GRC+ SERVICE SHEET · NOVEMBER 2026

Cloud Security Assessment

Most cloud incidents come from configuration, not from the cloud provider. We review who can do what in your AWS, Azure or Google Cloud environment, verify what is really exposed to the internet and check your setup against CIS Benchmarks.

SERVICE
Advisory service

What It Is

A review of your AWS, Azure or Google Cloud environment: identity and access, what is exposed to the internet and how services are configured, against CIS Benchmarks.

WHY IT MATTERS

Fast change, wide permissions

Teams move quickly, and wide roles and public storage are easy to create and easy to forget.
- Over-broad roles
- Public storage and snapshots
- Logging not switched on everywhere

THE OUTCOME

A cloud setup you can explain

You know the real risks across accounts, and the changes that reduce them most.
- Fixes by service
- Priorities by exposure
- Evidence for customers and auditors

What We Test

Identity and access	Roles and policies that give more than they should, and paths to higher privileges.
Attack surface	Storage, compute, databases and APIs that answer from the internet, each one verified.
Configuration	Encryption, logging, network rules and account settings across your services.
Detection	Whether the logs you need exist and are protected.
Container Security	A test of your container platform from outside and from inside a compromised pod, with a hardening review against the CIS Kubernetes Benchmark.

What You Receive

The cloud security report PDF	Each finding with its evidence, risk, the steps to reproduce it and a fix.
A management summary In the report	What was tested, the main risks and the decisions needed, without the technical detail.
A walkthrough Video call	A session with your team to go through the findings and answer questions.
A retest on request Updated report	We check your fixes and update the report, so you can show the result to auditors and customers.

From Scope to Verified Fixes

1	**Scoping** Targets, people, test windows and exclusions, with written authorisation and rules of engagement.
2	**Access review** Read-only access set up; identity and access policies reviewed.
3	**Attack surface** Public services identified and verified; configuration compared with the benchmark.
4	**Report** Findings with evidence, risk and a fix, a management summary and a walkthrough with your team.
5	**Retest** We check your fixes and update the report.

A guide, not a fixed promise: the length of each phase depends on your scope.

Regulations That Ask for It

CCC (Saudi Arabia)	A review of identity, exposure and configuration in your AWS, Azure or Google Cloud environment.
MTCS SS 584	
Digital Infra Act (Singapore)	A review of your AWS, Azure or Google Cloud environment: identity and access, what is exposed to the internet and how services are configured, against CIS Benchmarks.
CADA	
1054/2018 (Finland)	
ESMA65-294529287-4737	A review of the security of your cloud services against the information security requirements of Guideline 4.
ECB Cloud Guide	A review of your cloud set-up against the ECB expectations on data security, access management and resilience.
SFC 19EC59 (Hong Kong)	A review of your cloud and external data storage set-up against the SFC's access, audit trail and encryption key requirements.
MAS Outsourcing (Singapore)	A review of your cloud arrangements against Annex 5 of the guidelines.
CBUAE Outsourcing (UAE)	A review of cloud arrangements against the regulation's data location and access requirements.
QCB Cloud Regulation (Qatar)	A cloud security assessment and test plan matched to the QCB regulation's service-model test table.
MNB 2/2025	A review of your cloud set-up against the security controls in Section IV of the recommendation.

Why Organisations Choose GRC+

Independent of your suppliers	We test what you have. We take no margin on a product we assess or recommend.
Findings tied to your requirements	Our team also works on NIS2, DORA, ISO 27001, PCI DSS and Swift CSP, so results can serve your audits too.
Risk rated for your business	We rate each finding by what it could cost you, not only by a scanner's score.
Written rules of engagement first	Scope, limits and contacts are agreed in writing before any test starts.

Questions Buyers Ask

Do you need permission from the cloud provider to test?

AWS, Microsoft and Google allow customers to test many of their own services without asking first, under their published policies. We check the current policy against your scope before we start.

What do you need to test our cluster?

A test namespace with a pod we can use as a starting point, read access for the benchmark and the design review, and your network and platform documents.

What access do you need to our cloud environment?

A read-only role in your AWS accounts, Azure subscriptions or Google Cloud projects, which you create for the assessment and remove afterwards. We do not change anything in your environment.

Do you test production clusters?

We can, with agreed limits. A staging cluster built the same way is often a better place to try attack paths, with a read-only check of production.

Talk to Us

Thirty minutes with a principal consultant on what applies to you and what to do first.
Book a 30-Minute Call · sales@grc.plus · grc.plus/service/cloud-security-assessment

