How to build trust and assurance when adopting a "cloud-first" agenda

EY
Building a better working world

Asia-Pacific's financial institutions have been waiting to solve security and compliance issues before they move mission critical applications to the cloud. But now the region's regulators have adopted favorable positions on public cloud use, what will the cloud adoption journey look like across the sector?

As more financial institutions put technology at the heart of their businesses, the public cloud will become an inevitable part of this strategy for many players

Research indicates that companies are increasingly adopting a "cloud-first"or "hybrid" strategy to keep pace with the evolving digital ecosystem.

50%
of companies will be adopting services, applications and platforms enabled by the cloud in 2018 (Forrester)

6x
rate of growth for cloud computing spending compared with traditional IT spending through 2020 (IDC Research)

But although financial institutions are regularly putting their sandbox testing facilities or support functions, such as email, in the public cloud, the same cannot be said for their mission critical applications.

A vast majority of clients are hesitating to make this move because of security concerns and compliance requirements.

Yet, sooner or later, this will have to change. Cloud technology will be key for financial institutions to improve agility, reduce costs, boost speed to market and reconnect with their customers.

To capitalize on these benefits, institutions must find a way to navigate a path through cloud security issues.

How is a "cloud-first" agenda supporting institutional strategies?

Everywhere you look in Asia-Pacific, new financial challengers are entering the market with new services and ecosystems that are disrupting traditional banking and insurance businesses.

In mature markets, with lower growth, the financial services industry is under increasing pressure to reduce operating costs. Incumbents also need to reconnect with customers – whose increasing expectations of speed and efficiency are already being met by new entrants.

In growth markets, institutions are looking for ways to cope with rapid growth both inside and outside countries of origin.

Financial institutions are seeking the competitive advantage of using public cloud infrastructure for large-scale data analytics, artificial intelligence, machine learning and blockchain.

Against this backdrop, cloud-based technologies offer all players new opportunities to improve business agility, competitiveness, cost savings and customer experience.

With customer trust and confidence critical to the success of new, cloud-based services, organizations must first address key security concerns such as:

- Where is data stored and flowing to – and who has access to it?
- Is the cloud service provider's underlying infrastructure secure enough for the organization's sensitive data and able to support regulatory compliance?
- Are cloud-based security operations and monitoring integrated with on-premise controls to provide a single view?
- How is cloud computing regulated with regard to PCI, GLBA, FFIEC, FTC, SOX, FINRA, NY-DFS, SEC-OCIE, CFTC Cyber Exam, data protection and privacy?

Cloud-based emerging technologies already driving innovation in Asia-Pacific financial services

- **Analytics and big data** – high-performance processors, visualization and advanced data mining are enabling real-time analysis across vast data sets, allowing institutions to gain game-changing insights, including better understanding customer behaviors
- **as-a-Service** – decoupling software and business operations from physical IT infrastructure are enabling the move to as-a-Service models
- **Cognitive computing** – smart automation of complex business processes using robot agents and artificial intelligence are reducing human error and costs
- **Dev ops and agile architecture** – new tools, languages and architectures are enabling applications to be built at scale in the cloud
- **Distributed ledgers** – cryptographic networks are enabling trading, clearing and settling of virtualized financial assets with a single point of consensus
- **IoT** – the data collected from IoT sensors is enabling institutions to anticipate customer needs, allowing services and advice to be provided at the optimal time to secure a sale

What are the current cloud regulations in Asia-Pacific?

Incumbents often mistakenly believe regulations prohibit offering financial services through the public cloud for privacy reasons. In fact, cloud regulators across the region are increasingly supportive of the technology – albeit with their own, individual requirements for outsourcing protections.

Hong Kong – regulated financial institutions that intend to use cloud computing or outsource services may need to notify or consult with regulators before use, as required under their outsourcing guidelines. This would involve completing a risk assessment form for HKMA's review. Financial institutions must also comply with the general principles for technology risk management in the HKMA's Supervisory Policy Manual.

China (mainland) – permits the use of cloud services that do not connect with jurisdictions. Data centers in China are not connected internationally and are subject to complex local laws and regulations that make it challenging to migrate cloud technology in the country. Although cloud-users outside of China can still communicate and collaborate with their China-based colleagues, both must use separate user accounts and cannot access company data from a common source.

Singapore – permits the use of all cloud services. There is no need to pre-consult with or pre-notify the Monetary Authority of Singapore, nor to complete a formal outsourcing questionnaire. However, financial institutions are expected to comply with all relevant MAS Outsourcing and Technology Guidelines.

Malaysia – permits the use of all cloud services and deployment models. Where data centers outside Malaysia are used to deliver the cloud services, approval is required from Bank Negara Malaysia (BNM). Financial institutions need to adopt BNM's risk management practices set out in the Outsourcing Guidelines. Financial institutions are also generally required to adopt sound and robust risk management strategies, to perform a risk analysis of their IT environment, to develop effective data management system and to carry out disaster recovery and business continuity planning.

Australia – permits and specifically conceives of the use of cloud services, including public cloud services. If the use of cloud services is a "material outsourcing" or the services are provided outside of Australia, then the financial institution must notify or consult with the Australian Prudential Regulatory Authority.

52%

"of companies say cybersecurity is a high-priority investment in 2019."

EY Global Information Security Survey 2018-19

US$ 459m

Forecasted cloud security spend across the world in 2019, an increase of 50% from 2018 (Gartner)

95%

Of cloud security failures through 2022 will be the customer's fault (Gartner)

US$ 7.3m

Was the average total cost of a data breach for a US-based company in 2018 (Ponemon Institute)

83%

Of companies store sensitive and confidential data in the public cloud in 2018 (McAfee)

How to navigate securely towards the "cloud-first" agenda

Companies migrating to the cloud must address the inherent cyber risks associated with a boundary-less environment with unlimited scalability. But cloud technology, while introducing risks, also brings with it new security capabilities – courtesy of the cloud service provider – such as:

- Network security
- Monitoring, auditing and logging
- Access management
- Secure configuration management and patching using secure golden images and reference architecture
- Security automation and orchestration

On the upside, this means financial institutions don't need to build cloud security from the ground up but can augment their provider's capabilities to meet their own requirements. However, it also means that cybersecurity and compliance are now a shared responsibility between the cloud service provider and the cloud consumer, with the strong potential for coverage gaps. Frequently, data loss episodes in the cloud are a direct result of the consumer's failure to appropriately secure the cloud environment.

It's vital to know who is responsible for each security control. Institutions should take responsibility for:

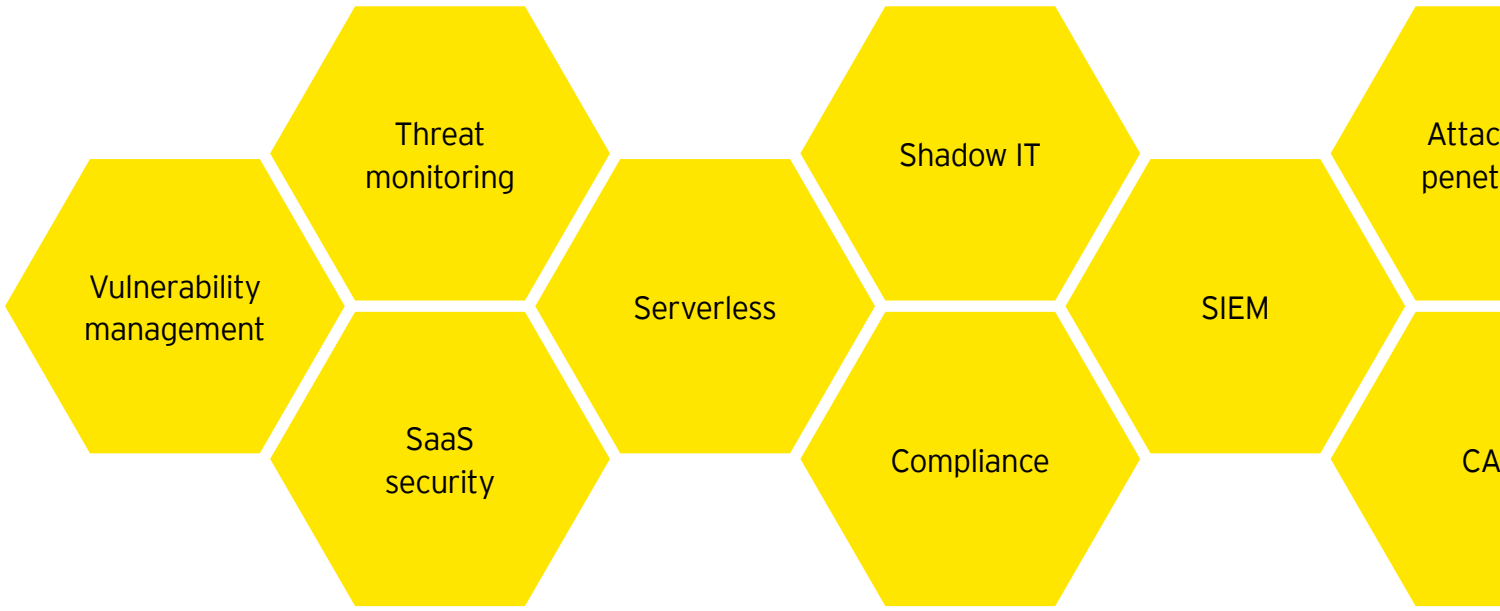
- Guardrails for proper use and controls of infrastructure
- Visibility into user actions and network activity
- Compliance of data storage and use
- Secure identity and permissions management across cloud platforms and service providers
- Secure use and monitoring of APIs and integrations
- Secure data storage and encryption as a front-line defense

How can we build trust and assurance in the cloud for regulators and internal stakeholders?

To solve cloud's inherent security and regulatory issues, institutions need a business solution focused on providing assurance to both internal and external stakeholders, including regulators.

The answer lies in a combination of security, risk, privacy and regulatory competencies. It will come, not just from cyber security professionals, but from a wide range of different disciplines, including risk, regulatory and privacy professionals.

EY cloud security services: Our portfolio of service offerings helps protect and grow security posture for clients as they leverage the cloud Cloud security capabilities can be delivered at any stage of client's journey to cloud, whether it's an assessment, design or implementation a



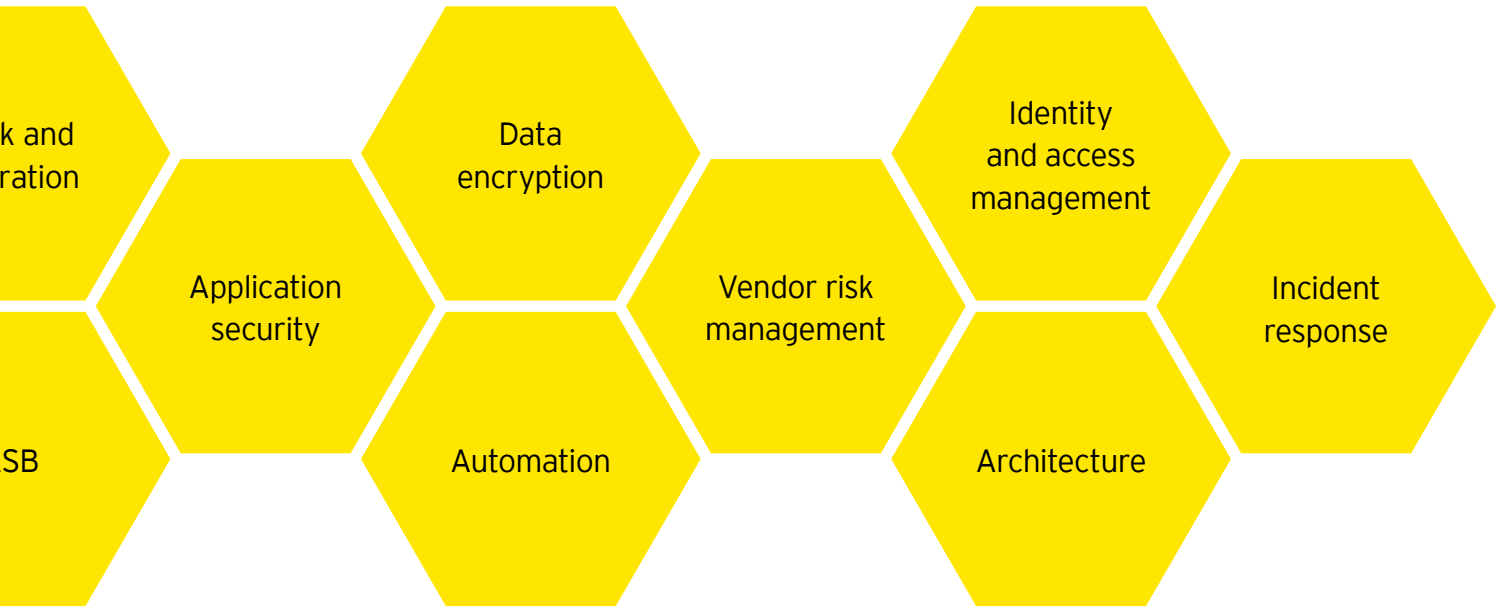
Assess

- Perform a cloud security health check aligning practices to industry standards
- Execute attack a penetration assessments identifying cloud misconfigurations
- Align cloud providers to third-party risk management practices
- Identify cloud services being used across the enterprise

Design

- Develop cloud security reference architectu
- Integrate cloud infrastructure to existing ca
- Architect and implement data encryption ac
- Implement automated security guardrails, p

d to unlock new business models, achieve scalability, and enable a safe connection to vendors, customers and employees.
nd managed service.



Implement

re and control frameworks
pabilities and leverage could-native solutions
cross cloud environments
rotecting environments to defined controls

Operate

- Perform real-time threat detection for SaaS, Paas and Iaas environments
- Identify vulnerabilities in compute, serverless and application environments
- Monitor and remediate deviations from cloud security guardrails
- Manage CASBs for data protection and threat detection use cases

Contacts

Australia
Anthony Robinson
Oceania Cyber Security Leader,
Financial Services
Email: anthony.robinson@au.ey.com
Tel: +61 2 9248 5975

Greater China
Wilson Feng
China Cyber Security Leader,
Financial Services
Email: wilson.z.feng@cn.ey.com
Tel: +86 21 2228 6855

Hong Kong
Jeremy Pizzala
Asia-Pacific Cyber Security Leader,
Financial Services
Email: jeremy.pizzala@hk.ey.com
Tel: +852 2846 9085

Hong Kong
Simon Chandran
Hong Kong Cyber Security Leader,
Financial Services
Email: simon.chandran@hk.ey.com
Tel: +852 2846 9888

Singapore
Sean Gunasekera
ASEAN Cyber Security Leader,
Financial Services
Cyber Security Leader
Email: sean.gunasekera@sg.ey.com
Tel: +65 6718 1162

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation is available via ey.com/privacy. For more information about our organization, please visit ey.com.

EYG no. 003556-19Gbl

ED None

ey.com