Cloud Security Maturity Model

Version 2.0

IANS | Securosis | CSA cloud security alliance®

		LEVEL 1 Initial	LEVEL 2 Repeatable	LEVEL 3 Defined	LEVEL 4 Capable	LEVEL 5 Efficient
Foundational Domain Core, critical categories to ensure availability of a secure baseline.	**Governance** Overall governance of cloud providers, deployments, applications and general usage.	No formal cloud governance. Either cloud is not allowed, not officially supported or teams completely self manage cloud usage.	Main cloud providers are approved. Some policies in development that often mimic non-cloud (on-prem) standards. No cloud-specific org structure.	Cloud team, CCoE or equivalent in place to guide usage. Initial policies in use. Basic use of standards and benchmarks (e.g., CIS) for configuration baselines. Partial control objectives established for at least one provider. Cloud registry in place.	Central cloud team has SMEs for current providers and responsibility and authority to set rules/baselines. Cloud security control objectives in use. Control specifications for primary cloud provider are defined/enforced.	Governance is managed using automated tooling (e.g., database, IaC). Defined process to update control objectives/specifications as cloud providers add/modify services.
	Organization Management Core cloud deployment security and multi-deployment/provider architectures to control blast radius and ensure baseline security.	Single or unconnected deployments with inconsistent core security.	Checklist for core deployment security on primary cloud platform. Most accounts associated with organization but manually managed.	Deployments centrally managed with consistent manual provisioning of core security. Security checklists for each current cloud provider. Initial use of CSPM or similar for security visibility.	Deployments provisioned via IaC including most core security controls. Multiple deployments in a provider used to control blast radius and organized hierarchically. CSP preventative policies (guardrails) in use.	Deployments used extensively to control blast radius. Deployment security provisioned through automation aligned with landing zone/account factory. Automated deprovisioning also in use.
	IAM Managing users, authentication and authorization to the cloud provider and resources within the cloud. Also refers to managing IAM within the provider.	Identities managed within individual cloud accounts. No federation. MFA inconsistent.	Initial federation, likely using a federated identity broker or similar. Extensive use of cloud-side entities. MFA mostly consistent for console but not for command line or API.	Federation consistent through broker or similar. Initial secrets management use for static credentials for command line and code. MFA mostly consistent across console, command line and APIs. Manual configuration of IAM policies within accounts.	Complete federation for all cloud accounts. MFA consistent. Initial use of automated provisioning of IAM. Secrets management consistent. Initial use of advanced conditional authorization where needed and supported to enforce IAM perimeter.	Fully automated provisioning of IAM. Extensive use of advanced conditional authorizations for robust IAM perimeter. Console, command line tools and API access integrated into privileged user and secrets management.
	Security Monitoring Monitoring and logging of both cloud administrative activity (the "management plane") and assets within the cloud (networks, workloads, applications, data).	No monitoring/alerting on telemetry gathered by the cloud provider.	Multi-account monitoring/alerting with logs aggregated across some accounts.	Management plane logs and some ad hoc service/workload logs collected across all relevant deployments. Initial alerts/threat detectors for security deviations, but inconsistently in place.	Comprehensive security telemetry collected for the management plane, services and workloads. Cloud-native threat detectors in place but not necessarily consistent across providers.	Consistent telemetry collected across all in-use cloud providers. Comprehensive cloud-native threat detectors with enrichment. Alerts routed to the team that owns/manages the deployment.
Structural Domain Categories to protect the building blocks of your cloud environment.	**Network Security** Security of the virtual networks in the cloud, and the connections to/from the cloud.	Cloud network architectures replicating on-prem patterns. Network security ad hoc using overly open controls. Utilizes virtual appliances from existing network security vendor instead of equivalent cloud-native capabilities.	Networks manually built to defined cloud standards. Applications forced to fit supported networking models. Initial use of cloud-native security controls but often overlapping with legacy controls.	Initial use of cloud-native architectures to isolate/segment cloud resources and break network attack paths. Initial use of network templates and transit networks. Uses a combination of cloud-native and hybrid networking approaches depending on the application.	Extensive use of cloud-native network architectures and PaaS. Initial adoption of the Minimum Viable Network concept. Network security policies enforced with automated guardrails.	Networks designed to fit the application and enhance app security (Minimum Viable Network). Use cloud-native architectures and design patterns. Centralized and automated controls.
	Workload Security Securing the environment where code runs, including VMs/instances, containers and function as a service (FaaS: serverless).	Most workloads are long-running VMs using existing datacenter-centric security controls ported directly to cloud.	Generally reliant on traditional datacenter management tools. Use of automated configuration management to standardize building of infrastructure. No FaaS or container-specific security.	Mostly cloud-native tools in use. Initial use of Immutable infrastructure. Initial integration of security configurations and tools into image creation/ pipelines. Initial security controls implemented on containers.	Immutable infrastructure is the recommended pattern, where possible. Security testing integrated into image pipelines. Only cloud-native tools in use. Baseline container security in place. FaaS security ad hoc, but available.	Immutable infrastructure is the standard (where possible) with multiple daily deployments. Code assessment and real-time defenses integrated using FaaS.
	Application Security Full stack application security. This includes testing and protection of pipelines, workloads, architectures, etc.	Traditional application security testing (*AST) and defenses (e.g., legacy WAF).	Mostly traditional testing. Ad hoc assessment of pipeline security. Initial use of cloud-provider's AppSec tools (WAF/DDoS). Serverless app security is a gap.	Some cloud-specific testing. Pipelines manually secured. Consistent WAF/DDoS for internet-facing apps. Serverless hardening within AppSec scope. Initial security testing in CI/CD.	Stack testing partially automated. Consistent pipeline security utilized. Extensive security testing in CI/CD pipelines. AppSec guardrails implemented.	Stack testing automated across all workload models and consistently implemented in CI/CD pipelines. Cloud-centric red team to test cloud-based applications.
	Data Security Encryption and access control of cloud data.	Basic access controls, usually improperly configured.	"Checkbox" data security. Encryption turned on using default keys. Manual encryption and key management. Manually configured access controls.	Initial use of customer managed keys. Simple automation for most. Policy-based access controls and encryption. Data access logs consistently collected in production deployments.	Extensive use of customer managed keys. All critical data encrypted. Some automation using data guardrails, but mostly manual. Initial content-based access controls and encryption.	Minimal use of default keys. Data lifecycles/backups automated for resiliency. Encryption specifications built into deployment pipelines. Deployments consistently assessed for unapproved data.
Procedural Domain Categories to highlight the processes needed to protect your cloud (and keep it protected).	**Risk Assessment and Provider Management** There are three aspects of risk assessment: 1. Provider selection (choosing providers) 2. Ongoing provider re-assessment and management 3. Risk assessment of specific projects and programs.	Use existing risk assessment models and provider selection process.	Provider selection driven by business unit, but security assesses the provider and can trigger an escalation. Security inconsistently engaged in early project risk assessments (e.g., architecture risk).	Basic security standards for cloud providers of different service models (IaaS, PaaS, SaaS) in use. Initial provider registry in use, showing approvals by data classification/risk/compliance.	Security engaged with process for evaluating providers and deployments. Existing provider and deployment risk profiles re-assessed either annually, or after major change. Risk registry includes approvals at the service level.	Security-driven risk assessment for new projects and cloud migrations, with formal templating and remediation plans. Existing providers and projects are evaluated continuously for updated risk profiles.
	Resilience Ensuring resilient use of cloud that meets an organization's business requirements for availability and recovery.	No formal resiliency for cloud deployments.	Some basic data backup/lifecycles. Some use of autoscaling/automation for workloads. Largely single provider/region deployments.	Moderate use of autoscaling/automation for workload resiliency, where possible. Initial use of multi-region resiliency. Some deployments use IaC for additional resiliency.	Most deployments provisioned with IaC. Some use of multi-region and multi-account resiliency. Deployments use assessable resiliency control specifications. Data-plane resilient to larger CSP failures.	All production deployments provisioned with IaC. IaC repositories implement resiliency. Automated failovers and redeployments in use. Chaos engineering in place.
	Compliance and Audit Meeting regulatory compliance requirements and mandates.	No reporting or compliance actions taken for cloud-specific resources.	No cloud-specific standards. Ad hoc assessment and remediation of deficiencies on cloud-based resources.	Cloud provider and service (SaaS or PaaS) approved list. Scheduled assessments of cloud providers. Manual reporting of cloud controls versus standards.	Continuous assessment of in-scope resources using automated guardrails, manual remediation of deficiencies. Reporting is partially automated.	Continuous assessment and automatic remediation of deficiencies using cloud automation. Reporting fully automated across all applicable standards with dashboarding.
	Incident Response Cloud-specific incident response processes, including compromise of the cloud console/management plane.	No cloud-specific response, uses existing IR playbooks (if they exist).	Manual IR response to cloud events. Inconsistent data collection and escalation.	Consistent manual response with rudimentary tooling.	Trained responders using cloud-specific tooling and refined processes. Some platform-based automation (quarantine asset, take snapshot, etc.). Cloud-native detection engineering.	Fully automated and orchestrated IR workflow backed by a cloud IR team and response platform. Testing using a cloud-focused red team and incident simulation.

DevSecOps

Threat and Vulnerability Management