

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

Sixteen domains to settle 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

General educational guidance, not affiliated with or endorsed by the Center for Internet Security, Amazon Web Services, Microsoft, Google, or Oracle. Cloud services change, so confirm a detail before you depend on it. Published 2026-10-03.

16 domains

what to settle before the first workload

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. Once workloads are live, you have to retrofit these controls into running systems, which is slow and easy to get wrong.

This checklist is for whoever builds or reviews that foundation. It covers sixteen domains, the service to use for each on AWS, Azure, GCP, and OCI, and the corresponding CIS Foundations Benchmark controls. The later domains depend on the early ones, so work them roughly in order. 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. Every entry describes the commercial regions; service names, tiers, and availability differ in the government and sovereign clouds. 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 has 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 cites representative 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 the landing-zone scope. Providers also surface the CIS standard in their own configuration-checking tools (AWS Security Hub CSPM, for cloud security posture management, plus Microsoft Defender for Cloud and 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 built into a provider's own checking tool is often older: AWS Security Hub CSPM offers v5.0.0. Match on the control title rather than the number alone. Two kinds of cell carry no number:

- n/a with a source in parentheses: the benchmark has no matching control, and the vendor documents the practice in that source.
- A bare n/a: no benchmark control at all. That covers cost, landing zone as code, and account provisioning throughout, and tagging on every cloud but OCI; those cells follow the vendor guidance named in the row itself.

The benchmarks cover backup 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.

Name an owner for each domain

Put a name against each of the sixteen domains before you start, and record who signs off an exception to one. Record the owners and the exceptions where you already track them; the anoBytes exception register and risk register templates cover both. Where security and the platform team are separate groups, agree in advance which of them owns the guardrail, logging, configuration-monitoring, and threat-detection domains. Tick the DONE column on a printed copy, or carry the domains into whatever you already track work in.

Scale it to your size

Get the separation right first; the number of accounts can grow later. 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 configuration checks and audit logging stay on. On AWS the configuration checks named here are paid. AWS Config bills from the start, and Security Hub CSPM bills after a 30-day free trial, whether you enable it alone or through the unified Security Hub's Essentials plan; that plan also covers the Config recording CSPM needs. The domains to do first are the ones that are hard 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. Check the service limits on each new account against what the workload needs. The defaults are set per account, or per tenancy on OCI, and raising one means asking the provider, except that Azure quota groups let an Enterprise Agreement or Microsoft Customer Agreement customer move IaaS compute quota between its own subscriptions.

DONE	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

DONE	CLOUD	BASELINE	CIS FOUNDATIONS
☐	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. - 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.

DONE	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 privileged root actions nobody can recover a member account's root user afterwards. - Only then delete root credentials in member accounts, which leaves no root password or key there to protect. - 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

DONE	CLOUD	BASELINE	CIS FOUNDATIONS
☐	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, and remove API keys from tenancy administrators. Require MFA with a FIDO passkey or hardware key, and alert on local (non-federated) interactive sign-in, because break-glass use of the group appears as a local sign-in. - Give the identity domain administrator roles, such as User administrator, to as few people as possible. A User administrator manages groups and who belongs to them, and deny policies do not override those roles, so a deny statement cannot limit what their holders do in the domain. - Keep a valid, monitored email address on every local account, subscribe a topic to Oracle's announcements, and, once another administrator path is in place, retire the legacy DefaultLocalUser account where the tenancy still has one. - Change the break-glass password on a schedule shorter than the password policy's expiry period, so the account still works when it is needed.	1.2, 1.3, 1.7, 1.12, 1.13, 4.18

Where they differ: 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.

DONE	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 in that identity provider, and prefer FIDO2 keys or passkeys for administrators. Identity Center's own MFA settings are unavailable once an external provider handles sign-in. 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
☐	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

DONE	CLOUD	BASELINE	CIS FOUNDATIONS
☐	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.

DONE	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; its findings are free. An unused access analyzer is billed per role or user and one covers every region. The unified Security Hub's Essentials plan includes one with a fixed 90-day lookback, which does not flag the 45-day credentials above. - For host access, use Systems Manager just-in-time node access, which grants time-limited access after approval and can record RDP sessions to Windows Server. Systems Manager does not end just-in-time sessions on its own, so set the maximum session duration and idle session timeout in each account and Region. Just-in-time node access needs the unified Systems Manager console and, after a free trial, is billed per node-hour for every node Systems Manager manages in each account and Region where it is enabled. Its recording covers RDP sessions only, so turn on session logging in its own session preferences too; where you keep plain Session Manager instead, turn on that service's session logging. Session logging does not cover sessions that connect through port forwarding or SSH.	2.11, 2.13, 2.14, 2.18

DONE	CLOUD	BASELINE	CIS FOUNDATIONS
☐	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 opens and closes the rule on the network security group rather than on a firewall. 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. To record sessions, turn on Bastion session recording, which needs the Premium SKU and a storage container with no immutability policy and no blob versioning, and does not cover sessions opened through the native client. - Microsoft documents just-in-time 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
☐	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 on the accounts CIS 1.16 exempts: the OCI Administrator, break-glass accounts, and service accounts. - 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: Only two clouds have built-in just-in-time role elevation: Azure with Privileged Identity Management (Microsoft Entra ID P2 or Entra ID Governance) and GCP with Privileged Access Manager. AWS has none, so use a partner integration or the AWS TEAM solution. OCI IAM has none either. Oracle Access Governance, a separate service, can grant OCI group membership for a set number of hours or days through a self-service request; without it, use a time-bounded policy condition. CIS Azure 5.3.4 and 5.3.7 ask for periodic reviews of role assignments, which their audit steps do by hand in Access control (IAM); automating them with access reviews needs P2, and only the newer review types need Entra ID Governance.

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.

DONE	CLOUD	BASELINE	CIS FOUNDATIONS
☐	AWS	Use Organizations service control policies (SCPs), resource control policies, and declarative policies, such as one requiring version 2 of the instance metadata service (IMDSv2) for all new instance launches organization-wide. Administer them from a delegated admin account rather than the management account. Add 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	- Where Google has already turned on Security Command Center, add Vulnerability Assessment for Google Cloud before you restrict resource locations, or Google may switch Security Command Center off within seven days. 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, and disable service account key creation. Organizations created on or after May 3, 2024 already enforce the last two. - Restrict IAM grants to your own organization with the domain restriction constraint, set to your customer ID or organization principal set; it is enforced by default in organizations created on or after May 3, 2024. The newer managed constraint iam.managed.allowedPolicyMembers can also list individual principals. - Deny all values on the external IP list constraint, which covers IPv4 only, and pair it with constraints/compute.disableVpcExternallpv6, which disables external IPv6 on VPCs, so no new VM gets a public address. - Add VPC Service Controls perimeters, which restrict access to the Google Cloud APIs you place in them, once you confirm each service you use is supported. Since September 30, 2026, a folder can be a perimeter member, which protects every project and subfolder under it automatically.	1.1.4, 1.5, 3.1, 3.8, 4.9, 5.1, 5.2
☐	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: 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 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.

DONE	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 once the subnets holding the firewall endpoints have a bidirectional exclusion. AWS lists Network Firewall traffic as blocked unless those subnets are excluded, and ingress-only mode ignores an egress-only exclusion. That mode still allows outbound connections through NAT gateways and egress-only internet gateways, which bidirectional mode blocks as well. - Enable VPC flow logs. - 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, and add Azure Bastion for admin access. - 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. - Create one Azure DDoS Network Protection plan and link every landing zone and platform virtual network to it. The Azure Landing Zone default policy assignment links those under the Connectivity and Landing Zones management groups, so link the rest yourself. One plan can serve every subscription in the 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. New Azure NSG flow logs can no longer be created. When the feature retires on September 30, 2027, Azure deletes the existing flow log

resources but keeps the records already in storage, so start on virtual network flow logs. The Azure 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.

DONE	CLOUD	BASELINE	CIS FOUNDATIONS
☐	AWS	Turn on S3 Block Public Access across the organization with an Amazon S3 policy in AWS Organizations, which every account inherits, including new ones. Turn on EBS encryption-by-default in every region (it covers only volumes created afterwards), 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. Keep TLS certificates in Certificate Manager, which renews only the Google-managed ones; uploaded ones are replaced by hand before they expire.	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. Choose that type when you create the vault, because 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 and configure automatic renewal for the ones it issues from your own CA and manages. Renew imported certificates, and any whose private key you manage outside the service, by uploading new PEM files. - 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 the old key material it generated for decryption until the whole key is deleted, so there is nothing to retire; for a key with imported material, deleting any of that material makes the whole key unusable.

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.

DONE	CLOUD	BASELINE	CIS FOUNDATIONS
☐	AWS	- Where Control Tower's CloudTrail integration is on, Control Tower already creates an organization trail; turn the integration off before creating the one below. AWS bills each copy of management events after the first, and from landing zone 4.0, Control Tower's controls block Object Lock on its own log bucket. - 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 too, for the metric-filter alarms in the root and configuration domains. A delegated admin can do that only through the CLI or the CreateTrail and UpdateTrail API, with the log group and role in its own 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 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, and Microsoft Sentinel makes 90 days free but tells you to raise the setting to 90 yourself; the Usage and AzureActivity tables keep at least 90 days at no charge. For the tamper-resistant copy, archive to storage under a time-based retention policy and lock it, because an unlocked policy 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, and alert from it with bucket-scoped log-based metrics. Log-based alerting policies do not read entries that an organization-level sink routes there. - 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. The lock takes effect after a 14-day delay; then the duration can only be increased, and only deleting the bucket removes the rule. - 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

Where they differ: Each cloud keeps a free copy of its control-plane events for a fixed period you cannot change. AWS keeps 90 days of CloudTrail event history in each account and region, Azure 90 days of activity log in each subscription, GCP 400 days in each _Required log bucket, and OCI 365 days of Audit in each region. Each copy stays inside its own account, subscription, project, or region, so on every cloud the central archive still needs a retention period you choose and record. An Azure workspace starts at 30 days, and an AWS trail keeps its S3 objects until a lifecycle rule removes them.

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.

DONE	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
☐	Azure	Track the Azure Policy compliance dashboard with remediation tasks, use Defender for Cloud regulatory compliance and secure score, and leave every non-deprecated Microsoft cloud security benchmark policy enabled.	8.1.1.1, 8.1.11
☐	GCP	- Use Security Command Center with Compliance Manager. Google turns its Standard tier on automatically only in organizations that do not restrict resource locations, so activate it yourself where you restrict them. Security Health Analytics is unavailable on every newly activated tier, Premium and Enterprise included. Some of its detectors, such as OPEN_GROUP_IAM_MEMBER, have no Compliance Manager control on any tier, so check that the ones you rely on are covered. Compliance Manager gives Security Essentials on Standard and a CIS v3.0 framework on Premium, an older version than the v5.0.0 numbers in the CIS column. - Add Vulnerability Assessment for Google Cloud, and Cloud Asset Inventory with asset feeds. Asset Inventory keeps change history for only 35 days, so store the feed messages yourself. - Compliance Manager detects and reports drift; to block a change, rely on the Organization Policy constraints in the guardrails domain. Bring anything else back by re-applying 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. Every Oracle-managed responder rule is set to ask by default except Cloud Event, which feeds problems to the Events service and already runs on its own. - Give each rule you switch at least one condition, because Cloud Guard allows automatic execution only on a rule that has one. For a rule that should apply everywhere, give it a condition that is always true; Oracle's example is Region, Not In, with a value no region has, such as abc.	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 a central security view

Run continuous threat detection and keep one central view of security findings 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.

DONE	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 with the CIS AWS Foundations Benchmark standard, and aggregate findings to one home region. - Use the unified Security Hub as the central view, and turn on Amazon Inspector scanning of EC2 instances, ECR container images, and Lambda functions in every account and region. Enabling Security Hub turns on Security Hub CSPM by itself; Inspector has to be turned on separately. The Essentials plan, billed per resource, covers both. - 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 (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 view of findings across the organization, exported to a SIEM. Enable the Container Scanning API for Artifact Analysis image scanning, billed once per new image digest. Advanced Vulnerability Insights for Google Kubernetes Engine (GKE) shut down on June 16, 2026, so cover GKE workloads with Security Command Center instead.	n/a (Security Command Center)
☐	OCI	Use Oracle Cloud Guard as the central findings dashboard with Threat Detector recipes and the Vulnerability Scanning Service for routine host and image scanning. Route logs toward a SIEM through Connector Hub, using its Streaming or Functions target. Scan findings arrive as Cloud Guard problems, so send those through an Events rule onto a notification topic, with a function alongside it for the SIEM feed.	4.14 , 4.15

Where they differ: 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.

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.

DONE	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, which becomes immutable once its three-day minimum grace time passes; 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

DONE	CLOUD	BASELINE	CIS FOUNDATIONS
☐	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. A VM with any disk on a customer-managed key can be backed up only to a vault created with a customer-managed key, and a key cannot be added to an existing vault. Before you create a vault on a customer-managed key, grant the Backup and DR service agent of the backup project the Cloud KMS CryptoKey Encrypter/Decrypter role on that key. That agent is a different identity from each vault's own service agent. Google normally creates that agent with the project's first Backup and DR resource, so in a backup project with no Backup and DR resources yet, trigger its creation first. • Grant each vault's service agent the Backup and DR Compute Engine Operator role in each project whose VMs it backs up or restores into. In each project whose Cloud SQL instances it backs up, grant it the Backup and DR Cloud SQL Operator role. Where those Cloud SQL instances use customer-managed encryption keys, also grant the Backup and DR service agent of the backup project the Cloud KMS CryptoKey Encrypter/Decrypter role on each instance's key before you back them 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

DONE	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, cross-region copy, or the retention lock below. - Withhold VOLUME_BACKUP_DELETE and BOOT_VOLUME_BACKUP_DELETE from the group that manages the backups, so day-to-day operators cannot delete volume or boot-volume backups. The CIS 1.15 example policy names only the first. - Turn on the retention lock for backups that must survive an attacker. Setting it takes the RETENTION_RULE_LOCK permission, which an administrator grants through an IAM policy. Since August 2026, a Block Volume backup with the lock on cannot be deleted, or its retention shortened, until the period ends. The lock can be set on each backup, or on a schedule in a user-defined backup policy for the backups it creates; Oracle-defined policies cannot be changed, so they cannot carry it. - Use Full Stack Disaster Recovery for cross-region orchestration, 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 rely on the vendor guidance. The Azure 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. Locked immutability is available for both vault types. The write-once (WORM) storage behind a locked vault is generally available only for listed workloads. Backup vaults have it in every public region for AKS, Azure Database for PostgreSQL, and Azure Cosmos DB, and Recovery Services vaults in a listed set of regions. For everything else the service enforces the lock itself, and backups switch to WORM storage on their own once it becomes available, with no data moved.

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.

DONE	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

DONE	CLOUD	BASELINE	CIS FOUNDATIONS
☐	OCI	- Use OCI Monitoring alarms with the notification topic and subscription CIS 4.2 asks for. - Wire one root-compartment Events rule onto that topic for each change CIS 4.3 to 4.12 names: identity provider, identity provider group mapping, IAM group, IAM policy, user, VCN, route table, security list, network security group, and gateway. - Build Console Dashboards over the metrics. - Patch Oracle Linux, Ubuntu, and Windows hosts with OS Management Hub (RHEL, SUSE, and Debian need their own patching path, and outside OCI it manages Oracle Linux only). Confirm the patching with the Vulnerability Scanning Service, which scans a host only when it was built from a supported Oracle platform image.	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.

DONE	CLOUD	BASELINE	CIS FOUNDATIONS
☐	AWS	- Set AWS Budgets with alert thresholds. Since September 30, 2026, a new email recipient gets no alerts until someone signed in to the AWS account that owns the budget follows its verification link. An address used in several accounts must be verified in each one. - In a management or standalone account where Cost Explorer was first enabled on or after March 27, 2023, Cost Anomaly Detection creates an AWS services monitor and a daily summary alert subscription; create both yourself where it was enabled earlier. Set the recipients and threshold on that subscription. A standalone account that later joins your organization, or creates it and so becomes the management account, has changed type and stops running that monitor, so recreate it there. The management account can add one more AWS managed monitor, for linked accounts, a cost allocation tag, or a cost category. - 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, open a Cost analysis smart view on each subscription so anomaly detection starts, 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. Cost Anomaly Detection creates a default monitor per service and region by itself. Add alert subscriptions with your thresholds and recipients, and create any custom monitor early, because a 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. A budget can also target one defined tag value.	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. Settle the resource naming convention in the same sitting, since names such as an S3 bucket, an Azure resource, and a GCP project ID cannot be changed after the resource is created.

DONE	CLOUD	BASELINE	CIS FOUNDATIONS
☐	AWS	- Standardize tag keys and values with Organizations tag policies, and add required tag keys, which CloudFormation, Terraform, and Pulumi can check before a deployment, warning or blocking when a tag is missing. For CloudFormation, that check runs only in the accounts and Regions where its tag policy hook is activated. - Tag policies check required tag keys before creation only through those three tools, and their compliance reports leave out any resource that has never had a tag, so also deny creation without the required tags using an SCP with the <code>aws:RequestTag</code> and <code>aws:TagKeys</code> conditions. - Control Tower does not tag the resources it creates, so an SCP like this can make account provisioning and enrollment fail in its organizational unit. Exempt the <code>AWSControlTowerExecution</code> role the way Control Tower's own SCPs do, then attach the SCP to a test organizational unit registered with Control Tower, which enables its <code>AWSControlTowerBaseline</code>, and provision an account there through Account Factory before you attach it anywhere else.	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 existing resources.	n/a
☐	GCP	Use Resource Manager tags for policy conditions, since tag bindings inherit down the hierarchy and labels do not, and condition an org policy on a required tag. Use labels for cost: Billing reports group and filter by resource labels, budgets filter by one, and neither accepts tags. Tags also reach the BigQuery billing export.	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 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.

DONE	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

DONE	CLOUD	BASELINE	CIS FOUNDATIONS
☐	Azure	- Keep the Azure Landing Zone modules in source control: the Azure Verified Modules (AVM) Bicep implementation, the ALZ Accelerator's only Bicep option since February 16, 2026, or the AVM ALZ Terraform modules. Classic ALZ-Bicep is deprecated and will be archived in February 2027. The older caf-enterprise-scale Terraform module left extended support on August 1, 2026, and its repository was archived in September 2026. - Build and release through Azure DevOps or GitHub Actions with separate build, test, and release stages. The accelerator creates separate managed identities for plan and apply, federated to the pipeline; keep each 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), using the blueprint's per-stage service accounts so each stage holds only its own permissions. Version 6.0.0, released in September 2026, removed the policy validation its pipelines ran, so add a policy check of your own to the plan stage. The blueprint's default Cloud Build path needs Cloud Source Repositories, which an organization that had not enabled it before June 17, 2024 cannot turn on, so a new organization takes one of the other pipelines.	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. Decide how one is closed at the same time, including where its logs go and who removes its access.

DONE	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. Each project inherits the environment tag the blueprint binds to its environment folder; add any other Resource Manager tags yourself, and put cost labels on the resources in each project, because Billing reports and budgets ignore project labels.	n/a

DONE	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 and policies, with dynamic groups for the workloads that need them. The stack's own tags record who created each resource and when, so the tag set from the tagging domain is still yours to add. It enables Cloud Guard by default and creates a target on the root compartment only if one does not already exist. It can also land the VCNs, Security Zones, logging, notifications, and a budget; the VCNs, Security Zones, and the budget stay off until you turn them on, and Security Zones also need the enclosing compartment.	n/a

Where they differ: The Azure Iz-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

These are the names, scopes, and limits most likely to have changed since publication:

- **Names and availability in flux:** AWS splits the CSPM service, Security Hub CSPM, from the newer unified Security Hub, and the Microsoft cloud security benchmark v2 is in preview alongside v1.
- **Scope and defaults:** AWS Config and GuardDuty are regional, so confirm they run in every enabled region of every account. Turn Config on there with Control Tower, StackSets, or Systems Manager Quick Setup, and GuardDuty with its organization auto-enable setting or, since October 1, 2026, an AWS Organizations GuardDuty policy, whose default block covers every region at once; turning on that policy type stops the auto-enable setting from applying.
- **Closed to new customers:** 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. Cloud Source Repositories closed on June 17, 2024 to any organization that had not used it before (see the GCP row under landing zone as code).
- **Dated retirements:** seven services and modules named in the rows above have announced end dates. Past: Advanced Vulnerability Insights for GKE (June 16, 2026), the Azure Iz-vending modules (June 2026), and the caf-enterprise-scale Terraform module (extended support ended August 1, 2026; repository archived September 2026). Ahead: classic ALZ-Bicep archives (February 2027), Microsoft Sentinel leaves the Azure portal (March 31, 2027), the Security Command Center Enterprise tier shuts down (May 21, 2027), and Azure NSG flow logs retire (September 30, 2027). Each date sits in the row it affects.
- **What things cost:** the checklist quotes no prices. It does name free allowances, free trials, break-even points, and which tiers are paid, and a provider can change any of these without renaming the service, so confirm them on each provider's pricing page before you budget.

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

Landing zone modules and accelerators: ALZ-Bicep, terraform-azurerms-caf-enterprise-scale, the Azure Verified Modules subscription vending patterns, terraform-example-foundation, terraform-oci-core-landingzone, and the AWS TEAM solution · github.com

anoBytes: Cloud tagging and cost governance across AWS, Azure, GCP, and OCI; exception register and risk register templates · anobytes.com/resources