



Cloud Security Posture & Governance

Identify weaknesses, mitigate misconfigurations, and secure your cloud workloads across IaaS, PaaS, and SaaS environments.





Cloud Security >

Provide complete visibility and security assurance over cloud workloads, identities, and infrastructure to your stakeholders and enterprise clients.

As organizations adopt cloud technologies at a rapid pace, the standard "Lift and Shift" model of cloud migration inherently transfers legacy application vulnerabilities directly into modern environments—compounded by cloud-native misconfigurations.

More often than not, critical security considerations are overlooked during fast-tracked deployments just to get applications operational. Furthermore, a widespread misconception persists that cloud security is entirely the responsibility of the Cloud Service Provider (CSP).

While CSPs secure the underlying physical infrastructure, security in the cloud remains a Shared Responsibility. Whether operating under Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS), your organization remains strictly accountable for data protection, access governance, and configuration hardening.

Scenarios >

Let's look at some of the practical scenarios to understand the challenges better:

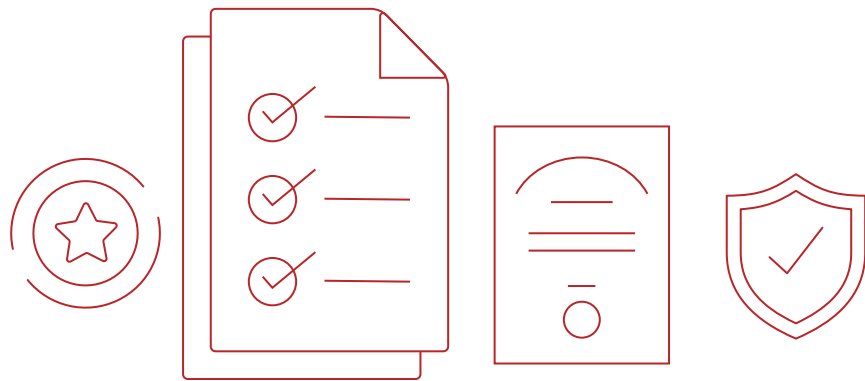
Scenario 1: SaaS & Software Service Providers

A mid-sized software company hosting financial reporting tools on AWS/GCP needs to give continuous assurance to enterprise clients that customer tenant data is completely isolated, API endpoints are secured, and underlying cloud infrastructure meets stringent information security standards.

Scenario 2: Enterprise Cloud Migration & Compliance

An enterprise collecting customer PII and sensitive operational data migrates core databases to PaaS/IaaS. They struggle with complex IAM over-privileging, unencrypted storage buckets, and unmonitored API routes, exposing the company to regulatory fines under DPDP, ISO 27001, and SOC 2 frameworks.





Solution >

The KGS Consulting Cloud Security Posture & Governance Framework provides an end-to-end evaluation of your cloud environment across AWS, Azure, and Google Cloud Platform (GCP).

Our certified cloud security architects conduct deep configuration audits, identity access reviews, and perimeter defense validations against industry benchmarks such as CIS (Center for Internet Security), NIST SP 800-53, and ISO 27017.

Cloud Security Pointers is organized by core operational domains, designed for security audits, architecture reviews, and risk assessments:

1. Identity & Access Management (IAM)
2. Data Protection & Cryptography
3. Network Architecture & Perimeter Security
4. Vulnerability Management & DevSecOps
5. Logging, Monitoring & SIEM
6. Shared Responsibility & Governance

Benefits >

- ✓ **Demonstrate Trust & Transparency:** Provide verifiable proof of cloud security posture to clients and enterprise buyers, creating a distinct competitive advantage during sales cycles.
- ✓ **Proactive Risk & Breach Prevention:** Identify and remediate cloud misconfigurations, publicly exposed assets, and broken access controls before they lead to security incidents or severe regulatory penalties.
- ✓ **Zero Trust Identity Governance:** Eliminate identity over-privileging and static API keys by enforcing least-privilege IAM policies and short-lived credentials.
- ✓ **Regulatory & Standard Alignment:** Seamlessly align your multi-cloud architecture with DPDP, ISO 27001, SOC 2, and RBI cyber security mandates.



KGS Consulting supports you through the full lifecycle of the Cloud Security & Compliance journey:

Readiness & Assessment

Assess current 'as-is' status across AWS, Azure, and GCP. Conduct automated scanning and manual configuration reviews against CIS Benchmarks and security baselines.

Implementation Support

Provide hands-on remediation engineering to lock down IAM roles, enforce encryption at rest/in transit, implement network micro-segmentation, and embed DevSecOps pipelines.

Attestation & Internal Audit

Validate implemented technical controls, perform revalidation testing, and issue official Cloud Security Posture Compliance & Assessment Reports.

Maintenance & Monitoring

Cloud security is an evolving journey. We provide ongoing Cloud Security Posture Management (CSPM), real-time threat monitoring advisory, and periodic baseline re-assessments.

Our Cloud Security Assessment provides complete visibility into your cloud architecture to identify hidden vulnerabilities, enforce least-privilege governance, and remediate critical misconfigurations before they lead to operational disruption or data breaches.



Thank you!

Stay Connected

Siddhi Dalvi

PHONE

+91 9146639547

EMAIL

siddhi.dalvi@consultkgs.com