Managed compliance as code service

A plug-and-play centralised compliance and code platform for both single and multi cloud environments leveraging Prisma Cloud by Palo Alto Networks

What is compliance as code (CaC)?

CaC is the organisational capability to automate the implementation, verification, remediation, monitoring and reporting of compliance status. This is an effective way to maintain governance over a complex cloud environment.

Common compliance monitoring technique in cloud:

- Implement configuration check before resources being built
- Customised based on compliance and regulatory requirement
- Set the alert and notify operation team to remediate the issue

PwC's plug-and-play managed compliance as code service

Leveraging **Prisma Cloud by Palo Alto Network**, PwC's managed compliance as code service helps businesses to convert company, organisation or regulatory cloud compliance policies into codes, ensuring your cloud architecture and operations meet various requirements from stakeholders such as end users, security, risk, compliance, and more.

Integration is simple. What we need is a read-only access key from your cloud platform for integration.

Identify & customise

- Define regulatory and organisational requirements
- Assess the cloud infrastructure
- Customise cloud compliance rules configuration

Integrate

- Develop managed CaC on Prisma Cloud
- Integration with your cloud environments

24x7 monitoring

- Review and continuous monitoring
- Remediation and reporting
- Managed rules with latest updates on all compliance requirements

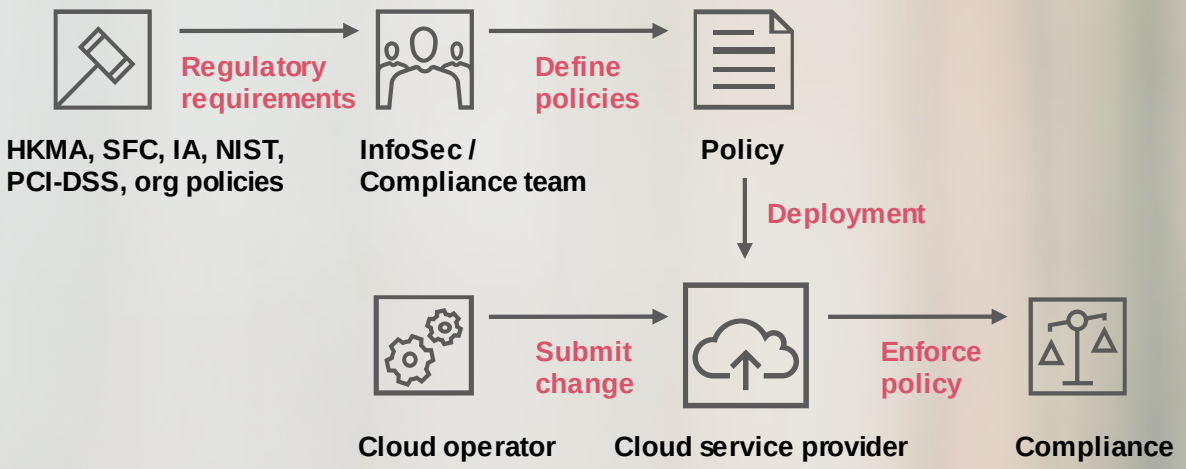
Start your one-month proof-of-concept now

To help you understand the benefits our Managed CaC Service, we're offering a free proof-of-concept for one month. Scan the QR code to fill up the form, and one of our product experts will get in touch with you.

pwc

paloalto NETWORKS | PRISMA BY PALO ALTO NETWORKS

Compliance as code development lifecycle



Define	Build	Deploy	Monitor
Mapping between regulatory requirements with cloud platform configurations based on **PwC managed CaC template**	Develop compliance as code related to compliance requirement across the whole organisation	Implementation of compliance as code to verify compliance status of resources created in the cloud environment	Review and regular monitoring for any remediation, and update compliance rules to latest requirements

Bringing compliance to cloud – Example of CaC from mapping between HKMA TM-G-1 and Cloud Configuration Rules

01

Identify HKMA requirements:
TM-G-1 (General Principles for Technology Risk Management)
3.2 Authentication and access control
Access to the information and application systems should be restricted by an adequate authentication mechanism associated with access control rules.

02

Map to cloud configuration rule name (as examples):

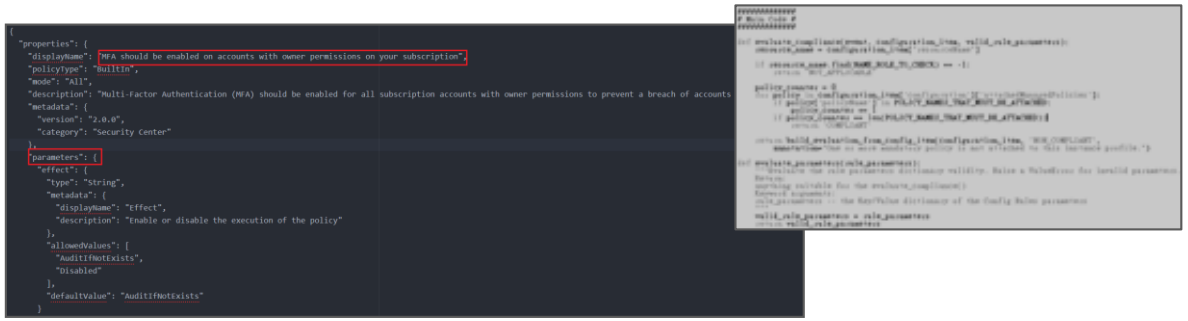
Rule Name	Description
ROOT_ACCOUNT_MFA_ENABLED	Checks whether the root user of your account requires multi-factor authentication for console sign-in
IAM_USER_NO_POLICY_FULL_STAR	Check whether IAM Users have an IAM policy with all permission enabled
INSTANCE_PROFILE_HAVE_DEFINED_POLICIES	Checks that the correct policies are attached to particular compute instance profiles.
MFA_OWNER_PERMISSION	MFA should be enabled on accounts with owner permissions on your subscriptions

03

Develop compliance as a code script with the configuration rules.

04

Deploy scripts to cloud environment
Example rules: ‘instance-profile-have-defined-policies’ and ‘MFA-owner-permission’



Get in touch with us

South

Kenneth Wong
Cybersecurity & Privacy Leader, Risk Assurance, Mainland China/Hong Kong
kenneth.ks.wong@hk.pwc.com

Kok Tin Gan
Partner
kok.t.gan@hk.pwc.com

Felix Kan
Partner
felix.py.kan@hk.pwc.com

Danny Weng
Partner
danny.weng@cn.pwc.com

Central

Chun Yin Cheung
Partner
chun.yin.cheung@cn.pwc.com

Miles Huang
Partner
miles.huang@cn.pwc.com

Sean Pan
Director
sean.pan@cn.pwc.com

North

Lisa Li
Partner
lisa.ra.li@cn.pwc.com

Ryan Yao
Partner
ryan.h.yao@cn.pwc.com

About PwC's DarkLab

As more people, products and services become connected, the need to proactively address cybersecurity and privacy risks has never been more urgent. A nuanced understanding of motivations and tactics of both internal and external cyber adversaries is vital to anticipate and detect cyber threats.

PwC's DarkLab was designed and built to simulate real life hacking scenarios and help mitigate the most sophisticated cyber attacks. Our 280+ cyber security professionals are equipped with a range of skills and expertise, in 24x7 security monitoring, cyber-attack simulation, incident response handling, purple teaming, etc., who are ready to help companies build a tailored, next generation cybersecurity defence.
Visit us at www.pwchk.com