Cross-Cloud Control Alignment

AI Infrastructure Security Playbooks — With ETSI EN 304 223 Mapping

This table maps cloud-neutral security invariants to specific AWS, Azure, and GCP implementations across all four assurance zones. Controls are aligned to the playbook's eight-tier risk gradient (L1–L8) and mapped to ETSI EN 304 223 provisions.

Zone	Security Invariant	AWS	Azure	GCP	ETSI EN 304 223
FOUNDATIONAL (L1–L2)					
	Identity & Access Control	IAM + MFA + Identity Center + SCPs	Entra ID + Conditional Access + PIM	Cloud Identity + 2SV + Context-Aware Access + Org Policies	P4, P5, P6
	Encryption & Key Management	SSE-KMS (S3/EBS) + CMK	Storage Encryption + Key Vault CMK	CMEK via Cloud KMS + Org Policy enforcement	P6
	Secrets Management	Secrets Manager (auto-rotation)	Azure Key Vault (auto-rotation)	Secret Manager (auto-rotation)	P5, P6
	CSPM Baseline Posture	Security Hub + GuardDuty + Inspector	Defender for Cloud + Sentinel	SCC Premium + Chronicle	P11, P12
	Data Classification & DLP	Macie + Lake Formation	Microsoft Purview + DLP policies	Cloud DLP + Data Catalog	P5, P8, P13
	CASB & Shadow AI Controls	Third-party CASB (Netskope, etc.)	Defender for Cloud Apps	Third-party CASB / Workspace controls	P3, P5, P8
	Credential Hygiene	IAM roles (no long-lived keys)	Managed Identity (no client secrets)	Workload Identity (org policy: disable SA key creation)	P4, P5
STANDARD (L3–L4)					
	Private Service Isolation	VPC Endpoints + PrivateLink + deny-all egress	Private Endpoints + VNet integration	Private Service Connect + VPC Service Controls	P2, P6
	API Gateway & Validation	API Gateway + WAF rate limiting + request validation models	APIM + WAF + request schema validation	Apigee + Cloud Armor + API schema validation	P2, P6, P11
	Circuit Breakers & Throttling	Step Functions Choice states + API Gateway throttling	Logic Apps + APIM rate limiting	Workflows + Apigee spike arrest	P2, P11
	Egress Enforcement	Network Firewall + VPC endpoint-only (aws:sourceVpc)	Azure Firewall + UDR egress lock	Cloud NAT + Firewall Rules + VPC SC	P2, P6
ADVANCED (L5–L6)					
	Per-Agent Identity Isolation	Dedicated IAM role per agent + permission boundaries	Unique Managed Identity per agent + deny assignments	Unique service account per agent + IAM Deny policies	P4, P5, P6
	Identity Self-Mutation Prevention	IAM deny policies (iam:Create/Attach/PutRolePolicy, sts:AssumeRole to self)	Entra deny assignments; agents cannot modify own role assignments	IAM Deny policies (modify bindings, create SA, generate keys)	P4, P5
	SA Key / Secret Prohibition	IAM roles only; no long-lived access keys for agents	Managed Identity only; client secrets prohibited unless unavoidable	Workload Identity only; iam.disableServiceAccountKeyCreation org policy	P4, P5, P6

Zone	Security Invariant	AWS	Azure	GCP	ETSI EN 304 223
	Automated Kill Switch	IAM deny + SG modify + Network Firewall + SNS; note: STS creds invalidated by removing permissions, not direct revocation	Entra WI disable + NSG modify + Firewall; coordinated containment runbook, not a single feature	IAM deny + Firewall automation + WI revoke; coordinated containment runbook	P2, P4, P11
	Model Registry & Integrity	SageMaker Registry + SHA-256 hash; compare approved vs deployed; block on mismatch	Azure ML Registry + SHA-256 hash; compare approved vs deployed; block on mismatch	Vertex AI Registry + SHA-256 hash; compare approved vs deployed; block on mismatch	P7, P9
	Training Environment Isolation	VPC-only SageMaker + EnableNetworkIsolation=true	Azure ML Managed VNet + workspace isolation	Vertex AI VPC Peering + CMEK + egress controls	P2, P6, P13
	Signed Images & SBOM	ECR scanning + Inspector SBOM + AWS Signer	ACR + Content Trust + Defender scanning	Artifact Registry + Binary Authorization + Container Analysis	P7
	Periodic Model Integrity Verification	Recompute deployed hash vs Registry (daily min); automate via EventBridge + Lambda	Recompute deployed hash vs Registry (daily min); automate via Azure Automation / Logic Apps	Recompute deployed hash vs Registry (daily min); automate via Cloud Scheduler + Cloud Functions	P7, P9, P12
HIGH ASSURANCE (L7–L8)					
	mTLS Between Agents	App Mesh + ACM Private CA; or Envoy sidecars (mechanism may vary)	AKS Service Mesh (Istio/Linkerd/OSM); or equivalent mesh	Anthos Service Mesh; or Envoy/Istio-compatible sidecars (mechanism may vary)	P2, P6
	Agent Certificate Lifecycle	ACM Private CA; certs bound to per-agent identity; <24h lifetime; automated rotation	AKS mesh certs bound to pod identity; <24h lifetime; shared certs prohibited	ASM certs bound to Workload Identity; <24h lifetime; automated rotation	P6
	Capability-Scoped Identity Tokens	Signed short-lived JWT; audience-bound, action-scoped, minute TTL, cryptographically validated	Entra token with audience/scope restrictions; short-lived	IAM conditions + signed tokens; audience-bound, short TTL	P4, P5, P6
	Model Extraction Detection	API Gateway + WAF logs + SageMaker Data Capture + CloudWatch anomaly detection	APIM + Sentinel analytics + Azure Monitor anomaly	Apigee + Cloud Monitoring + Cloud Logging anomaly	P11, P12
	Workload Policy Enforcement	EKS PSA (restricted) + OPA Gatekeeper / Kyverno admission controllers	AKS Pod Security + Azure Policy / Gatekeeper	GKE PSA (restricted) + OPA Gatekeeper / Kyverno	P2, P4, P7
	Cascade Detection & Correlation	CloudWatch composite alarms + Detective cross-account correlation	Sentinel cross-workspace correlation + Defender alerts	SCC custom findings + Chronicle cross-namespace correlation	P11, P12
CROSS-CLOUD SECURITY INVARIANT: *Agents must never be permitted to modify their own identity bindings, access policies, or trust relationships under any circumstance.*					

Clarifications:

Data governance and CASB controls are not cloud-exclusive. Enterprise tools such as Microsoft Purview, Defender for Cloud Apps, Netskope, BigID, Collibra, and others can operate across AWS, Azure, and GCP environments.

mTLS implementation may vary. The requirement is cryptographic peer authentication and encrypted east-west traffic. App Mesh, Anthos Service Mesh, and AKS service mesh are the primary implementation options; Envoy sidecars or equivalent are acceptable alternatives.

Kill switches are containment runbooks, not single features. Containment requires coordinated identity revocation, network isolation, and workload quarantine. Network containment alone is insufficient.

ETSI provision references. P2 = Network Security, P3 = Governance, P4 = Access Control, P5 = Identity & Authentication, P6 = Cryptographic Controls, P7 = Supply Chain, P8 = Data Protection, P9 = Integrity, P11 = Monitoring, P12 = Logging & Audit, P13 = Data Governance.

https://deepcyber.ai