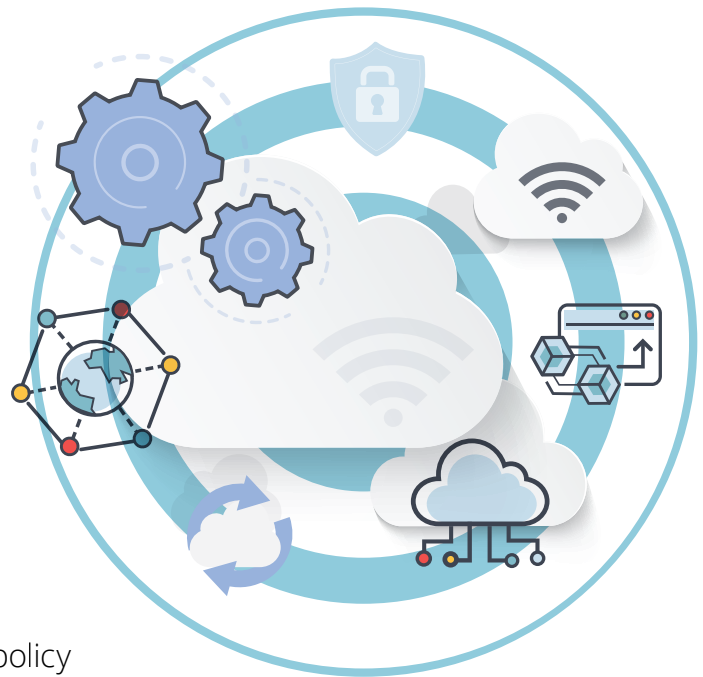




Deloitte Services for Cloud IaaS and PaaS Policy



Enabling agencies to achieve compliance to Cloud policy

Agencies that have footprint in Government on Commercial Cloud (GCC) platform are expected to comply to the requirements stated in the Cloud Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) policies by 1 November 2023.

The policy covers areas surrounding cloud security architectures, cloud security controls, processes and governance.

Key areas



• • • • •

Architectural changes

Aligning the existing security architecture with the new policy requirements and adopting security by design principles.

• • • • •

New security controls

Designing and implementing controls such as WAF, EDR, DLP, CI/CD, logging and monitoring for threats specific to cloud use cases.

• • • • •

Data resiliency

Mechanisms to implement backup and restoration requirements in the cloud, in alignment with backup plans.

• • • • •

Automation

Incorporating automation in container security, security testing and incident playbooks for common incidents with automatic incident handling.

• • • • •

Identity and access management

Establishing IAM lifecycle for new agency users, third-party users and API's, enforcing least privilege, privileged account monitoring and management.

• • • • •

Threat & risk management







Performing threat modelling and risk assessment to strike the right balance between the asset criticality and the security controls.

How can Deloitte support?

Deloitte's Cyber Cloud offering supports organisations in the complete cycle from moving business processes to the cloud through to operating it in a secure and private way.

We have worked with government agencies and have institutional knowledge of designing and implementing security solutions in Government on Commercial Cloud (GCC) platform. Our focused approach leverages a mix of deep practitioner insights, accelerators, technology tools and innovation frameworks to help agencies understand the multitude of factors that shape their cloud security posture.

Our approach

Deloitte offerings	Our approach	Estimated timeline	Outcomes
 <p>Cloud security assessment Assess existing architecture and processes and develop actionable recommendations to align with cloud policy requirements.</p>	<ul style="list-style-type: none"> Conduct workshops with key agency stakeholders (e.g., security architect, cloud security architect, cloud security engineer) to understand and review the existing applications deployed in GCC, security architecture, existing controls and processes. Conduct analysis of existing controls vis-à-vis the cloud security policy requirements and identify gaps. Develop prioritised and pragmatic recommendations to align with cloud policy requirements. 	 <p>3 to 4 weeks per application</p>	<ul style="list-style-type: none"> Actionable remediation plans to align with cloud policy requirements. Changes required in existing security architecture and processes to align with cloud policy requirements.
 <p>Architecture design Develop security reference architectures to align with the cloud policy requirements.</p>	<ul style="list-style-type: none"> Based on the recommendations from the "Cloud security assessment", design the target-state security architecture blueprint incorporating the additional security controls to be implemented. For applications that are hosted in AWS and Azure, design the target state security architecture to migrate from GCC 1.0 to GCC 2.0. 	 <p>3 to 4 weeks per application</p>	<ul style="list-style-type: none"> Target state cloud security architecture that is aligned with cloud policy requirements.
 <p>Implementation Assist with implementation of security controls to align with the cloud policy requirements.</p>	<ul style="list-style-type: none"> Based on the architecture design, determine the new security controls to be implemented, changes to existing security controls and dependencies. Obtain approval on the implementation approach and plan from Architecture committee. Agency to subscribe/procure additional security capabilities and Deloitte to implement as per change plan. Perform security testing. 	 <p>3 to 6 months</p>	<ul style="list-style-type: none"> Implemented security architecture and controls that is aligned with cloud policy requirements.

Key credentials

Cloud security design and implementation (Government)

Designed security architecture and implemented security controls for cloud-based data analytics solution in GCC. Deloitte also conducted a cloud threat and risk assessment and provided advice on security control options to align with the agency's risk profile and compliance requirements.

Cloud security reference architectures (Government)

Designed secure cloud reference architecture across all the major CSPs and developed infrastructure-as-code (IaC) templates for common application use cases.

Cloud security reference architectures (Financial Institution)

Designing security architecture, implementing and carrying out security testing for the direct debit functionality on CSP to be used by the various financial institutions and billing organisations. The team hardened the security configurations of the various IaaS and PaaS services used in the solution and the 3rd party commercial-off-the-shelf solutions.



Our accelerators

CSP security reference architecture:

Repository of cloud security architecture guiding principles which can be leveraged to build cloud security blueprints for future cloud cyber risk program across all major cloud service providers (CSP).

Deloitte cloud security risk framework:

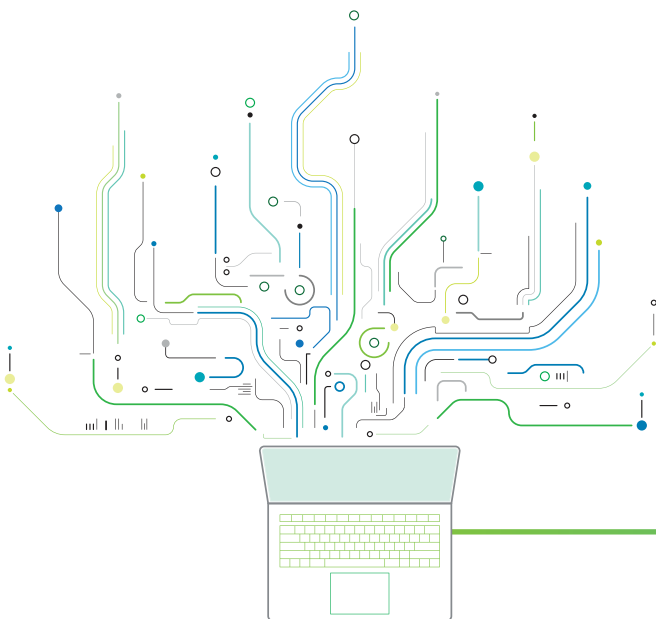
The cloud security risk framework incorporates specific security areas and is built on industry-leading practices and regulatory expectations. It allows an organisation to take stock of current capabilities to manage cloud risk.

Deloitte cloud controls framework:

An integrated cloud controls framework mapped to industry control sets and common controls. It is an accelerator and can be customised for an organisation's specific controls environment.

Deloitte DevSecOps framework:

Used by multiple clients to measure the maturity of DevSecOps and do road-mapping and gap-remediation in DevSecOps across people, process and technology.



Contact details



Weng Yew Siah
Executive Director
Deloitte Risk Advisory
wysiah@deloitte.com



Edna Yap
Executive Director
Deloitte Risk Advisory
edyap@deloitte.com



Manoj Wadhwa
Director
Deloitte Risk Advisory
mwadhwa@deloitte.com



Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

About Deloitte Singapore

In Singapore, risk advisory services are provided by Deloitte & Touche Enterprise Risk Services Pte. Ltd. and other services (where applicable) may be carried out by its subsidiaries and/or affiliates.

Deloitte & Touche Enterprise Risk Services Pte. Ltd. (Unique entity number: 197800820D) is a company registered with the Accounting and Corporate Regulatory Authority of Singapore.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.