligence activities for Cloud outsourcing arrangements:
   - Governance
   - Assessment of the cloud service provider
   - Contractual consideration

6. A breakdown of key controls guiding the usage of cloud computing:
   - Governing the cloud infrastructure
   - Designing and securing the cloud infrastructure
   - Run the cloud ecosystem

In Essence

The greatest urgency in the updated guidelines revolves around three key factors:

1. PEOPLE

Senior Management, third party vendors and internal users.

2. CYBERSECURITY

Preemptive and end-to-end defence protocols, open threat intelligence sharing, tighter control of collaborations via APIs, speed of detection and mitigation, threat intelligence monitoring, preparedness and muscle-memory boosting through simulation exercises.

3. CLOUD

Governance, design, security and operations; CSPs ABS guideline compliance, regulations for securing material versus standard (non-material) workloads; due-diligence activities for cloud outsourcing arrangements (Governance, Assessment of CSP and contractual issues).

4.

THE EPSILON PROPOSITION

Epsilon has evolved from serving single cloud to multi-cloud requirements to help FIs solve increasingly complex challenges today. Our offering not only ensures clients meet all compliance regulations but goes beyond the benchmark through other value-adds.

By delivering best-in-class connectivity solutions through our service, innovation and technical partnership, Epsilon is well-positioned to help Singapore FIs meet local regulations and compliance. At the same time, ensuring maximum performance and reliability of their services and applications. We help organisations differentiate themselves:

CUT RELIANCE ON CARRIERS. Infiny ensures you will never be burdened by slow service provisioning or inflexible contracts and minimal options to move or alter your network connections.

INTEGRATED OFFERING. Solve challenges from the middle mile to the last mile and bridge any users or end points to your business-critical applications and data on public and private clouds.

FAST, SECURE, RELIABLE CONNECTIVITY. Unshackle your organisation with instant access to global interconnection and cloud networking backed by a team of experts and proactive compliance framework.

NETWORK CONTROL. Our Cloud Networking, SD-WAN and Security services make it easy to monitor, control and orchestrate network services with full visibility for resource planning.

CONNECTIVITY ON THE FLY. Network automation and orchestration enable you to consume and deploy network services for your cloud and business applications as easily as end users consume SaaS solutions.

COST EFFICIENT. Pay for only the bandwidth consumed with the ability to scale up during business peak and down during lull periods.

GLOBAL PRIVATE NETWORK. Secure global backbone providing high-capacity connectivity to over 250+ points of presence in 41 cities via state-of-the-art Juniper network, ensuring application security and compliance with data protection.

All stages of cloud transformation

Epsilon's Cloud Connectivity portfolio provides an array of services for both single and multi-cloud requirements. They complement every stage of an FI's cloud transformation journey and maximise their investments in the cloud.

CLOUD CONNECT – A connection between a private network (data centre/branch) and public cloud:

FIs can use Cloud Connect to directly connect to the CSP of their choice via Epsilon's global private network. CSPs include Amazon Web Services, Alibaba Cloud, Microsoft Azure, Google Cloud, Oracle Cloud and IBM Cloud. It is a simple layer 2 connectivity to the cloud and can be easily deployed using the Infiny by Epsilon Network-as-a-Service (NaaS) platform.

CLOUD NETWORKING – Fully managed Cloud Networking Platform for any-to-any connection among single, multiple clouds (up to VPC/VNET) & DC/branch:

FIs progressing towards cloud maturity will need a cloud connectivity solution that enables them to overcome native cloud limitations. Epsilon's purpose-built cloud networking solution delivers a multi-cloud network platform with the simplicity, automation, operational visibility and control that enterprises need. The solution provides a private network as underlay and a centralised controller as an overlay to create an enterprise-class network inside and between public clouds, up to the VPC/VNET level.

Our Cloud Networking also allows customers to consume security services, such as FQDN filtering and service insertion of next-gen firewalls to meet their security and compliance requirements.

5.

HOW A GLOBAL BANK STAYS READY FOR ANY REGULATORY REVISIONS

A leading international bank in Singapore operating across the Asia-Pacific, Western Europe and North America decided that it needed to simplify how it connects its regional office footprint directly to the leading CSPs.

Well before this plan, the bank had already been digitally innovating to differentiate its services to both corporate and retail customers, offering cloud-based banking solutions for corporate customers to manage multiple core processes such as sales, invoicing, payroll, and accounting remotely. It was the first in Singapore to digitalise the application process for its consumer banking products.

With such excellence in its grasp, the bank's competitive, forward-looking vision also spelt out the need to achieve even more:

- ✓ With IT workloads deployed across multiple clouds, it needed direct, secure connection between its branch locations to Amazon Web Services (AWS), Google Cloud Platform (GCP) and IBM Cloud. The bank wanted to carefully recalibrate its existing port to the three different CSPs based on bandwidth. The solution had to complement the existing infrastructure and be rolled out within a short timeframe.

- ✓ Another critical need was to rapidly deliver new applications and services with a comprehensive end-to-end solution.

- ✓ With significant investment into its digital strategy, the bank aims to be at the forefront of leveraging digital technology to shape the future of banking. It expects to lead in the use of customer insights to deliver new business models and digital innovations to build deeper relationships with all customers and partners.

- ✓ As their digital customers and branch location footprint was expanding globally, the bank cannot afford to let their network infrastructure slow down the performance of their digital applications. Instead of having to manage multiple service providers, which increased costs and reduced agility, the bank needed a one-stop service provider to manage everything from last-mile connectivity to the CSPs.

- ✓ Lastly and importantly, the bank's top people knew that leaping ahead digitally to remain competitive came with risks: surging cyber threats; data protection and privacy regulations; and business continuity preparedness challenges. The cloud connectivity solution they selected would have to be in accordance with the MAS guidelines; specialised in FSI compliance; possess best-in-class security track records; and demonstrate a continually-upgraded infrastructure that prioritises future-proofing for customers.

What solutions did the bank engage?

Despite its multiple demanding specifications, the bank's requirements can be easily met with Epsilon's Cloud Networking. The solution quickly gave the bank a flexible networking foundation to support their cloud-based business applications and expectations.

THE BENEFITS

Epsilon's Cloud Networking offer greater operational visibility and control with automation to manage end-to-end cloud service across single and multiple clouds. The solution gives the bank a single pane of glass to view its entire cloud network estate and simplify their network operations.

Epsilon provided a comprehensive solution with full site-to-port connectivity as well as hands-on cabling within the data centre. It provides a complete view of the network architecture as well as support from a compliance perspective to get the bank started quickly and efficiently without needing its own team to manage the setup.

- Epsilon's private global network offers best-in-class security and a solid track record for connecting to the cloud.
- Single-point of contact which means no hassles of managing multiple vendors and service providers.
- Cloud connectivity offering in compliance with the TRM and ABS frameworks for FIs in Singapore.
- Improved productivity of engineering & operation teams (14x build/deployment and 7x tactical ops).
- Simplify networking and security in the cloud.
- Hassle-free configuration and networking onboarding.
- Overcome skillset gap in public cloud.

The prescient choice of partnering with Epsilon has allowed the bank to freely expand its connectivity to the cloud, without needing to worry about the challenges associated with regulatory guidelines. The flexible nature of a multi-service port also means it can continually scale-up, adjust and adapt its network to serve the changing needs of its business. It is an ideal model for a bank that is dedicated to fast-paced digital innovation and one that prides itself on offering new and enhanced customer experiences.

WORKING WITH EPSILON: A MUTUAL ACTION PLAN

A leading international bank in Singapore operating across the Asia-Pacific, Western Europe and North America decided that it needed to simplify how it connects its regional office footprint directly to the leading CSPs.

Well before this plan, the bank had already been digitally innovating to differentiate its services to both corporate and retail customers, offering cloud-based banking solutions for corporate customers to manage multiple core processes such as sales, invoicing, payroll, and accounting remotely. It was the first in Singapore to digitalise the application process for its consumer banking products.

Epsilon's compelling proposition for FIs begins with a simple 4-step iterative process.

1

INTRODUCTION / PLANNING

With Epsilon's total commitment to Singapore financial institutions, our liaison teams make this stage easy and painless. As each FI's digital transformation journey has to be our success as well, this important stage is navigated with mutual and full disclosure of all expected deliverables.

2

VALIDATION

After success criteria has been defined and signed off, Proof of Concept (PoC) plans are reviewed until validation for a final decision to progress to approval stage.

3

APPROVAL

Every level of stake-holders, including the InfoSec team, will review and sign off on iterative revisions of the PoC.

4

DEPLOYMENT

Training and actual deployment undergo continual 30-day and 60-day reviews where issues are ironed out.

Our Commitment

Businesses today want to deliver application performance and user experience. They need to be able to connect their applications and data with greater efficiency and control. With Financial Institutions challenged by digitalisation and cybersecurity directives, our commitment is to bring our cumulative expertise to the industry for future-proof connectivity and cyber resilience. Get in touch with us to accelerate your cloud transformation journey.

info@epsilontel.com
www.epsilontel.com

epsilon
a kt company