anoBytes | TECHNOLOGY SOLUTIONS

Cloud landing zone and account baseline across AWS, Azure, GCP, and OCI

Sixteen foundational controls to establish before deploying workloads in the cloud. Covers account structure, identity, guardrails, logging, networking, encryption, backup and disaster recovery, operations, and automation, with the corresponding services for AWS, Azure, GCP, and OCI.

LANDING ZONE · ACCOUNT BASELINE · SECURITY · MULTI-CLOUD · CHECKLIST

16 foundations
the baseline every new resource inherits

4 cloud providers
AWS · Azure · GCP · OCI, mapped to CIS

A landing zone is the secure foundation you set up before you deploy or build: the account structure, identity, guardrails, logging, network, and encryption that every resource then inherits. Adding those later, once workloads are live, is slow and error-prone. This checklist covers sixteen foundations that apply across all four major clouds, the service to use for each on AWS, Azure, GCP, and OCI, and the corresponding CIS Foundations Benchmark controls. Work the domains roughly in order, since the later ones depend on the early ones. The last two, landing zone as code and account provisioning, describe how you deliver everything above them, so read those early even though you finish them last. It is a starting baseline; the full per-cloud benchmark and your provider's own landing-zone guidance go deeper.

START HERE Terms and foundations to build on

The isolation unit has a different name on each cloud

AWS isolates workloads by **account**, Azure by **subscription** (inside a management-group tree), GCP by **project**, and OCI by **compartment**. Read "account" in the checklist as the isolation unit for your cloud.

Each cloud ships a foundation you can build on

Use each cloud's own accelerator as your starting point. **AWS:** Control Tower and the Security Reference Architecture, with the Startup Security Baseline as a single-account starting point for the earliest stage. **Azure:** Azure landing zones in the Cloud Adoption Framework, deployed with the ALZ Accelerator. **GCP:** the enterprise foundations blueprint. **OCI:** the Core Landing Zone.

The CIS Foundations column shows anchor controls

We map to the CIS Foundations Benchmarks because they are the consensus security baseline for each cloud's account and tenant configuration, which is exactly the landing-zone scope. Providers also surface the CIS standard in their own posture tooling (AWS Security Hub CSPM, Microsoft Defender for Cloud, Google Security Command Center). That makes them an independent, auditable reference alongside each vendor's own landing-zone guidance. The entries are benchmark section numbers, so `6.3` in the AWS column means section 6.3 of the AWS benchmark. Each row cites representative controls; the benchmarks hold more per area.

Check the benchmark version before you match a number

The citations here follow AWS v7.0.0, Azure v6.0.0, GCP Foundation v5.0.0, and OCI v3.1.1. Section numbers move between versions, and the version your posture tool ships is often older: AWS Security Hub CSPM offers v5.0.0. Match on the control title rather than the number alone. Where a benchmark has no matching control but the vendor documents the practice, the cell reads `n/a` with that source in parentheses. Cost, landing zone as code, and account provisioning sit outside these benchmarks, so those rows read `n/a` and follow the vendor guidance. Backup and tagging are covered only in part. Some of that ground sits in a sibling CIS benchmark: Azure Backup, for one, is in the CIS Azure Storage Services Benchmark.

Scale it to your size

The structure matters more than the count. A small team can start with three accounts (management, security and logging, and workload) and split further as it grows. It can defer the paid detection tiers while the free posture checks and audit logging stay on. On AWS, Config bills from the start and Security Hub CSPM once its 30-day free trial ends. The foundations to do first are the ones that are painful to retrofit: the hierarchy, root and break-glass protection, centralized identity with MFA, org-wide audit logging, and the guardrails. Everything after those can follow in stages.

ORG Organization and account structure

Bring the whole footprint under one organization or tenancy. Build a hierarchy so policy is inherited, separate production from non-production, and stand up dedicated security, log-archive, and shared-services containers. Keep the top management or payer account free of workloads.

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**AWS**	AWS Organizations with all features on, organizational units by environment and sensitivity, dedicated accounts for Log Archive, Security Tooling, Network, and Shared Services, and no workloads in the management account.	2.1.3, 2.1.4
☐	**Azure**	One Microsoft Entra tenant with a prefixed intermediate root management group over the hierarchy (Platform, Landing Zones, Sandboxes, Decommissioned), a default management group so new subscriptions never land in the Tenant Root Group, and platform subscriptions for management, security, connectivity, and identity. Separate environments at the subscription level, and confirm subscriptions leaving and entering the tenant are set to Allow no users, the platform default since May 1, 2026. CIS v6.0.0 predates that change, so it calls the setting Permit no one and still records the old Allow everyone default.	5.6
☐	**GCP**	One Organization resource with folders by environment and sensitivity, dedicated projects for logging, security, KMS, and billing export, and Shared VPC host projects.	1.1.3
☐	**OCI**	One tenancy with a compartment hierarchy (network, security, app, and database), each compartment with its own admin group, a dedicated security compartment, and separate compartment subtrees for production and non-production. Keep workload resources out of the root compartment, where budgets and tenancy-scope event rules must live and where tag defaults belong so every compartment inherits them. Where the footprint spans more than one tenancy, link them with Organization Management for subscription mapping, central cost reporting, and governance rules, which cover allowed regions, quotas, and tags only. Each tenancy keeps its own IAM users, policies, and administrator, so apply this baseline separately in every one, and keep the parent tenancy free of workloads.	6.1, 6.2

ROOT Root and break-glass access

Secure the root or global-admin identity with hardware or phishing-resistant MFA, remove long-lived root credentials, reserve and limit the top admin role, and alert on every use of it. Register the contacts your provider will use to reach you.

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**AWS**	Enable hardware or FIDO MFA on the management account root user, remove its access keys, and stop using root for daily tasks. Then turn on centralized root access management with both root credentials management and privileged root actions, since without the second nobody can recover a member account root user afterwards. Only then delete root credentials in member accounts, where root MFA no longer applies. Alert on any root sign-in, and register account and security contacts.	2.1.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 5.3
☐	**Azure**	Create two or more cloud-only emergency-access accounts with FIDO2 or certificate MFA, exclude them from any Conditional Access policy that blocks or restricts sign-in, and alert on every sign-in. Keep Global Administrators to fewer than five and out of daily use, and set a Defender for Cloud security contact email with high-severity alert notifications on every subscription.	5.3.1, 8.1.13, 8.1.14
☐	**GCP**	Hold super-admin accounts outside the SSO path, enforce security keys, keep super admin out of day-to-day administration, and configure Essential Contacts. Turn on Google Workspace and Cloud Identity data sharing first, or the Workspace audit logs never reach Cloud Audit Logs. Super-admin sign-in arrives in the Login audit log rather than the Admin one. Then route those org-level entries into a log bucket in the security project (set up in the logging domain below) and alert on super-admin sign-in with a bucket-scoped log-based metric, since log-based alerting cannot read organization-scoped logs directly.	1.1.1, 1.1.2, 1.4, 1.17, 2.2
☐	**OCI**	Reserve the built-in Administrators group for break-glass, block IAM administrators from changing its membership, remove API keys from tenancy administrators, require MFA with a FIDO passkey or hardware key, and alert on local (non-federated) interactive sign-in, which is how break-glass use of the group shows up. Keep a valid, monitored email address on every local account, and subscribe a topic to Oracle's announcements. Change the break-glass password on a schedule, since the 365-day expiry is counted from when the password was last set.	1.2, 1.3, 1.7, 1.12, 1.13, 4.18

Where they differ: The top admin identity behaves differently on each cloud: the AWS per-account root user sits outside IAM, the Azure Global Administrator does not control resources by default, GCP super admins keep a Google-password sign-in path outside SSO, and OCI reserves the Administrators group.

IDENTITY Centralized identity and MFA

Use one central identity provider with federation and single sign-on. Enforce MFA everywhere, and prefer phishing-resistant methods for administrators. Give applications a managed identity instead of a long-lived secret.

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**AWS**	Federate IAM Identity Center to your corporate identity provider (SAML for sign-in plus SCIM for automatic user provisioning) with permission sets. Require MFA, and prefer FIDO2 keys or passkeys for administrators. Avoid IAM users and static access keys, give EC2 workloads an IAM instance role rather than embedded keys, and enforce a password policy, MFA, and 90-day key rotation on any IAM user that remains.	2.8, 2.9, 2.10, 2.12, 2.16, 2.19

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**Azure**	Make Microsoft Entra ID the central identity provider, require MFA for every user and phishing-resistant MFA for admins, apply Conditional Access, and give applications managed identities or workload identity federation instead of long-lived client secrets.	`5.1.1, 5.1.3 (free tier only)`
☐	**GCP**	Federate Cloud Identity to your provider, use corporate login credentials, enforce 2-Step Verification for all non-service accounts and security keys for admin accounts, allow only Google-managed service account keys, and give workloads attached service accounts, using Workload Identity Federation for anything outside Google Cloud.	`1.2, 1.3, 1.4, 1.5`
☐	**OCI**	Federate the OCI IAM identity domain over SAML and extend MFA beyond administrators. Set the identity domain password policy to at least 14 characters with a numeric or special-character minimum of 1, 24 previous passwords remembered, and expiry within 365 days, which covers every local account left after federation, break-glass included. Use dynamic groups with instance or resource principals instead of static user API keys.	`1.4, 1.5, 1.6, 1.7, 1.8, 1.14`

Where they differ: Azure gates part of this baseline behind a paid identity edition. Conditional Access needs Microsoft Entra ID P1; on the free tier the equivalent is Entra security defaults and per-user MFA (CIS Azure 5.1.1 and 5.1.3), which CIS tells P1 and P2 tenants to bypass once Conditional Access is in use. Security defaults cannot be enabled alongside Conditional Access; per-user MFA can, so turn it off yourself once Conditional Access enforces MFA. Foundations v6.0.0 has no Conditional Access control of its own; those controls moved to the CIS Microsoft 365 Foundations Benchmark.

ACCESS Access management and least privilege

Grant access through roles and groups under the principle of least privilege, where an account gets the access it needs and no more, and cap what a delegated role can reach. Find and remove unused or over-broad access, and grant privileged access and host access just in time, with a record of each session.

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**AWS**	Assign permissions through groups and permission sets, cap delegated roles with permission boundaries, keep full "*:*" admin policies unattached, and disable credentials unused for 45 days. Enable an external access analyzer in every active region; external access findings are free, while the unused access analyzer is billed per role or user and one covers every region. Use Systems Manager Session Manager with session logging turned on for host access.	`2.11, 2.13, 2.14, 2.18`
☐	**Azure**	Use Azure RBAC under least privilege (roles to groups), Privileged Identity Management for time-bound elevation with approval, and periodic access reviews. Add Defender for Cloud just-in-time VM access (Defender for Servers Plan 2) and reach machines through Azure Bastion, so just-in-time acts on the network security group. Scope the just-in-time request to the AzureBastionSubnet range, since the default scopes it to the requester's own address and would not admit the Bastion session. The Premium Bastion SKU records the sessions. Microsoft documents it as unsupported where the inbound path is an Azure Firewall managed by a Firewall policy or by Azure Firewall Manager, so do not plan on opening admin ports through the hub firewall. Avoid custom subscription-admin roles.	`5.3.4, 5.3.7, 5.4`

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**GCP**	Bind predefined or custom roles to groups by job function, avoid the basic Owner, Editor, and Viewer roles, and keep service accounts free of admin privileges. Act on IAM role recommendations to remove unused permissions, which need a paid Security Command Center tier once you are off the basic roles. Set IAM deny policies at the org node as an upper limit that project-level grants cannot override, checking each permission against the published list of the ones deny policies support. Use Privileged Access Manager for time-bound elevation, with Identity-Aware Proxy and OS Login for host access, enabling Data Access audit logs for Identity-Aware Proxy so connections are recorded.	1.6, 3.12, 4.4
☐	**OCI**	Scope IAM policy statements to the smallest compartment and resource type, and create service-level admin groups, withholding delete on the resources each one manages. Disable credentials unused for 45 days, except the break-glass and service accounts CIS 1.16 exempts. Use IAM Deny statements as a permission boundary once the feature is enabled, and put a request.utc-timestamp condition on any elevated policy statement so the grant expires on its own. Use OCI Bastion for host access, cutting the session time-to-live well below the three-hour maximum OCI allows, with OCI Audit recording session creation and deletion (session content is not captured).	1.1, 1.2, 1.15, 1.16

Where they differ: Just-in-time elevation is where these clouds diverge most. Azure has Privileged Identity Management (Microsoft Entra ID P2 or Entra ID Governance) and GCP has Privileged Access Manager, AWS has no built-in equivalent, so use a partner integration or the AWS TEAM solution, and OCI has none either, so it falls back to a time-bounded policy condition. Access reviews are an Entra ID Governance feature; the capabilities already generally available under P2 still run on P2.

GUARDRAILS Preventive guardrails

Set org-wide, inherited controls that define what identities and resources may do. Block risky configurations when a resource is created or changed.

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**AWS**	Use Organizations service control policies (SCPs), resource control policies, and declarative policies (for example, requiring IMDSv2 for all new instance launches organization-wide), administered from a delegated admin account rather than the management account, plus Control Tower controls, which are enabled from the management account only. Restrict which regions can be used with an SCP or the organizational-unit-scoped Control Tower region-deny control, exempt global services, and test on one organizational unit before the root.	2.1.2, 2.1.5, 6.7
☐	**Azure**	Assign Azure Policy definitions and initiatives at the management-group scope (Deny and DeployIfNotExists), apply the Azure Landing Zone default policy assignments, and restrict allowed locations, types, and SKUs (resource sizes and tiers).	n/a (Azure Policy)
☐	**GCP**	Set Organization Policy constraints at the org node: skip default network creation, restrict resource locations, require OS Login, prevent public storage, enforce uniform bucket-level access, disable service account key creation, and restrict IAM grants to your own organization with the domain restriction constraint, which takes your Cloud Identity customer ID rather than a domain name. Deny all values on the external IP list constraint, which covers IPv4 only, and pair it with constraints/compute.disableVpcExternalIpv6 so no new VM gets a public address. Add VPC Service Controls perimeters, which restrict access to the Google Cloud APIs you place inside them, once you confirm each service you rely on can go in a perimeter.	1.1.4, 1.5, 3.1, 3.8, 4.9, 5.1, 5.2

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**OCI**	Enable Cloud Guard at the tenancy root with the Oracle-managed detector and responder recipes first, then bind sensitive compartments to a Security Zone recipe so non-compliant create and update operations are denied. Disable the legacy instance metadata endpoint, and enable IAM Deny policies (a permanent, tenancy-level opt-in) as the deny mechanism.	3.1, 4.14

Where they differ: Guardrails do not cover everything. AWS SCPs and resource control policies do not apply to the management account or to service-linked roles, and the OCI default Administrators group is exempt from deny policies. Keep those identities workload-free, MFA-protected, and alerted on.

NETWORK Network baseline and connectivity

Remove or secure default networks. Block ingress from 0.0.0.0/0 and ::/0 to the admin ports (22 for SSH and 3389 for RDP). Keep private resources off the public internet with controlled egress, capture flow logs, and design the connectivity topology and private DNS up front, around a central hub that carries the hybrid links.

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**AWS**	Delete unused default VPCs, restrict the default security group to no traffic, and block 22 and 3389 from both 0.0.0.0/0 and ::/0. Use private subnets and VPC endpoints, route egress through a central NAT gateway with AWS Network Firewall, and turn on VPC Block Public Access in ingress-only mode, since bidirectional mode blocks both. Enable VPC flow logs, and centralize hybrid connectivity on a Transit Gateway hub with Direct Connect or Site-to-Site VPN and Route 53 VPC Resolver (formerly Route 53 Resolver) for private DNS. Keep managed databases off the public internet too.	3.2.3, 4.7, 6.2, 6.3, 6.4, 6.5, 6.8
☐	**Azure**	Route through a Connectivity hub with Azure Firewall, and connect on-premises through ExpressRoute or a VPN gateway. Put a network security group on every workload subnet, and restrict inbound RDP, SSH, and UDP from the internet. Use Private Endpoints with Azure Private DNS zones, add Azure Bastion for admin access, and enable virtual network flow logs, which write to a storage account; only Traffic Analytics puts them in the central workspace, in an aggregated form rather than the raw logs, and collection, Traffic Analytics, and the storage are billed separately per gigabyte. Turn on Azure DDoS Network Protection for the hub virtual network, where one plan covers the whole tenant for a fixed monthly charge that includes 100 public IPs.	6.1.1.6, 7.1, 7.2, 7.3, 7.11, 8.4.1, 8.5
☐	**GCP**	Skip default network creation on new projects and delete the default network and its rules from existing ones, then use hierarchical firewall policies to block 22 and 3389 from the internet. Keep instances off public IPs, use Cloud NAT with Private Service Connect endpoints for Google APIs, which CIS prefers to Private Google Access, and enable VPC flow logs. Connect on-premises through Cloud Interconnect or HA VPN into a hub Shared VPC, with Cloud DNS private zones for name resolution.	3.1, 3.6, 3.7, 3.9, 3.10, 4.9
☐	**OCI**	Allow no 0.0.0.0/0 or ::/0 ingress to 22 or 3389 in security lists or network security groups, and restrict each VCN's default security list. CIS tests only the IPv4 form, so check IPv6 by hand. Segment the VCN (OCI's virtual cloud network) with NAT and Service Gateways for private egress, use Bastion for admin access, and enable VCN flow logs. Connect on-premises through FastConnect or Site-to-Site VPN over a hub DRG (dynamic routing gateway, OCI's hub router), with private DNS views.	2.1, 2.2, 2.3, 2.4, 2.5, 4.13

Where they differ: A rule open to ::/0 on an admin port passes every IPv4 check, so close both address families. On Azure, put network security groups on workload subnets only: the platform disables them on AzureFirewallSubnet, GatewaySubnet does not support them, and AzureBastionSubnet needs Bastion's own rule set. Two more Azure notes: NSG flow logs can no longer be created and are deleted when they retire in September 2027, so start on virtual network flow logs, and the DDoS per-IP tier costs less below about 15 public addresses.

ENCRYPT Data protection and encryption

Turn on encryption at rest by default and use customer-managed keys with rotation. Enforce TLS in transit, block public object storage, and keep secrets and certificates in a managed store with scoped access.

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**AWS**	Turn on account-level S3 Block Public Access, EBS encryption-by-default per region, and RDS and EFS encryption. Use KMS customer-managed keys with rotation, require HTTPS on S3, keep secrets in AWS Secrets Manager with rotation, and issue TLS certificates from AWS Certificate Manager rather than uploading them to IAM, removing any expired ones already stored there.	2.17, 3.1.1, 3.1.4, 3.2.1, 3.3.1, 4.6, 6.1.1
☐	**Azure**	Use customer-managed keys in Azure Key Vault with RBAC, purge protection, and automatic rotation. Require secure transfer to storage with a minimum TLS version of 1.2, block anonymous blob access and public network access, and keep application secrets and certificates in Key Vault.	8.3.5, 8.3.6, 8.3.9, 9.3.2.2, 9.3.4, 9.3.6, 9.3.8
☐	**GCP**	Use Cloud KMS customer-managed keys rotated every 90 days in place of the default Google-managed keys, block public buckets with public access prevention, require SSL on Cloud SQL connections, keep managed databases off public IPs, and keep secrets in Secret Manager.	1.11, 1.18, 5.1, 6.4, 6.7
☐	**OCI**	At-rest AES-256 is on by default and cannot be turned off for block, boot, and object storage. Use OCI Vault customer-managed keys for block, boot, object, and file storage, and rotate them at least annually. Automatic scheduled rotation needs a virtual private vault, an isolated HSM partition that costs more than the default shared vault and has to be chosen when the vault is created, since a vault's type cannot be changed afterwards. Keep Object Storage buckets private, and secrets in the Secret Management Service. Keep TLS certificates in OCI Certificates, which renews only the certificates it issues from your own CA; imported ones are updated by hand. Enable block volume in-transit encryption on paravirtualized attachments for VM instances launched from platform images (three bare metal shapes have it on by default, and imported custom images mostly do not support it).	3.3, 4.16, 5.1.1, 5.1.2, 5.2.1, 5.2.2, 5.3.1

Where they differ: Rotation changes only the key used for new encryptions and does not re-encrypt data already written. Azure re-wraps its data encryption keys onto the new version automatically, but only where the service points at the key without a version. That takes an hour to a day or longer depending on the service, and the old version must stay enabled until it finishes. GCP lets you disable or destroy an old version once nothing needs it. OCI has only scheduled deletion at the version level, so retire an old version that way: Disable in OCI Vault applies to the whole key and would lock you out of everything it protects. AWS KMS keeps old key material for decryption until the whole key is deleted, so there is nothing to retire.

LOGGING Org-wide audit logging

Capture an org-wide control-plane audit trail. Deliver it to a centralized, tamper-resistant archive with a retention you have set deliberately, and add service telemetry. Network flow logs belong to the network baseline above.

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**AWS**	Enable a multi-region organization CloudTrail from a delegated admin account, delivering to a central S3 bucket in the Log Archive account with log-file validation, SSE-KMS (server-side encryption with a KMS key), and S3 Versioning plus Object Lock in compliance mode with a default retention period. Send the trail to a CloudWatch Logs group as well, since the metric-filter alarms in the root and configuration rows read from it. A delegated admin must set that up with the CLI or the CreateTrail and UpdateTrail API, and the log group and its role have to sit in the delegated admin account, not the Log Archive account. Turn on S3 server access logging for the trail bucket, writing to a separate bucket in the same account and region with SSE-S3 and no Object Lock. Decide deliberately on data events for sensitive buckets, which are billed per event.	2.1.6, 4.1, 4.2, 4.4, 4.5, 4.8, 4.9
☐	**Azure**	Send the Activity Log and resource diagnostic settings to a central Log Analytics workspace in the management subscription, and export Entra sign-in and audit logs. Set the workspace retention explicitly; the default is 30 days, or 90 where Microsoft Sentinel is enabled, though the Usage and AzureActivity tables keep at least 90 days at no charge. Archive to storage under a locked time-based retention policy for the tamper-resistant copy, since an unlocked one can still be shortened or removed.	6.1.1.1, 6.1.1.2, 6.1.1.8, 6.1.4
☐	**GCP**	Configure Cloud Audit Logs and route all entries through an org-level aggregated sink to a Cloud Storage bucket whose retention policy is sealed with Bucket Lock, which cannot later be shortened or removed. Send a second aggregated sink to a log bucket in the security project, which is what alerting can read. Admin Activity logs are always on. Data Access logs are billed at volume and are off by default everywhere except some BigQuery services, whose logs cannot be turned off, so enable the rest deliberately, starting with services that hold sensitive data. Enable Cloud DNS logging on every VPC network.	2.1, 2.3, 2.4, 2.13
☐	**OCI**	OCI Audit records calls to every supported API and keeps them for 365 days across all regions and compartments, a tenancy-wide period that cannot be changed. It covers Object Storage bucket events but not object events, so pair it with write-level bucket logging. Consolidate logs in OCI Logging and stream a copy to an Object Storage archive through Connector Hub, one connector per region, since Oracle documents no cross-region connector support. Protect that bucket with a time-bound retention rule and lock it, since an indefinite rule cannot be locked. A 14-day delay runs before the lock takes effect; afterwards the duration can only be increased and the rule goes only when the bucket does. Versioning and a retention rule cannot both be active on one bucket, so record the archive as a documented exception to CIS 5.1.3.	4.17

CONFIG Configuration and compliance monitoring

Continuously assess conformance and detect drift across every account and region. Roll the findings up centrally, and bring anything that has drifted back to the approved configuration.

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**AWS**	Run AWS Config in every account and region with an organization aggregator and conformance packs, remediate drift with Config remediation actions, add Control Tower detective controls, and alarm on changes to the Config recorder itself.	4.3, 5.9

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**Azure**	Track the Azure Policy compliance dashboard with remediation tasks, use Defender for Cloud regulatory compliance and secure score, and keep the benchmark policies enabled rather than disabled.	8.1.1.1, 8.1.11
☐	**GCP**	Use Security Command Center with Compliance Manager, since Security Health Analytics is disabled for new Standard-tier activations and only most of its detectors carried over. Compliance Manager gives Security Essentials on Standard and the CIS GCP Foundations Benchmark v3.0 framework on Premium, an older version than the v5.0.0 numbers in the CIS column. Add Vulnerability Assessment for Google Cloud, still in Preview, and Cloud Asset Inventory with asset feeds so configuration changes are recorded. Compliance Manager controls monitor in detective mode by default; a preventative mode can block the change instead. For what stays detect-only, re-apply the foundation from your pipeline.	2.14
☐	**OCI**	With Cloud Guard already enabled, switch the responder rules you trust from Ask me before executing rule to Execute automatically at the target level, since nine of the ten Oracle-managed rules ship set to ask. Cloud Guard accepts automatic execution only when the rule also carries at least one condition. The Cloud Event rule is the exception and already runs automatically, which is what feeds problems to the Events service. Use Security Zones so non-conforming resources cannot be created in protected compartments.	4.14

Where they differ: On Azure, compliance standards beyond the Microsoft cloud security benchmark need a paid Defender plan, though Defender for Servers Plan 1 and Defender for APIs Plan 1 do not include them. The Azure portal classic secure score and the Defender portal Cloud Secure Score are separate models, so track one of them rather than both.

THREAT Threat detection and posture

Run continuous threat detection and a central security-posture view across the whole footprint. Scan workloads and images for vulnerabilities. Aggregate the findings into a SIEM, a security information and event management platform, so whoever owns security has one queue to work from.

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**AWS**	Delegate GuardDuty and Security Hub CSPM administration to the Security Tooling account. Enable GuardDuty across all accounts and regions, turn on Security Hub CSPM (cloud security posture management) with the CIS AWS Foundations Benchmark standard, and aggregate findings to one home region. Scan workloads and images with Amazon Inspector, and forward findings to your SIEM through EventBridge, or through Security Hub CSPM into Amazon Security Lake.	2.1.6, 5.16
☐	**Azure**	Enable Microsoft Defender for Cloud plans on every subscription and keep them on with policy. Scan machines with Defender for Servers Plan 2, since Plan 1 has no agentless scanning and none of the premium Defender Vulnerability Management features, and container images with Defender for Containers. Use Microsoft Sentinel in the Microsoft Defender portal as the central SIEM.	8.1.1.1, 8.1.3.1, 8.1.3.2, 8.1.3.4, 8.1.4.1
☐	**GCP**	Use Security Command Center on the paid Premium tier for threat detection, vulnerability findings, and a central posture view across the organization, exported to a SIEM. Enable the Container Scanning API for Artifact Analysis image scanning, billed once per new image digest. GKE Advanced Vulnerability Insights shut down on June 16, 2026, so cover GKE workloads with Security Command Center instead.	n/a (Security Command Center)

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**OCI**	Use Oracle Cloud Guard as the central posture dashboard with Threat Detector recipes and the Vulnerability Scanning Service for routine host and image scanning. Route logs and scan findings toward a SIEM through Connector Hub, using its Streaming or Functions target, and Cloud Guard problems through an Events rule onto a notification topic, with a function alongside it for the SIEM feed.	4.14, 4.15

Where they differ: Free versus paid: AWS GuardDuty, the Azure Defender for Cloud workload plans, and the GCP Security Command Center Premium tier are paid. OCI Cloud Guard configuration and activity posture management carries no separate charge, though it needs a paid tenancy and its Instance Security Enterprise recipe is a paid add-on. The Security Command Center Enterprise tier shuts down on May 21, 2027, with a default move to Premium. Microsoft Sentinel leaves the Azure portal after March 31, 2027, so stand it up in the Defender portal.

RESILIENCE Backup and disaster recovery

Automate backups and keep them immutable and isolated from production. Set recovery targets for each workload tier: RTO, how long recovery may take, and RPO, how much data loss is acceptable. Spread across zones and regions, then test and document the recovery.

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**AWS**	Apply AWS Organizations backup policies with copy actions into a dedicated, non-default vault in a backup account, enabling cross-account backup from the management account first. Lock the vault in compliance mode, immutable once its three-day minimum grace time passes, since a governance-mode lock can be removed by anyone with sufficient IAM permissions. Design for recovery across multiple Availability Zones and regions with AWS Elastic Disaster Recovery against your defined RTO and RPO, and test the restore.	3.2.4
☐	**Azure**	Use Azure Backup with an immutable vault, enabled and locked, plus multiuser authorization through a Resource Guard owned by a different identity. Soft delete is platform-enforced on Recovery Services vaults; on Backup vaults it can still be turned off outside a few regions, so set it to always-on with a deliberate retention between 14 and 180 days. Cross Region Restore needs the vault on geo-redundant storage, which is the default, and that setting locks once the first backup is configured, so choose it before you protect anything. Disable Cross Subscription Restore, which is on by default. Add Azure Site Recovery through Azure Policy. Set critical storage accounts to geo-redundant storage with blob and container soft delete, and spread across Availability Zones and a second region (a region pair where one exists, since many newer regions are unpaired). Back up Key Vault objects separately; restores are limited to the same subscription and geography. Test the restore.	9.2.1, 9.2.2, 9.3.11
☐	**GCP**	Use the Backup and DR Service with backup plans writing to a backup vault. Set a minimum enforced retention period and lock it, since the period can still be shortened until the lock's effective date arrives. Create the vaults in a dedicated backup project, and choose the vault access restriction at creation, since it cannot be changed later. Grant the vault service agent the Backup and DR Compute Engine Operator role in each project you back up. Enable managed database backups and deletion protection explicitly, since Terraform leaves backups off, spread across zones and regions, and test recovery against your defined RTO and RPO.	6.8, 6.9

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**OCI**	Set Block Volume backup policies: the Oracle-defined bronze, silver, and gold tiers, or a user-defined policy where you need a different schedule or cross-region copy. Use Full Stack Disaster Recovery for cross-region orchestration, withhold VOLUME_BACKUP_DELETE from the group that manages the backups so day-to-day operators cannot delete them, and keep production separate from backup data. Spread across availability domains where the region has more than one, and fault domains otherwise, since most OCI regions have one. Test the restore.	1.15

Where they differ: The Foundations benchmarks reach this domain only partly: Azure covers storage redundancy and soft delete but puts Azure Backup itself in the CIS Azure Storage Services Benchmark, and OCI requires no backups at all, only that they cannot be deleted by the admins who manage them. Both lean on the vendor guidance. Two Azure limits are worth planning around: the Site Recovery policy covers newly created machines only, so run a remediation task for existing ones, and it skips customer-managed-key and Azure Disk Encryption disks, scale sets, Ultra Disks, and powered-off machines; and locked immutability itself is available for both vault types, while the WORM storage tier behind a locked vault is region-limited and still in preview for Backup vaults.

OPERATIONS Operational observability and patching

Collect metrics and health data centrally, set up alerting and dashboards, and patch operating systems and software on a defined cadence. Decide deliberately whether this telemetry shares a workspace with the security audit trail, because that choice drives both access control and cost.

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**AWS**	Collect CloudWatch metrics, logs, and dashboards in a dedicated monitoring account and route alarms to an Amazon SNS topic for notification. Patch across accounts and regions with a Systems Manager Quick Setup patch policy, created from the organization management account and only in the regions where it is offered, and turn on auto minor version upgrades for RDS instances.	3.2.2
☐	**Azure**	Use Azure Monitor with a centralized Log Analytics workspace, alerts including one for Service Health, and dashboards, and patch virtual machines on a schedule with Azure Update Manager, with Azure Policy checking that every machine is enrolled.	6.1.2.11, 8.1.10
☐	**GCP**	Use Cloud Monitoring dashboards and alerting policies with a central metrics scope and notification channels, and install the Ops Agent for guest metrics and logs. Patch operating systems on a schedule with VM Manager, free for 100 VMs per billing account each month and then metered per agent-hour.	4.12
☐	**OCI**	Use OCI Monitoring alarms with the Events and Notifications framework, wire root-compartment Events rules for identity provider, IdP group mapping, IAM group, IAM policy, user, VCN, route table, security list, network security group, and gateway changes onto the notification topic, and build Console Dashboards over the metrics. Patch Oracle Linux and Windows Server hosts with OS Management Hub (Ubuntu, RHEL, SUSE, and Debian need their own patching path, and outside OCI it manages Oracle Linux only), and verify coverage with the Vulnerability Scanning Service.	4.2-4.12

COST Cost and billing baseline

Set budgets with cost alerts, add anomaly alerts where the provider offers them, restrict billing and payment access under least privilege, and turn on cost allocation.

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**AWS**	Set AWS Budgets with alert thresholds, and set the recipients and threshold on the Cost Anomaly Detection monitor that enabling Cost Explorer already creates, adding AWS managed monitors for linked accounts and cost allocation tags. Keep the root user out of routine billing, grant billing access under least privilege, and activate cost allocation tags from the management account.	n/a
☐	**Azure**	Set Microsoft Cost Management budgets with actual and forecast alerts, and add a cost anomaly alert rule per subscription. Set cost allocation rules for shared platform costs; these need an Enterprise Agreement or Microsoft Customer Agreement, and a billing account role rather than an Azure one. Separate cost roles from resource control, with Cost Management Reader to view and Cost Management Contributor to set budgets.	n/a
☐	**GCP**	Set Cloud Billing budgets with alert thresholds and billing export to BigQuery, and keep the Billing Account Administrator and Billing Account Costs Manager roles to a small group. Cost Anomaly Detection is on by default, so set its alert recipients deliberately.	n/a
☐	**OCI**	Set OCI Budgets on compartments with actual and forecast alerts, and turn on Cost Anomaly Detection early, since a cost monitor activates only after 60 days of spending history. Write the budget policy at the tenancy root, since all budgets live there and compartment-scoped budget policies have no effect, and use cost-tracking tags.	n/a

See also: For full cost governance, see the anoBytes Cloud tagging and cost governance guide.

TAGS Tagging and resource organization

Define a mandatory tag set: environment, owner, cost-center, data-classification, and application. Enforce it so untagged resources are blocked or tagged automatically.

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**AWS**	Standardize tag keys and values with Organizations tag policies, which never evaluate untagged resources, so also deny creation without the required tags using an SCP with the aws:RequestTag and aws:TagKeys conditions.	n/a
☐	**Azure**	Enforce a baseline tag schema with Azure Policy (deny, append, or modify). Azure resources do not inherit tags, so use the built-in Modify policies that copy a tag from the resource group or subscription, with a remediation task for the resources that already exist.	n/a
☐	**GCP**	Use Resource Manager tags for policy conditions and cost allocation, since tag bindings inherit down the hierarchy and labels do not, and condition an org policy on a required tag. Tags reach the BigQuery billing export; the console reports still group by labels.	n/a
☐	**OCI**	Use defined tags with Tag Defaults on compartments to auto-apply the tag set to new resources, or set the default to require a value the creator must supply, then sweep and tag whatever predates the defaults.	4.1

See also: For the full tagging standard, see the anoBytes Cloud tagging and cost governance guide.

AUTOMATION Landing zone as code

Define and deploy the landing zone as version-controlled infrastructure-as-code. Keep it in source control with peer review, apply and roll it back through a pipeline, separate the environments, and give the deployment identity only the permissions it needs.

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**AWS**	Manage the foundation with Control Tower, adding the Landing Zone Accelerator on top where you need deeper coverage, plus CloudFormation StackSets. Keep the configuration in Git, promote it through CodePipeline and CodeBuild, and scope the pipeline and StackSets execution roles to only the actions the deployment needs.	n/a
☐	**Azure**	Keep the Azure Landing Zone modules in source control: Bicep AVM, now the default in the ALZ Accelerator, or the Azure Verified Modules ALZ Terraform modules. Classic ALZ-Bicep is deprecated and is archived in February 2027. The older caf-enterprise-scale Terraform module left extended support on August 1, 2026 and is being archived. Build and release through Azure DevOps or GitHub Actions with separate build, test, and release stages, and a deployment service principal scoped to only what it needs.	n/a
☐	**GCP**	Apply the terraform-example-foundation through its GitHub Actions or Terraform Cloud pipeline (plan on pull requests to the environment branches, apply on merge) with infrastructure-as-code policy validation, using the blueprint's per-stage service accounts so each stage holds only its own permissions. The GitLab path is no longer tested upstream, and the Cloud Build path needs Cloud Source Repositories, which a new organization cannot enable.	n/a
☐	**OCI**	Keep the OCI Core Landing Zone Terraform (now oci-landing-zones/terraform-oci-core-landingzone) in Git and deploy it through Resource Manager stacks backed by a configuration source provider, with drift detection and plan-and-approve before apply. Give each stack a dedicated IAM group holding only the policies that stack needs, and launch its jobs from a user who belongs to that group, since Resource Manager has no run-as identity and a job carries the launching user's own permissions. Keep one stack per environment.	n/a

VENDING Account and project provisioning

Provide a governed, automated way to issue new accounts, subscriptions, or projects. Each one should arrive with its place in the hierarchy, guardrails, centralized logging, network connectivity, tags, a budget, and least-privilege access already applied before it is handed over.

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**AWS**	Vend accounts with Control Tower Account Factory (or Account Factory for Terraform), applying organizational-unit placement, guardrails, logging, network, and IAM Identity Center access at creation. Account Factory for Terraform sets account tags from the account request itself; a budget still needs an account customization or a post-provisioning step.	n/a
☐	**Azure**	Vend subscriptions with the Azure Verified Modules subscription vending pattern (Terraform avm-ptn-alz-sub-vending, Bicep avm/ptn/lz/sub-vending) through a pipeline with a request and approval step, applying management-group placement, tags, budget, and hub peering at creation.	n/a
☐	**GCP**	Vend projects with the project factory module used by the blueprint's projects stage, applying enabled APIs, group and service account roles, Shared VPC attachment, and a budget, with organization policy inherited from the parent folder. The stage sets labels only, so add Resource Manager tags yourself.	n/a

	CLOUD	BASELINE	CIS FOUNDATIONS
☐	**OCI**	Use the Core Landing Zone Terraform to vend Network, Security, Application Development, and Database compartments, either in the tenancy root or under an optional enclosing compartment. Each gets its own admin group, policies, and tags, with dynamic groups for the workloads that need them, and the same stack lands the VCNs, Cloud Guard and Security Zones, logging and notifications, and a budget.	n/a

Where they differ: Vending tools differ in what they actually apply. The Azure lz-vending modules were archived in June 2026 and replaced by the Azure Verified Modules pattern above, and stock AWS Account Factory applies neither tags nor budgets without customization.

RE-CHECK What to confirm before you rely on it

Cloud services and names move quickly. As of August 2026, a few worth confirming against current docs:

- **Names and availability in flux:** AWS splits the CSPM (cloud security posture management) service, Security Hub CSPM, from the newer unified Security Hub; the Microsoft cloud security benchmark v2 is in preview alongside v1; the GCP Security Command Center Enterprise tier retires on May 21, 2027 with a default move to Premium, and Security Health Analytics is disabled for new Standard-tier activations in favor of Compliance Manager.
- **Scope and defaults:** AWS EBS encryption-by-default covers only new volumes, and most services are scoped to one region, so Config recorders and GuardDuty detectors must be enabled region by region (GuardDuty through its organization auto-enable setting, Config through Control Tower or StackSets), while one multi-region CloudTrail covers every enabled region.
- **Closed to new customers:** a documented feature is not always one you can still turn on. GCP Cloud Source Repositories is closed to new customers, which puts the foundations blueprint's Cloud Build path out of reach for a new organization. AWS Systems Manager patch groups are no longer offered in the console to any account and region pair not already using them before December 22, 2022, so a new account uses a patch policy instead.

Verify each item against your provider's current documentation and your own risk and compliance needs before you rely on it.

REF References

CIS Foundations Benchmarks: Amazon Web Services v7.0.0, Microsoft Azure v6.0.0, Google Cloud Platform Foundation v5.0.0, Oracle Cloud Infrastructure v3.1.1 · `cisecurity.org`

AWS: Control Tower, Security Reference Architecture, Startup Security Baseline, Organizations best practices · `docs.aws.amazon.com`

Azure: Cloud Adoption Framework landing zones, Microsoft cloud security benchmark, Azure Policy · `learn.microsoft.com`

Google Cloud: landing zone design, enterprise foundations blueprint, Organization Policy Service · `cloud.google.com`

OCI: Core Landing Zone, Security Zones, security best practices · `docs.oracle.com`