Deloitte.

Securing the public cloud

Addressing the technology and cyber security risks associated with public cloud adoption

October 2021

MAKING AN IMPACT THAT MATTERS since 1845

Securing the public cloud

The cloud is increasingly becoming the primary location for financial institutions to store and process data: most financial institutions have moved their applications to cloud platforms, and many of those that still have their data on-premise today are planning their imminent migration to cloud. Across all sectors, financial institutions are also modernising their digital platforms to leverage new-age application technologies and advanced analytics in tandem with their move to the cloud.

Yet too often, financial institutions are moving rapidly to migrate to the cloud without paying enough attention upfront to security. In Singapore, this concern has been made more salient following the recent circular issued by the Monetary Authority of Singapore (MAS) on 1 June 2021, which details an advisory on addressing the technology and cyber security risks associated with public cloud adoption for financial institutions.

Broadly, the advisory spells out five common key risks and control measures that financial institutions in Singapore should consider before adopting public cloud services. Throughout this report, we will examine each of these in turn, and provide financial institutions with a series of steps or considerations that would enable them to comply with the requirements, and in doing so, overcome the respective security risks that the requirements have been designed to address.

Ultimately, however, our view is that the implications of the MAS advisory for financial institutions go beyond piecemeal remediation efforts. Indeed, financial institutions who are looking to enhance their business and technology resilience, increase security, and cultivate trust during their cloud migration journey must now make the conscious decision to embrace cloud security by design.

More specifically, we believe that financial institutions should adopt a conscious and integrated approach to security right from the get-go. Such an approach would better position them to embed security into their cloud DNA at every step along the way – from conducting baseline analysis and assessing security requirements during discovery and cloud vendor selection, to determining the shared responsibility model with the cloud vendor, setting up infrastructure guardrails, and managing DevSecOps processes.

We hope that this report will provide you with some insights into the security considerations associated with public cloud adoption, as well as the steps that you can take to ensure security by design as you lead your organisations on the cloud migration journey.

Addressing the technology and cyber security risks associated with public cloud adoption

In view of the growing adoption of public cloud platforms by financial institutions, especially given the accelerated pace of digital transformation on the back of the COVID-19 pandemic, MAS recently issued an advisory on addressing the technology and cyber security risks associated with public cloud adoption in its circular dated 1 June 2021[1].

The advisory highlights several common key risks and control measures that financial institutions in Singapore should consider before adopting public cloud services, including:

Developing a public cloud risk management strategy that takes into consideration the unique characteristics of public cloud services

Implementing strong controls in areas such as Identity and Access Management (IAM), cyber security, data protection, and cryptographic key management

Expanding the financial institution's cyber security operations to include security of public cloud workloads

Managing cloud resilience, outsourcing, vendor lock-in and concentration risks

Ensuring financial institutions have adequate skillset to manage public cloud workloads and risks

In this report, we will take a closer look at each of the five risks and control measures, and detail a series of steps or considerations that would enable financial institutions to overcome these security impediments by design – and thereby, benefit from the advantages that public cloud platforms offer, while also mitigating the attendant technology and cyber security risks from the get-go.

1 "Advisory on addressing the technology and cyber security risks associated with public cloud adoption". Monetary Authority of Singapore. 1 June 2021.

Developing a public cloud risk management strategy

To develop a public cloud risk management strategy, financial institutions will first need to develop a clear understanding of the shared responsibility model, and risk of misconfigurations of the meta-structure layer that is under their responsibility. This will then, in turn, inform the design of a cloud risk management strategy that is customised to the financial institution's specific needs and threats. Finally, to identify and close any existing gaps, financial institutions should then conduct a baseline assessment of their cloud configuration management (see Figure 1).

Figure 1: Three steps to develop a public cloud risk management strategy

Step 1: Develop a clear understanding of the shared responsibility model and risk of misconfigurations of the meta-structure layer that is under their responsibility

The MAS advisory highlights the need for financial institutions to pay particular attention to several new risks introduced by public cloud platforms. These include, but are not limited to, critical fundamental issues such as the misinterpretation of the shared responsibility model, as well as misconfigurations of the meta-structure layer that is under the customer's responsibility.

As a first step to addressing these risks, financial institutions should conduct a maturity benchmarking exercise of their security process, tools, and technology. This exercise, in particular, should be conducted with the use of an appropriate standards-based cyber cloud framework, such as the National Institute of Standards and Technology (NIST) or Cloud Security Alliance (CSA) standards. Based on the outcomes of this exercise, financial institutions can then design a detailed strategy roadmap to close any identified gaps, and develop cloud security reference architectures and design patterns to implement these roadmaps.

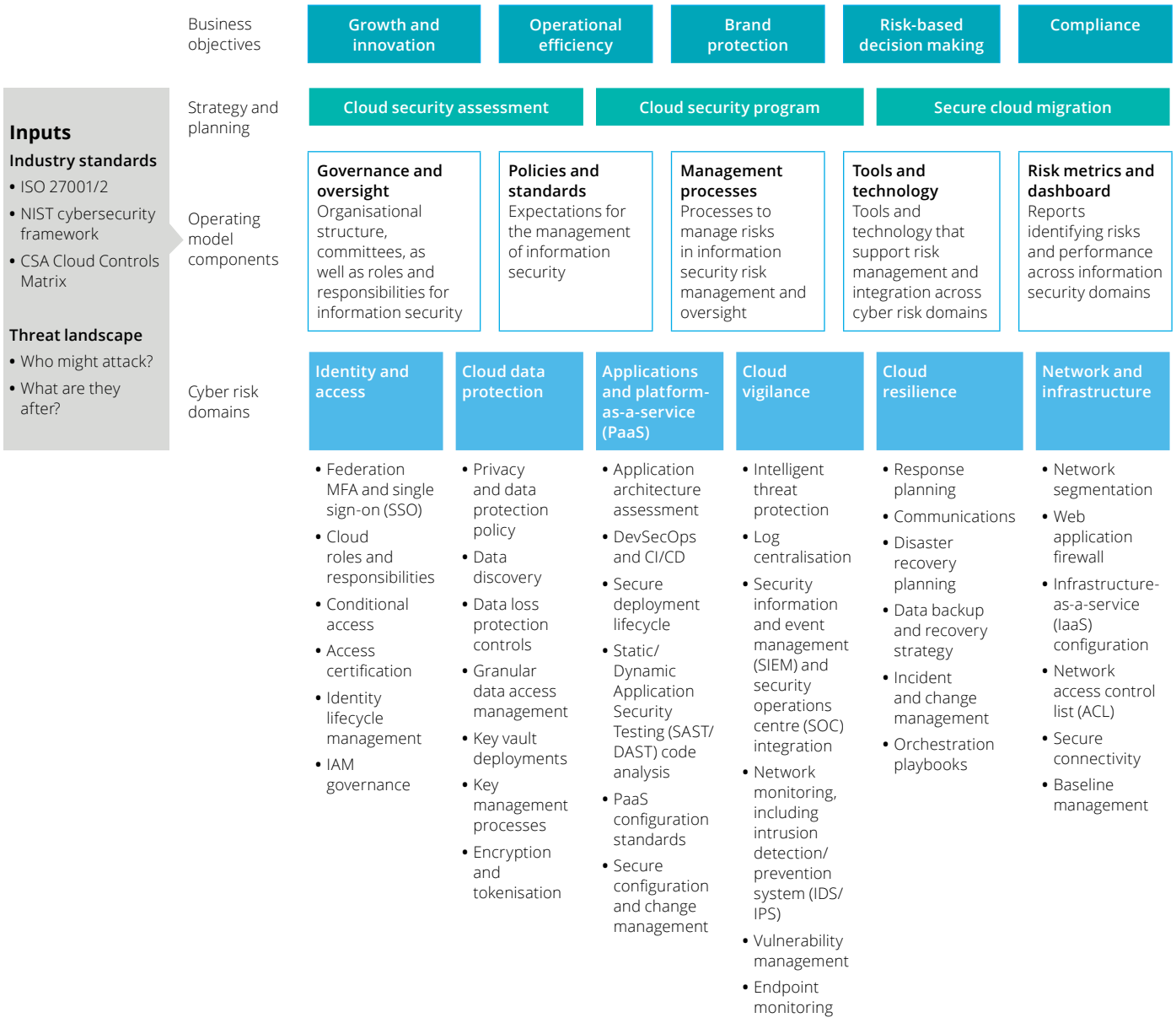
To ensure that all new interfaces, including those in the meta-structure layer, are taken into consideration during the cloud security design, implementation, and subsequent assessments, financial institutions should follow up with a threat modelling exercise for critical applications and assets in the public cloud. Threat modelling will yield not only detailed analyses of the risks and threats that exist at all cloud-enabled interfaces, but also enable the creation of security-focused test cases to help financial institutions ensure that their solution is compliant and in line with leading practices.

Step 2: Design a cloud risk management strategy that is customised to the organisation

To develop a customised approach to managing cloud risks in their organisations, financial institutions should leverage the use of an industry-standard cloud computing risk framework to conduct a current state assessment, and identify any gaps from the people, process, and technology perspectives.

Broadly, such a framework should cover all the key technology, cyber, and extended enterprise risks, including but not limited to the following: governance, risk management, and compliance; delivery strategy and architecture; infrastructure security; IAM; data management; business resiliency and availability; IT operations; vendor management; and business operations (see Figure 2).

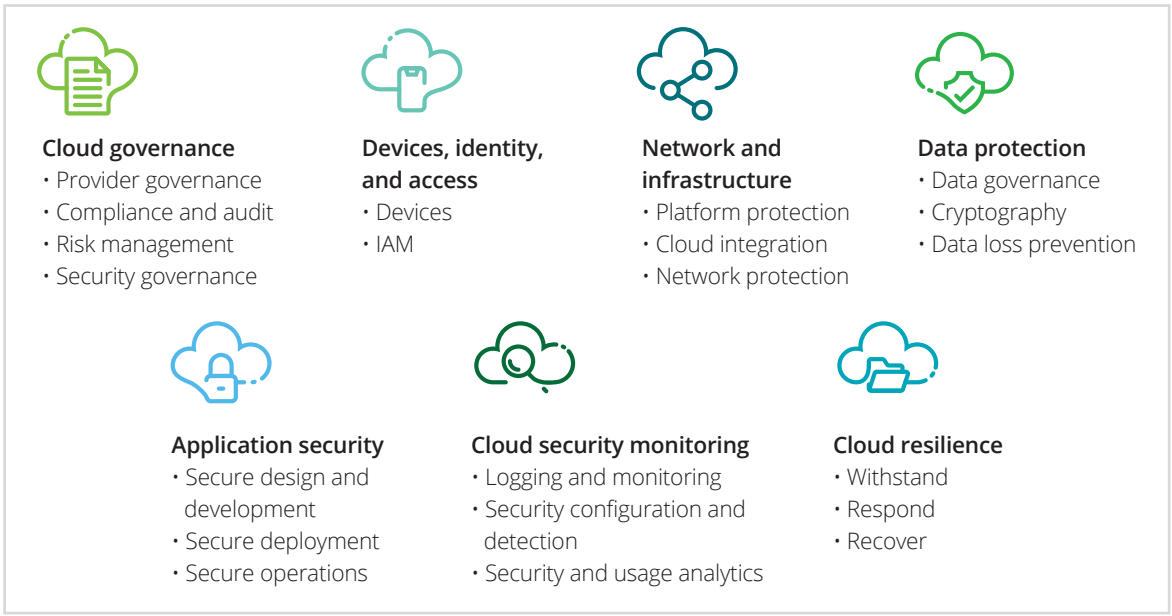
Figure 2: An industry-standard cloud computing risk framework



Apart from benchmarking against industry best practices such as the NIST cybersecurity framework and CSA Cloud Controls Matrix, the maturity assessment should also cover a number of cloud-specific areas to identify gaps that will need to be addressed in future roadmaps or process improvements. In particular, financial institutions should consider benchmarking their capabilities across 21 critical cloud security capabilities (see Figure 3) – each of which can be further distilled into additional sub-capabilities and closed statements.

The takeaways from this exercise can then be used to inform the design of customised reference architectures for specific cloud solution providers (CSPs), cloud-based solutions, and software-as-a-service (SaaS) deployments.

Figure 3: 21 critical cloud security capabilities



Step 3: Conduct a baseline assessment of cloud configuration against security benchmarks to identify and close any gaps

To identify and mitigate existing security gaps, financial institutions should conduct a baseline assessment of cloud configuration against security benchmarks. This assessment should cover areas such as cloud security configuration; comprehensive container security; discovery scanning of assets; roles, responsibilities, and leading practices in account management; as well as a compliance review of policies and standards.

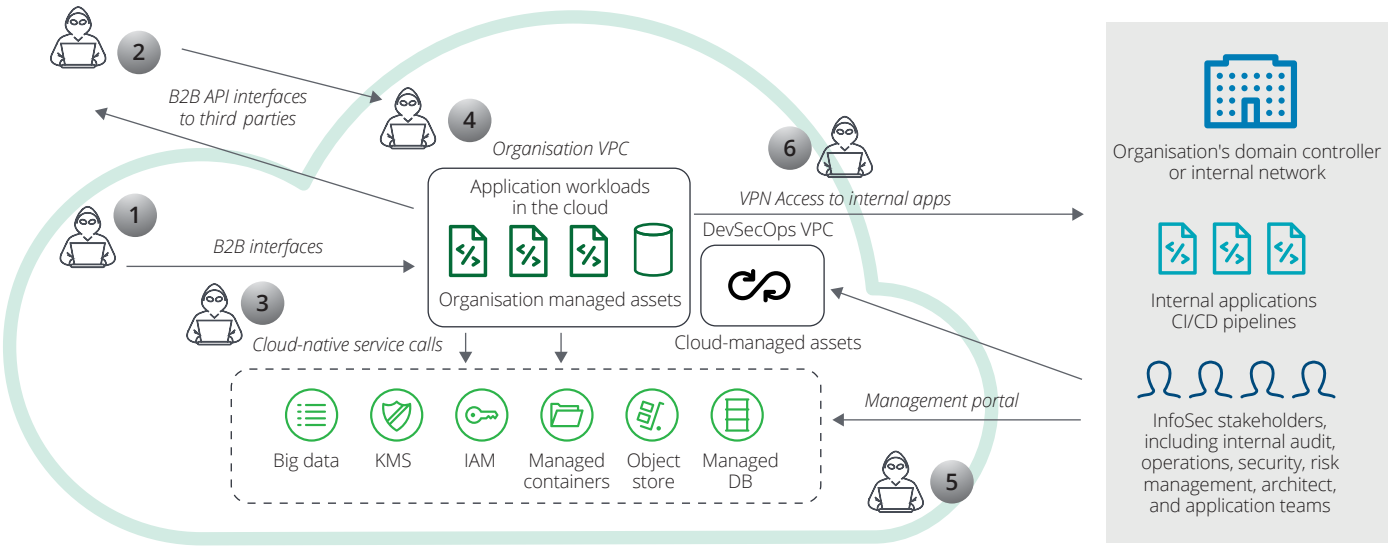
Typically, the outputs of such an assessment will take the form of comprehensive reports specifying the gaps and respective risk ratings, with detailed remediation recommendations. Additionally, good practices identified during the assessment should also be analysed in greater detail to enable the financial institution to build on its strengths. Thereafter, the open risk items must be quickly remediated to create a clean baseline on which the financial institution can build additional capabilities to automate cloud security for continuous compliance.

Depending on whether the model in question is a platform-as-a-service (PaaS) or software-as-a-service (SaaS), the automation of cloud security could differ in terms of implementation. Specifically, for PaaS models, financial institutions would be able to work with their managed service providers to implement cloud security posture management (CSPM) and container workload protection platform (CWPP) solutions.

On the other hand, for SaaS models, financial institutions will need to pay more attention to the configuration of their applications. With some enterprise SaaS solutions today possessing more than 200 service configuration settings – not to mention third-party integration and other customisation options – this challenge is becoming increasingly complex for financial institutions. To flag any insecure configurations in the SaaS solution as soon as it reaches the user acceptance testing (UAT) or production phases, monitoring tools can be deployed to provide SaaS security posture management. Incident response can also be managed by integrating the detailed remediation recommendations for specific events with the financial institution's IT service management (ITSM).

Unlike conventional vulnerability assessments or penetration testing (VA/PT) exercises that examine only the Application Programming Interfaces (APIs) and other infrastructure interfaces exposed to the end-customer, a cloud security assessment examines all areas within the financial institution's areas of responsibility. To understand the differences between conventional VA/PT exercises and cloud security assessments, it is useful to have an overview of the six different types of interfaces in a typical cloud application (see Figure 4).

Figure 4: An illustration of the six interfaces in a typical cloud application



- **Type 1** and **2 interface**: Traditional web and mobile business-to-customer (B2C) interfaces and business-to-business (B2B) or B2C APIs that are well-understood
- **Type 3 interface:** Interfaces that enable the integration of cloud-native services with the financial institution's existing solutions
- **Type 4 interface:** Interfaces that manage solutions or workloads on the cloud, such as IaaS virtual machines (VM) or customer-managed container deployments
- **Type 5 interface**: Interfaces that manage rules, policies, or rules as defined by the management portal or API-based access of the CSP
- **Type 6 interface**: Interfaces that enable the secure integration of workloads which have migrated to the cloud

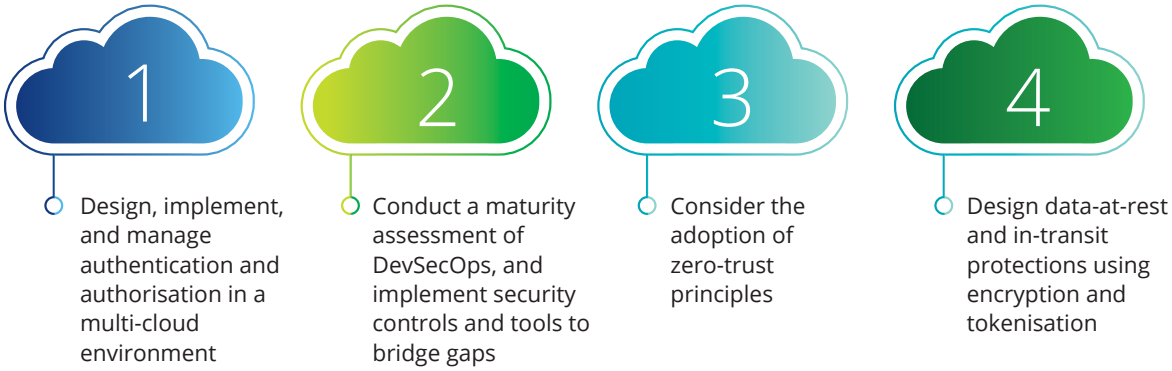
At most financial institutions, Type 1 and 2 interfaces are already frequently tested for security issues under conventional VA/PT approaches. In the context of the cloud, the configurations and meta-structure of the cloud application will need to be additionally considered, and any new Type 1 and 2 interfaces that have been introduced will also need to be secured.

On the other hand, Type 3 to 6 interfaces will require additional sets of tools to ensure that the solution migration process does not result in any new vulnerabilities. As pointed out in the MAS advisory, it is crucial for financial institutions to focus on their cloud meta-structure configurations, as these are responsible for defining the security level of the interactions between a financial institution's applications and its cloud-native services.

Implementing strong controls in a cloud environment

Financial institutions will be expected to implement strong controls for their cloud environments in areas such as IAM, cyber security, data protection, and cryptographic key management. This requires them to design, implement, and manage authentication and authorisation in a multi-cloud environment; conduct a maturity assessment of DevSecOps and implement security controls; consider the adoption of zero-trust principles; as well as design data-at-rest and in-transit protection using encryption and tokenisation (see Figure 5).

Figure 5: Four considerations to implement strong controls in a cloud environment



Consideration 1: Design, implement, and manage authentication and authorisation in a multi-cloud environment

To design and implement enterprise-wide identity access management and privileged access management (IAM/PAM) in the cloud, financial institutions should seek to leverage the use of cloud-native services. These include, for example, role-based access controls, multi-factor authentication (MFA), as well as blast radius containment strategies to integrate the authentication processes of on-premise and cloud environments.

Key activities include defining users, roles, and permissions; designing authentication specifications; defining platform processes for privileged identity management and privileged access management (PIM/PAM); building user, user groups, and roles; implementing MFA for users; performing user mapping; as well as developing user management and privileged access management processes.

Consideration 2: Conduct a maturity assessment of DevSecOps, and implement security controls and tools to bridge gaps

To ensure that security is embedded throughout their continuous integration and deployment (CI/CD) pipelines, financial institutions should adopt the appropriate secure software development lifecycle (SSDLC) for their DevOps. This approach, known as DevSecOps, is especially relevant for financial institutions operating in the cloud environment.

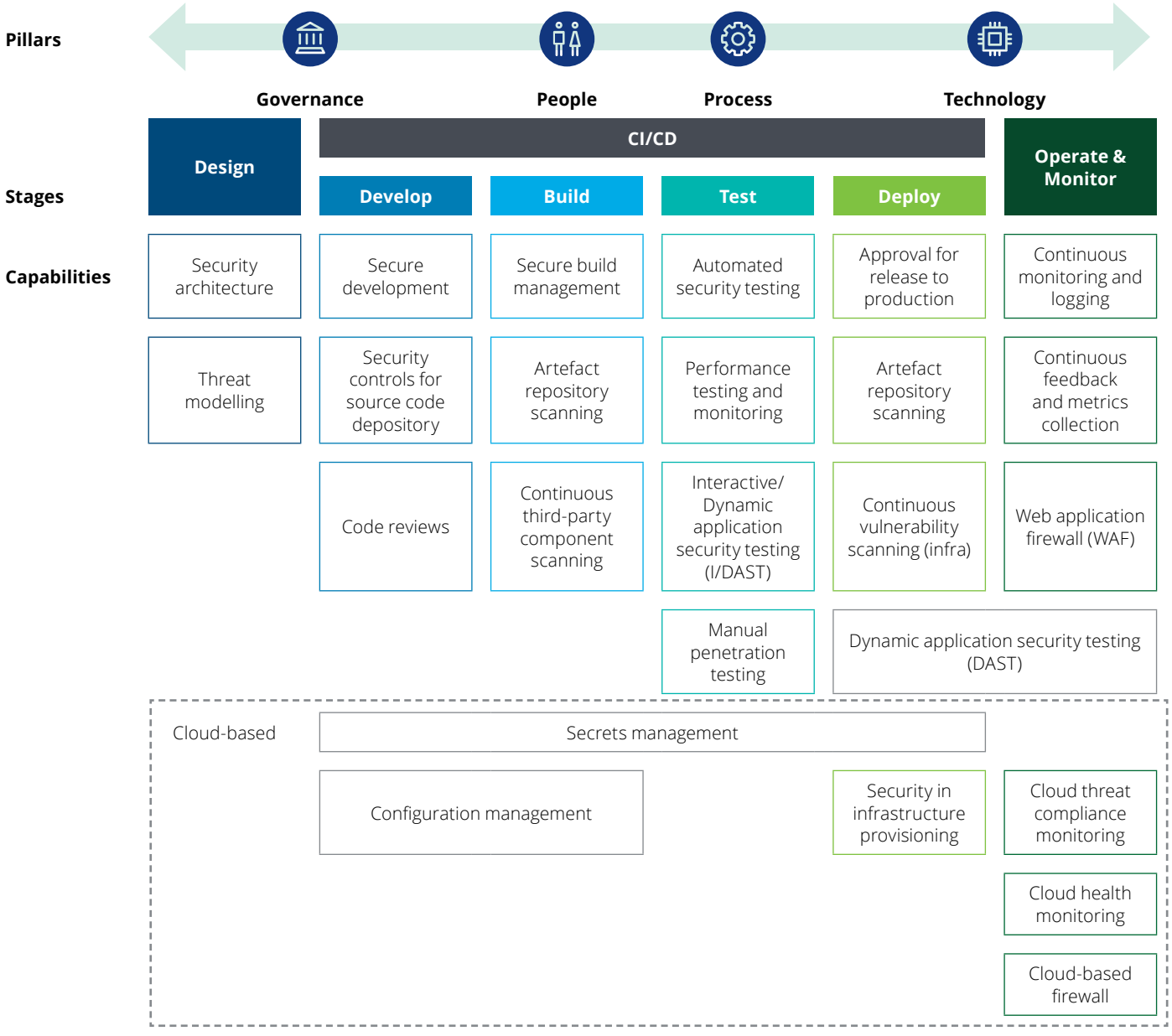
Generally speaking, DevSecOps enables organisations to embed security into their workflow rather than as a bolt-on to development. This allows developers and security professionals to achieve their shared goals of having secure configurations continuously monitored, remediated, and managed for cybersecurity to drive the creation of agile, resilient solutions.

For their part, cloud platforms typically provide their users with comprehensive sets of tools and services to accelerate the development and deployment of their software pipelines. However, this increased speed also tends to be accompanied by a corresponding increase in software vulnerabilities.

To design, implement, and operate DevSecOps pipelines securely in the cloud, financial institutions should therefore conduct a maturity assessment and gap analysis by benchmarking their DevSecOps processes against industry benchmarks. Broadly, the DevSecOps framework should cover the six main stages of a pipeline – Design; Develop; Build; Test; Deploy; as well as Operate & Monitor – with the security capabilities and controls for each stage mapped to leading practices (see Figure 6).

Apart from detailed maturity assessments, the framework can also be leveraged to generate health scorecards and strategy roadmaps for a financial institution's DevSecOps journey across both on-premise and cloud environments. At this juncture, security controls – such as static application security testing (SAST), dynamic application security testing (DAST), container security, and cloud compliance monitoring – should also be designed and implemented to bolster the security of the financial institution's cloud applications and pipelines.

Figure 6: Six main stages in a DevSecOps pipeline



Consideration 3: Consider the adoption of zero-trust principles

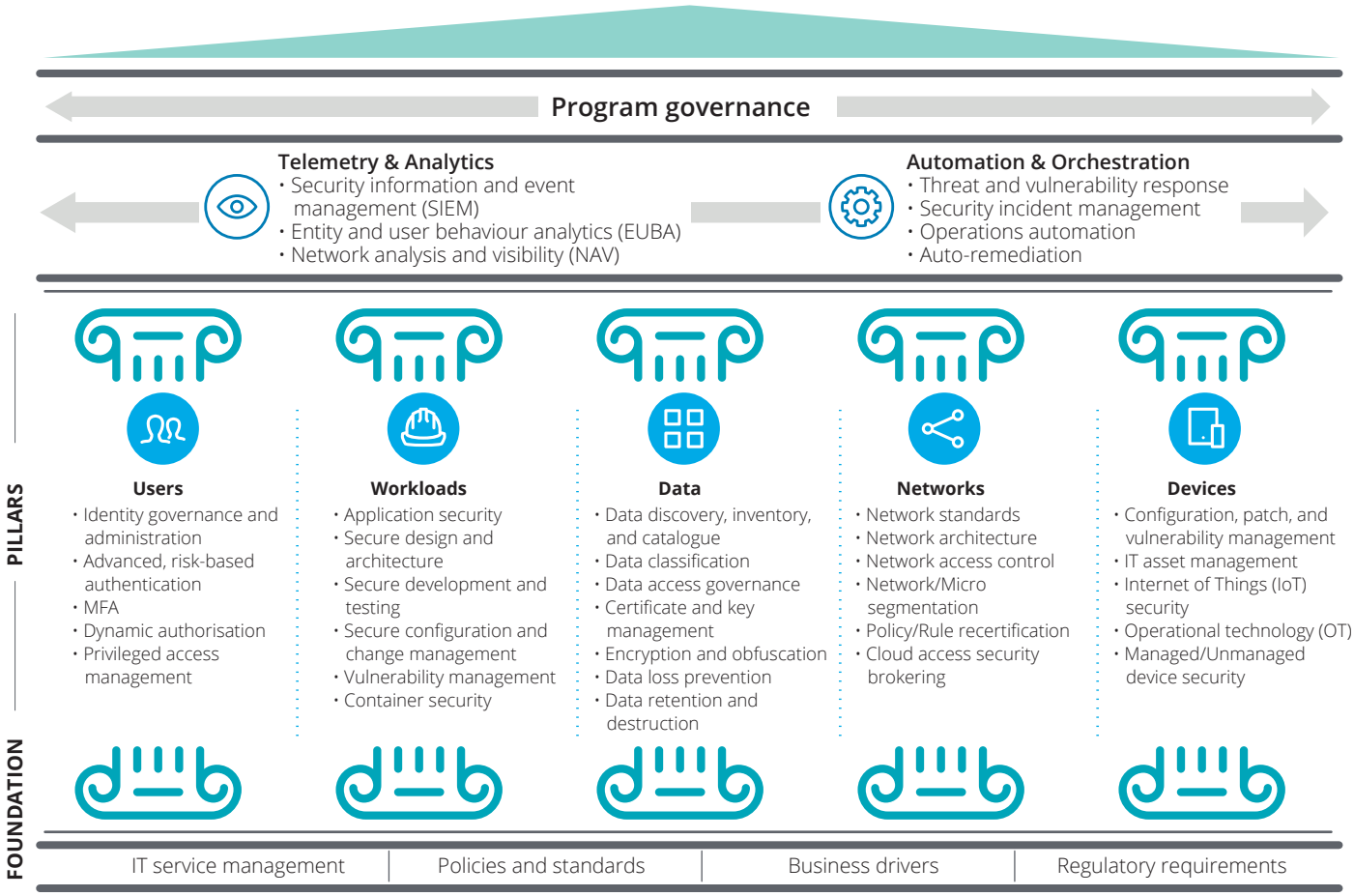
Under the MAS advisory, financial institutions are encouraged to consider the adoption of zero-trust principles in their overall cloud architecture. Broadly, a comprehensive adoption and implementation of zero-trust principles should entail the development of strong capabilities across five pillars: Users; Workloads; Data; Networks; and Devices. These five vertical pillars should, in turn, be supported throughout by two horizontal pillars: Telemetry & Analytics, and Automation & Orchestration (see Figure 7).

As financial institutions differ in terms of their maturity levels across each pillar, a customised roadmap should be developed to cover the different zero-trust milestones. Key initial activities could include, for example, determining the zero-trust scope; establishing foundational capabilities and mapping traffic flows or application relationships; federating and centralising user management; as well as establishing data discovery, inventory, encryption, and governance. In tandem, financial institutions should also begin implementing telemetry and analytics, as well as automation and orchestration, to give these capabilities a sufficient runway to mature over time.

Thereafter, financial institutions should implement device security services; secure the wide area network (WAN) and network security between cloud and on-premise environments to support cloud adoption; restrict network access using software defined perimeters (SDP); and build zero-trust cloud environments; and integrate or extend cloud-native security capabilities to on-premise environments.

Once financial institutions have assessed and migrated their applications to a zero-trust cloud environment, they would then need to define a strategy for their applications. This could entail virtualising systems that are not suitable for the cloud, implementing micro-segmentation in the cloud enclave, and finally, further advancing their zero-trust capabilities through additional integrations and adoption of leading capabilities across the five fundamental zero-trust pillars.

Figure 7: Comprehensive adoption of zero-trust principles across five vertical pillars



Consideration 4: Design data-at-rest and in-transit protections using encryption and tokenisation

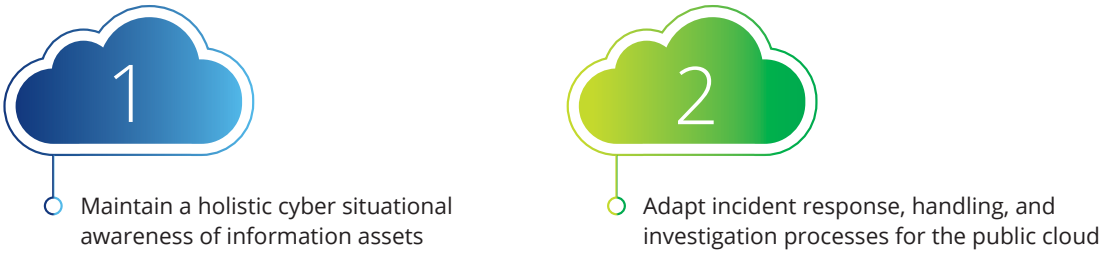
To ensure adequate and appropriate data protection coverage at all stages – from in-use to at-rest, and in-transit – financial institutions should adopt a cloud-native perspective in the design, implementation, and deployment of managed services for its data protection.

Key focus areas include designing and integrating data protection on the cloud with the use of encryption, tokenisation, and masking; cryptography and key management, including managed key services offered by CSPs and dedicated cloud-hosted hardware security modules (HSM); as well as certificate management and mutual transport layer security (mTLS) authentication.

Expanding the financial institution's cyber security operations

In order to expand their cyber security operations to include security of public cloud workloads, financial institutions will need to maintain a holistic cyber situational awareness of information assets, and adapt their incident response, handling, and investigation processes for the public cloud (see Figure 8).

Figure 8: Two steps to expand the financial institution's cyber security operations



Step 1: Maintain a holistic cyber situational awareness of information assets

To maintain a holistic cyber situational awareness of information assets, financial institutions must avoid performing the security monitoring of their cloud and on-premise assets in siloes. This requires adequate monitoring capabilities to cover all the new assets and technologies introduced by the cloud environment, as well as the seamless integration of logging and monitoring solutions with existing on-premise solutions to create a single, integrated security incident event monitoring (SIEM) solution.

The MAS advisory also goes one step further to recommend that financial institutions put in place a single pane of glass architecture to centralise all monitoring and logging activities. The advantages of having such a single point of access and control include a consistent view of all monitoring and logging activities, ease of managing data storage and retention, as well as centralised access control and auditing. The caveat, however, is that financial institutions will need to take measures to ensure the security of data that is in transit to this central repository.

Although every CSP has its own solutions for the monitoring and management of the different services, containers, applications and infrastructure, some leading practices have been observed across the board. These include, for example, setting up log storage according to requirements to ensure compliance for log retention; setting up log exports for security and access analytics; enabling data access audit logs to track users who have accessed data for sensitive engagements; and creating rules to filter sensitive log data to comply with standards.

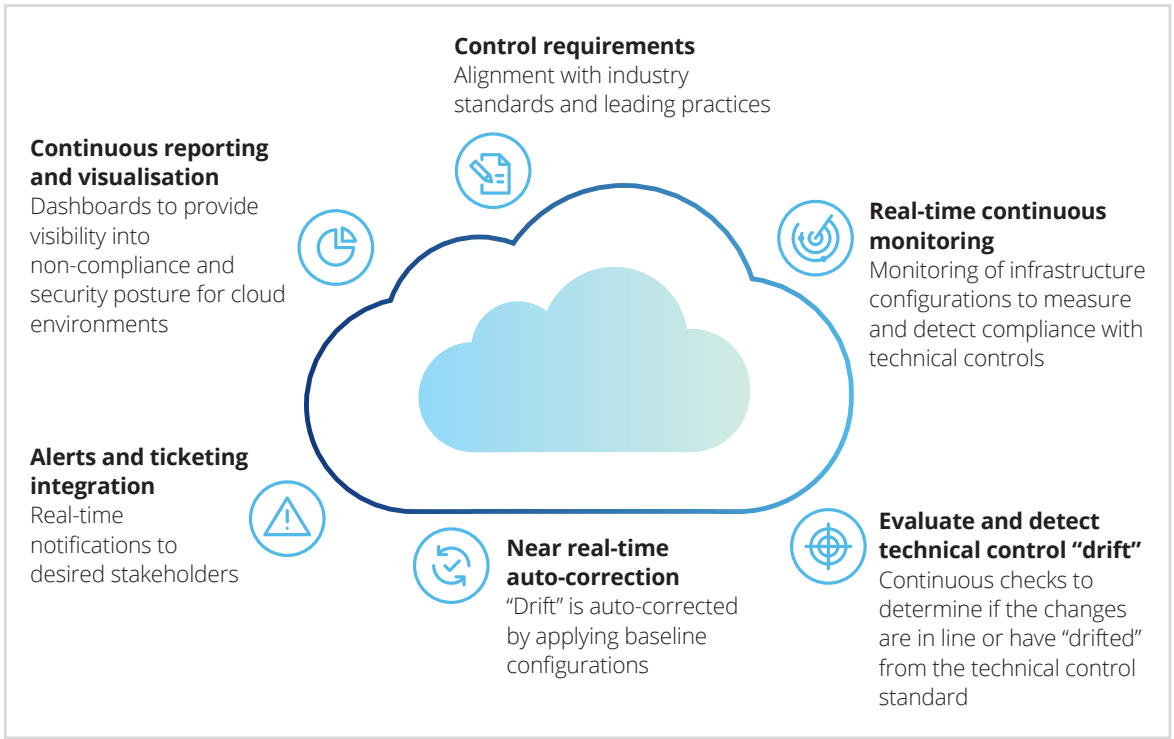
Step 2: Adapt incident response, handling, and investigation processes for the public cloud

Under the MAS advisory, financial institutions are encouraged to integrate non-compliance alerts from their CSPM and CWP platforms to their ITSM tools. To achieve this, financial institutions will first need to baseline their cloud security controls framework, before leveraging the capabilities of their CSPM/CWPP for cloud compliance monitoring, or cloud security posture management. Then, they would need to establish continuous cloud compliance metrics and analytics, before integrating the security alerts with their ITSM tools.

To enable near real-time auto-remediation of non-compliance – which would represent a drastic reduction in the risk window from minutes or even hours – financial institutions will also need to consider how they can operate their incident response processes at DevSecOps speed. In this respect, Deloitte Fortress – our proprietary platform – has been developed to enable financial institutions to achieve this through coverage and automation against a full set of industry standards and leading practices (see Figure 9).

In addition to established security configuration guardrails that automatically revert unacceptable configurations back to compliance with control standards, the Deloitte Fortress platform also enables financial institutions to build in custom automation on top of the existing framework for organisation-specific controls at low-to-no cost. Furthermore, the use of context-based policy enforcement also allows for the use of specific data-driven rules to address a variety of different control cases.

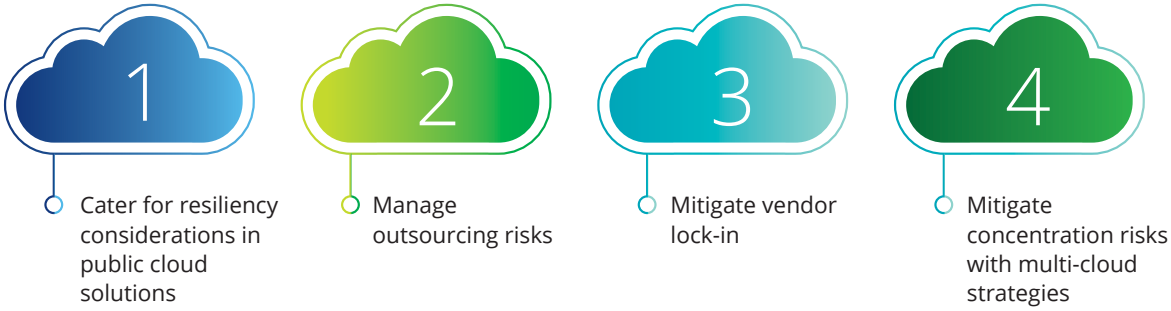
Figure 9: An overview of Deloitte Fortress



Managing cloud resilience and other risks

In addition to resiliency considerations, financial institutions should also take steps to manage other risks associated with the use of public cloud platforms. These include, for example, outsourcing risks, vendor lock-in risks, as well as concentration risks (see Figure 10).

Figure 10: Four steps to manage cloud resilience and other risks



Step 1: Cater for resiliency considerations in public cloud solutions

While cloud platforms provide resiliency options, applications do not by default become resilient by virtue of residing in the cloud. More specifically, to ensure resiliency, financial institutions need to understand the application requirements for resiliency, analyse whether their CSP – whether it is an IaaS, SaaS, or another type of provider – provides the necessary options for the required level of resiliency, and ensure that their cloud architecture is correctly configured to deliver that desired level of resiliency.

When translating resiliency requirements and commitments to corresponding cloud configurations, financial institutions must examine the specifics in detail. These include, for example, identifying business needs in order to measure the appropriate metrics, such as the Recovery Point Objective (RPO) and Recovery Time Objective (RTO), over time; developing IT disaster recovery plans and conducting exercises; as well as identifying and establishing possible redundancies and recovery plans for cloud service disruptions.

Step 2: Manage outsourcing risks

In terms of their outsourcing due diligence, financial institutions should consider the use of independent audits and expert assessments of their cloud outsourcing arrangements. These include, but are not limited to, readiness assessments for a variety of regulatory and industry requirements – such as the MAS Technology Risk Management (TRM) Guidelines, and requirements set out by the Association of Banks in Singapore's Outsourced Service Provide Audit Report (OSPAR) – as well as in-depth security assessments of proposed cloud solutions, to provide a view of the security issues within the financial institution's area of responsibility on the cloud.

Step 3: Mitigate vendor lock-in

To plan for the continuation of business activities during unforeseen disruptions, most financial institutions already have business continuity management (BCM) strategies in place. As part of the BCM process of documenting procedures that should be employed in the event of an adverse disruption, financial institutions should also seek assurance that they would be able to operate at a minimum level of service if their CSPs were to fail.

In particular, financial institutions should draw up a clear and robust exit plan from their CSP right from the start. This requires understanding the modalities of exiting their arrangements with the CSP, including developing back-up plans to mitigate any risks associated with switching to alternative CSPs or bringing their activities back to in-house operations; as well as understanding the extent to which their applications are using proprietary components, how easily these applications can be transferred to alternative CSPs, and the availability of such applications in the market, to enable financial institutions to anticipate vendor lock-in risks early on in the cloud migration process.

Step 4: Mitigate concentration risks with multi-cloud strategies

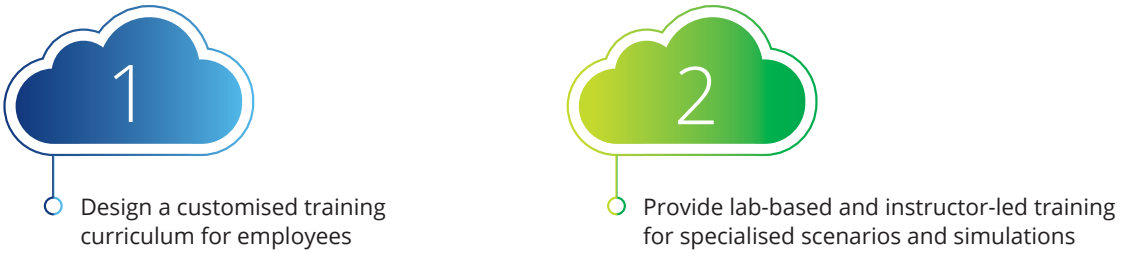
Multi-cloud strategies enable financial institutions to deploy workloads across multiple cloud platforms, and thereby provide greater flexibility than single-cloud strategies by enabling them to better manage costs, avoid vendor lock-in, and improve resiliency.

Nevertheless, this approach comes with several security pitfalls that will need to be mitigated. To benefit from the advantages of multi-cloud deployments, while avoiding these pitfalls, security controls and processes must be developed in a way that enables persistent controls to follow workloads wherever they run. These controls must also be put in place throughout the entire lifecycle to ensure uniform security and compliance enforcement across all of the financial institution's multi-cloud environments.

Ensuring adequate skillsets

To ensure that they possess adequate skillsets to manage public cloud workloads and risks, financial institutions should design customised training curricula for their employees to cover cloud and technology-related topics. In addition, lab-based and instructor-led trainings may also be useful in equipping employees with the necessary skills to manage specific scenarios (see Figure 11).

Figure 11: Two steps to ensure adequate skills



Step 1: Design a customised training curriculum for employees

To bolster cloud and technology-related skills across the organisation, financial institutions could benefit from the design of a customised training curriculum for their employees. For frontline IT teams in particular, a simulated cyber training curriculum could be beneficial in helping them to learn to respond to real-world cyber attacks.

Specifically, by providing a hyper-realistic, virtual environment – one that closely mimics the financial institution's real environment – such a curriculum could enable application developers to experience simulated, real-time attacks on their applications, and develop the necessary security acumen and cross-team communication skills that they will need to effectively protect their organisation's infrastructure.

Other training areas could also include cyber cloud topics, such as continuous compliance, security monitoring, and security configuration; DevSecOps topics, such as maturity planning and roadmaps and SAST/DAST; as well as zero-trust topics, including roadmaps to zero-trust maturity, and the design of zero-trust reference architecture.

In addition, certifications provided by the major CSPs could also be useful for obtaining platform-specific knowledge in key domain areas, and could provide a framework for financial institutions to design training and learning paths with CSP-specific certifications in mind.

Step 2: Provide lab-based and instructor-led training for specialised scenarios and simulations

Often, specific situations that a financial institution is facing may also necessitate specialised training sessions. These include, for example, the need for IT and security teams to increase their familiarity with new platforms that the financial institution is looking to migrate to, or the need to resolve certain specific issues that accompany the implementation or design of specific cloud technologies.

Ideally, such training activities should be conducted through labs or other instructor-led demonstrations to enable employees to gain more hands-on experience. In certain instances, it may also be possible to combine other organisational goals with the training curriculum, for example, by facilitating the employees' creation of a minimum viable product (MVP) or some form of prototype as part of a training session.

Looking ahead

In recent years, cloud has emerged as one of the largest areas of investments for financial institutions: many of them already have a significant portion of their IT infrastructure in the cloud, and many more are in the process of migrating their core business applications. But as more data and applications move outside their traditional security perimeter, the risk of cyberattacks increases exponentially for financial institutions.

As we have reiterated throughout this report, staying one step ahead of these attacks will require financial institutions to adopt a conscious, integrated approach to security by design from the get-go. Nevertheless, we are cognisant that even the most well-designed integrated strategies can fail if they are not implemented by an integrated team.

In many financial institutions, cyber security teams tend to be siloed from the rest of the organisation, often with minimal or incomplete transparency. As financial institutions continue to accelerate their cloud migration journeys, this issue will likely only grow – and perhaps even cause the migration process itself to become more difficult.

What is urgently needed, therefore, is for cloud and cyber teams to come together under a shared operating model – one that takes into consideration the various aspects related to the cloud migration journey, including but not limited to the talent operating model, DevSecOps, and microservices.

Apart from enabling higher levels of collaboration, coordination, and implementation across controls, such a shared operating model could also ensure that risk management, compliance, and other security practices are built in at the IT infrastructure layer from the very beginning – and thereby allow financial institutions to focus their efforts on more value-adding activities, such as leveraging the cloud platform for enhanced business performance and improved customer experiences.

Ultimately, the cloud migration process presents financial institutions with both the opportunity and necessity to rethink their security models, tools, and capabilities. As they embark on this journey, now is an opportune time for them to re-examine their controls framework, lever it up with a more integrated cloud and cyber approach – and build the secure cloud landing zones that will eventually form the basis of their operating models for a long time to come.

Contact us

For more insights, please contact

Thio Tse Gan
Financial Services Industry Leader
Deloitte Southeast Asia
tgthio@deloitte.com

Eric Lee
Executive Director, Risk Advisory
Deloitte Southeast Asia
ewklee@deloitte.com

Amol Dabholkar
Director, Risk Advisory
Deloitte Southeast Asia
adabholkar@deloitte.com

Southeast Asia Financial Services industry practice

Southeast Asia Financial Services Leader
Thio Tse Gan
tgthio@deloitte.com

Guam
Tung Wei-Li
wtung@deloitte.com

Indonesia
Rosita Sinaga
rsinaga@deloitte.com

Malaysia
Anthony Tai
yktai@deloitte.com

Justin Ong
keaong@deloitte.com

Philippines
Anna Marie Pabellon
apabellon@deloitte.com

Singapore
Thio Tse Gan
tgthio@deloitte.com

Thailand
Nisakorn Songmanee
nsongmanee@deloitte.com

Vietnam
Ngoc Tran
ntran@deloitte.com

Audit & Assurance
Tay Boon Suan
bstay@deloitte.com

Consulting
Mohit Mehrotra
momehrotra@deloitte.com

Financial Advisory
Jeff Pirie
jpirie@deloitte.com

Radish Singh
radishsingh@deloitte.com

Risk Advisory
Thio Tse Gan
tgthio@deloitte.com

Tax & Legal
Michael Velten
mvelten@deloitte.com

Deloitte.

Designed by CoRe Creative Services. RITM0869961