AWS CLOUD SECURITY CHECKLIST

Deployments & Operations • 2026 Edition

Prepared by Bithost | ZHOST Consulting Private Limited | sales@bithost.in

v1.0 • February 2026 • Confidential — for internal use

How to use this checklist: Work through each section in order for new deployments. For existing environments, start with every HIGH-priority item across all sections, then return for MEDIUM and LOW. Tick the checkbox when an item is fully in place. For items not applicable to your workload, mark N/A in the Details column.

PRIORITY KEY	
HIGH	Must be done before going live. Direct risk of breach or data loss.
MEDIUM	Important. Address within 30 days of deployment.
LOW	Best practice. Address within 90 days or on next review cycle.

✓	Checklist Item	Details / Notes	Priority
1 | ACCOUNT STRUCTURE & GOVERNANCE			
AWS Organizations & Multi-Account Setup			
☐	**Enable AWS Organizations**	Create a management account and enroll all accounts under it.	HIGH
☐	**Separate Production from Non-Production**	Distinct accounts for prod, staging, dev, and sandbox.	HIGH
☐	**Create Dedicated Logging Account**	All CloudTrail, Config, and flow logs land here only.	HIGH
☐	**Create Dedicated Security/Audit Account**	Security Hub, GuardDuty aggregator, and audit tooling live here.	HIGH
☐	**Apply Service Control Policies (SCPs)**	Block disabling CloudTrail, making S3 public, and disabling GuardDuty org-wide.	HIGH
☐	**Use AWS Control Tower for New Accounts**	Enforce baseline guardrails automatically when new accounts are vended.	MEDIUM
☐	**Enable Delegated Administrator for Security Services**	Delegate GuardDuty, Security Hub, and Config to the security account.	MEDIUM
☐	**Tag Every Account with Owner and Environment**	Enables cost allocation and incident escalation routing.	MEDIUM
Root Account Hardening			
☐	**Enable MFA on Root Account (All Accounts)**	Use a hardware FIDO2 key. Mandatory for management accounts in 2026.	HIGH
☐	**Remove All Root Access Keys**	Root should have zero active programmatic credentials.	HIGH

✓	Checklist Item	Details / Notes	Priority
☐	**Store Root Credentials Offline**	Physical vault or offline password manager. Never in a shared drive.	HIGH
☐	**Create Break-Glass Runbook for Root Access**	Document exact steps, approvals required, and post-use audit process.	HIGH
☐	**Audit Root Usage Monthly via CloudTrail**	Alert immediately on any root login event.	HIGH

✓	Checklist Item	Details / Notes	Priority
2 | IDENTITY & ACCESS MANAGEMENT			
Human Identity			
☐	**Deploy IAM Identity Center (SSO)**	Connect to your IdP (Azure AD, Okta, Google). No standalone IAM users for humans.	HIGH
☐	**Enforce MFA for All Human Identities**	Prefer FIDO2 hardware keys. Minimum: TOTP app for all users.	HIGH
☐	**Require Phishing-Resistant MFA for Admins**	Hardware security keys (YubiKey, etc.) for anyone with privileged access.	HIGH
☐	**Define Permission Sets per Role**	Developer, ReadOnly, DataEngineer, SecurityAdmin — scoped, not shared.	HIGH
☐	**No IAM Users for Humans**	Disable and remove all human IAM users. Replace with Identity Center roles.	HIGH
☐	**Review and Remove Unused IAM Users**	Quarterly audit. Any user inactive 90+ days should be disabled.	MEDIUM
Machine / Service Identity			
☐	**Use IAM Roles for All Workloads**	EC2 instance profiles, ECS task roles, Lambda execution roles — never static keys.	HIGH
☐	**One Role Per Workload**	No shared roles across multiple services or environments.	HIGH
☐	**Apply Least-Privilege Policies**	Start with AWS managed policies; tighten with Access Analyzer findings.	HIGH
☐	**Remove All Unused Access Keys**	Any key not used in 90 days should be deleted, not just disabled.	HIGH
☐	**Rotate Remaining Access Keys (If Any)**	90-day maximum rotation for any approved programmatic keys.	HIGH
☐	**Use IAM Roles Anywhere for On-Prem Workloads**	Eliminate keys for servers that need AWS access from outside.	MEDIUM
☐	**Set a Maximum Session Duration on Roles**	Limit to 1 hour for high-privilege roles; 8 hours maximum for any role.	MEDIUM
Policy Design & Monitoring			
☐	**Enable IAM Access Analyzer in All Regions**	Detect external and cross-account access to S3, KMS, IAM roles, and more.	HIGH

✓	Checklist Item	Details / Notes	Priority
☐	**Use Access Analyzer to Generate Least-Privilege Policies**	Generate policies from observed CloudTrail activity, not guesswork.	HIGH
☐	**Triage Access Analyzer Findings Weekly**	Assign ownership. No finding should sit unreviewed for more than 7 days.	HIGH
☐	**Enable Permission Boundaries for Developer Roles**	Limit maximum permissions developers can grant to any role they create.	MEDIUM
☐	**Use Conditions in Sensitive Policies**	Restrict by VPC, source IP, required encryption context, or MFA status.	MEDIUM
☐	**Quarterly IAM Entitlement Review**	Review all roles, policies, and group memberships for each workload.	MEDIUM

✓	Checklist Item	Details / Notes	Priority
3 | NETWORK SECURITY			
VPC Architecture			
☐	**Use Private Subnets for App and Data Tiers**	No application server or database should be in a public subnet.	HIGH
☐	**Restrict Public Subnets to Entry Points Only**	ALB, API Gateway, NAT Gateway, and bastion hosts (if needed).	HIGH
☐	**Separate VPCs for Prod and Non-Prod**	At minimum — ideally separate accounts. Prevents dev-to-prod pivoting.	HIGH
☐	**Implement Hub-and-Spoke with Transit Gateway**	Shared services VPC connected to spoke VPCs for consistent inspection.	MEDIUM
☐	**Enable VPC Flow Logs in All VPCs**	Send to centralized logging account S3 bucket with 12-month retention.	HIGH
☐	**No Default VPC in Production Accounts**	Delete the default VPC in every production account to prevent accidental use.	MEDIUM
☐	**Use Separate Subnets per Tier**	Web, app, and data tiers in distinct subnets with distinct route tables.	MEDIUM
Security Groups & NACLs			
☐	**No Security Groups with 0.0.0.0/0 Ingress (except ALB/ELB)**	Review and remediate all overly permissive inbound rules.	HIGH
☐	**Reference Security Groups Instead of IP Ranges**	Use SG-to-SG rules for internal traffic; avoids IP drift issues.	HIGH
☐	**Document Every Security Group Rule**	Add description field with the reason, owner, and date added.	MEDIUM
☐	**Audit Unused Security Groups Monthly**	Remove SGs not attached to any resource.	LOW
☐	**Use NACLs as Coarse Blocklists Only**	NACLs for broad deny rules (e.g., blocking known bad CIDRs); SGs for allow rules.	LOW
Edge & Public Exposure			

✓	Checklist Item	Details / Notes	Priority
☐	**Attach AWS WAF to All ALBs and API Gateways**	Enable AWS Managed Rules: Core Rule Set, SQL injection, known bad inputs.	HIGH
☐	**Enable AWS Shield Standard on All Accounts**	Free and automatic. Confirm it's active for critical public endpoints.	HIGH
☐	**Enable AWS Shield Advanced for Critical Services**	For DDoS response support and cost protection on public-facing apps.	MEDIUM
☐	**Use AWS Network Firewall for Egress Filtering**	Inspect and control outbound traffic from VPCs to the internet.	MEDIUM
☐	**Enable Route 53 Health Checks and Failover**	Automatic DNS failover when primary endpoints are unhealthy.	MEDIUM
☐	**Restrict Direct Internet Access from Private Subnets**	All outbound internet traffic routes through NAT Gateway or Firewall.	HIGH
☐	**Treat On-Premises Connections as Untrusted**	VPN and Direct Connect terminate in dedicated networking VPC with inspection.	MEDIUM

✓	Checklist Item	Details / Notes	Priority
4 | DATA PROTECTION & ENCRYPTION			
Encryption at Rest			
☐	**Enable Default Encryption on All S3 Buckets**	Use SSE-S3 minimum; SSE-KMS for sensitive data.	HIGH
☐	**Enable Encryption on All EBS Volumes**	Set account-level default for EBS encryption using KMS.	HIGH
☐	**Enable Encryption for All RDS and Aurora Instances**	Must be done at creation — cannot be added post-launch without snapshot restore.	HIGH
☐	**Enable Encryption for DynamoDB Tables**	Use customer-managed KMS keys for regulated or sensitive tables.	HIGH
☐	**Encrypt All EFS File Systems**	Enable at creation. Enforce via SCP or Config rule.	HIGH
☐	**Encrypt All Backups in AWS Backup**	Apply backup vault encryption with a dedicated KMS key.	HIGH
☐	**Encrypt ElastiCache and OpenSearch Clusters**	Both at-rest and in-transit encryption should be enforced.	HIGH
AWS KMS Key Management			
☐	**Use Customer-Managed Keys for Sensitive Workloads**	CMKs give you rotation control, access policies, and detailed audit logs.	HIGH
☐	**Separate Keys by Workload and Environment**	prod-payments key vs dev-analytics key. Compromise of one doesn't expose all.	HIGH
☐	**Enable Automatic Key Rotation**	Annual rotation for CMKs. More frequent for high-risk workloads.	MEDIUM

✓	Checklist Item	Details / Notes	Priority
☐	**Separate Key Admin from Key Usage**	Key administrators cannot use the key; key users cannot manage it.	HIGH
☐	**Audit KMS Key Usage with CloudTrail**	Alert on unusual decrypt or GenerateDataKey calls.	MEDIUM
☐	**Delete Unused KMS Keys After 30-Day Waiting Period**	Review dependencies before scheduling deletion.	LOW
S3 Security			
☐	**Enable S3 Block Public Access at Account Level**	One setting that overrides all bucket and object ACL settings.	HIGH
☐	**Disable S3 ACLs on New Buckets**	Use bucket policies and IAM only. Object ACLs are a legacy footgun.	HIGH
☐	**Enable S3 Versioning for Critical Buckets**	Protects against accidental deletion and ransomware overwriting objects.	HIGH
☐	**Enable S3 Object Lock for Compliance Logs**	Write-once protection for audit logs and compliance records.	MEDIUM
☐	**Restrict Bucket Access to Specific IAM Roles**	No bucket should be accessible via wildcard principal (*) in its policy.	HIGH
☐	**Enable S3 Access Logging for Sensitive Buckets**	Track GET/PUT/DELETE operations on buckets holding sensitive data.	MEDIUM
☐	**Set S3 Lifecycle Policies for All Buckets**	Auto-expire or archive objects to reduce cost and attack surface.	LOW
Encryption in Transit			
☐	**Enforce TLS 1.2+ on All ALBs**	Update security policies; reject older TLS versions.	HIGH
☐	**Require SSL/TLS on RDS Parameter Groups**	Set rds.force_ssl = 1 for PostgreSQL; require_secure_transport for MySQL.	HIGH
☐	**Enforce HTTPS-Only Access on S3 Buckets**	Add bucket policy Deny on aws:SecureTransport = false.	HIGH
☐	**Use ACM-Managed Certificates**	Automatic renewal. Never manually manage expiring TLS certificates.	MEDIUM
☐	**Enable TLS for All Internal Service Communication**	Service-to-service traffic should not travel in cleartext inside VPC.	MEDIUM

✓	Checklist Item	Details / Notes	Priority
5 | LOGGING, MONITORING & DETECTION			
CloudTrail			
☐	**Enable CloudTrail in All Regions for All Accounts**	Multi-region trail is the baseline. Single-region trail misses lateral movement.	HIGH
☐	**Send Logs to Centralized Logging Account**	Separate account with S3 bucket that workload accounts cannot modify.	HIGH

✓	Checklist Item	Details / Notes	Priority
☐	**Enable CloudTrail Log File Integrity Validation**	Detect if log files are altered or deleted after delivery.	HIGH
☐	**Retain CloudTrail Logs for Minimum 12 Months**	Compliance baseline. 24+ months recommended for regulated workloads.	HIGH
☐	**Enable CloudTrail Insights for Unusual API Activity**	Detects anomalous spikes in write management events automatically.	MEDIUM
☐	**Enable CloudTrail Lake for Cross-Account Queries**	Enables SQL queries across all accounts without custom Athena setup.	MEDIUM
☐	**Alert on Critical CloudTrail Events**	Root login, IAM policy changes, SG changes, trail deletion — all alert immediately.	HIGH
Amazon GuardDuty			
☐	**Enable GuardDuty in All Regions and All Accounts**	Centralize findings into security account via Organizations delegated admin.	HIGH
☐	**Enable GuardDuty S3 Protection**	Detects suspicious data access and permission changes on S3 buckets.	HIGH
☐	**Enable GuardDuty EKS Protection**	Kubernetes audit log and runtime threat detection for EKS clusters.	HIGH
☐	**Enable GuardDuty Malware Protection for EC2**	Scans EBS volumes of suspicious instances without impacting workload.	MEDIUM
☐	**Enable GuardDuty RDS Protection**	Detects unusual login attempts and anomalous access patterns for RDS.	MEDIUM
☐	**Route GuardDuty Findings to Incident Management Tool**	EventBridge rule to Slack, PagerDuty, JIRA, or your SIEM.	HIGH
☐	**Review HIGH Severity Findings Within 4 Hours**	Define SLA for finding triage in your incident response policy.	HIGH
AWS Security Hub			
☐	**Enable Security Hub in All Accounts (Org-wide)**	Aggregate findings from GuardDuty, Config, Inspector, WAF, and partners.	HIGH
☐	**Enable AWS Foundational Security Best Practices Standard**	Continuously scores environment against ~200 AWS security controls.	HIGH
☐	**Enable CIS AWS Foundations Benchmark**	CIS Level 1 minimum; Level 2 for regulated workloads.	HIGH
☐	**Assign Owners to All CRITICAL and HIGH Findings**	Unowned findings are effectively invisible. Ownership drives resolution.	HIGH
☐	**Set SLA for Remediation by Severity**	CRITICAL: 24 hr. HIGH: 72 hr. MEDIUM: 30 days. LOW: 90 days.	HIGH
☐	**Review Security Hub Score Weekly**	Track trend. Any downward movement should trigger investigation.	MEDIUM
☐	**Suppress False Positives with Documented Justification**	Every suppression needs a reason and expiry date.	MEDIUM
AWS Config & Posture Management			
☐	**Enable AWS Config in All Regions and Accounts**	Track configuration changes for all supported resource types.	HIGH

✓	Checklist Item	Details / Notes	Priority
☐	**Enable Config Rules for Critical Controls**	Encryption enabled, public access blocked, MFA required — as Config rules.	HIGH
☐	**Set Up Auto-Remediation for Critical Config Rules**	Use SSM Automation to auto-fix non-compliant resources where safe.	MEDIUM
☐	**Enable Config Conformance Packs**	AWS pre-built packs for PCI DSS, HIPAA, CIS — map compliance automatically.	MEDIUM
☐	**Retain Config History for 12 Months Minimum**	Config history is invaluable during post-incident investigations.	MEDIUM

✓	Checklist Item	Details / Notes	Priority
6 | VULNERABILITY MANAGEMENT			
Amazon Inspector			
☐	**Enable Inspector for All Accounts (Org-wide)**	EC2, ECR container images, Lambda functions, and IaC templates.	HIGH
☐	**Integrate Inspector into CI/CD Pipeline**	Fail builds when container images have CRITICAL vulnerabilities.	HIGH
☐	**Enable Inspector Code Scanning for Lambda**	Detects vulnerabilities in Python, Node.js, and Java Lambda code.	MEDIUM
☐	**Set Vulnerability Remediation SLAs**	CRITICAL: 24 hr. HIGH: 7 days. MEDIUM: 30 days. LOW: 90 days.	HIGH
☐	**Enable Inspector ECR Continuous Scanning**	Re-scan pushed images as new CVEs are published, not just on push.	MEDIUM
Patch Management			
☐	**Use SSM Patch Manager for EC2 Patching**	Define patch baselines per OS. Automate in maintenance windows.	HIGH
☐	**Patch Critical Vulnerabilities Within 24 Hours**	Emergency patching process defined and tested for critical CVEs.	HIGH
☐	**Use Latest AMIs as Base Images**	Pull from AWS-maintained Golden AMIs or rebuild your base monthly.	MEDIUM
☐	**Enable EC2 Image Builder for AMI Pipelines**	Automate AMI creation, hardening, and patching on a schedule.	MEDIUM
☐	**Track Unmanaged (Non-SSM) Instances**	Any EC2 not in SSM is a visibility gap. Alert on unmanaged instances.	MEDIUM

✓	Checklist Item	Details / Notes	Priority
7 | CONTAINER & SERVERLESS SECURITY			
Amazon EKS			

✓	Checklist Item	Details / Notes	Priority
☐	**Enable GuardDuty EKS Audit Log Monitoring**	Detect suspicious kubectl commands, privilege escalation, and container escapes.	HIGH
☐	**Enable GuardDuty EKS Runtime Monitoring**	Process-level visibility for detecting runtime threats inside containers.	HIGH
☐	**Use RBAC with Least-Privilege Kubernetes Roles**	No wildcard verbs or cluster-admin bindings for workload service accounts.	HIGH
☐	**Enable EKS Pod Security Standards (Restricted Profile)**	Enforce restricted PSS for sensitive namespaces as minimum.	HIGH
☐	**Run Containers as Non-Root**	Security context: runAsNonRoot: true, runAsUser: 1000 minimum.	HIGH
☐	**Use Private EKS API Endpoint**	Disable public endpoint for clusters not needing external kubectl access.	MEDIUM
☐	**Scan Kubernetes Manifests in CI**	Use Checkov or kube-score to catch privileged containers before deploy.	MEDIUM
☐	**Enable EKS Control Plane Logging**	Enable audit, authenticator, and API server logs to CloudWatch.	HIGH
Amazon ECS			
☐	**Use ECS Task Roles (Not Instance Roles)**	Task-level IAM scoping. Instance roles give all tasks the same access.	HIGH
☐	**Enable ECS Exec for Debugging (With Logging)**	Disable in production, or enable with CloudTrail logging and time limits.	MEDIUM
☐	**Use AWS Fargate for Untrusted Workloads**	No shared kernel surface with Fargate. Reduces container escape blast radius.	MEDIUM
☐	**Run Containers Read-Only Where Possible**	Read-only root filesystem blocks many persistence techniques.	MEDIUM
AWS Lambda			
☐	**One Execution Role Per Function**	No shared Lambda roles. Scope each function's permissions exactly.	HIGH
☐	**Store Secrets in Secrets Manager (Not Env Vars)**	Env vars are visible in the Lambda console and CloudTrail.	HIGH
☐	**Validate All Input to Lambda Functions**	Treat all invocation payloads as untrusted. Validate and sanitize.	HIGH
☐	**Enable Lambda Advanced Logging (JSON Structured)**	Structured logs enable filtering and alerting in CloudWatch.	MEDIUM
☐	**Set Appropriate Timeout and Memory Limits**	Over-provisioned Lambda functions are a DoS risk and waste budget.	LOW
☐	**Use Lambda Layers for Shared Dependencies**	Centralize and scan dependency updates rather than per-function copies.	LOW

✓	Checklist Item	Details / Notes	Priority

8 | SECRETS & CONFIGURATION MANAGEMENT

✓	Checklist Item	Details / Notes	Priority
Secrets Manager			
☐	**Store All Secrets in AWS Secrets Manager**	Database passwords, API keys, OAuth tokens — none in env vars or code.	HIGH
☐	**Enable Automatic Secret Rotation**	Use Lambda-based rotation for RDS, Redshift, and DocumentDB secrets.	HIGH
☐	**Audit Secret Access with CloudTrail**	Alert on GetSecretValue calls from unexpected roles or outside business hours.	HIGH
☐	**Grant GetSecretValue Only to Roles That Need It**	Scoped resource-level IAM policy per secret ARN.	HIGH
☐	**Enable Secret Replication for Multi-Region Apps**	Replicate secrets to disaster recovery regions.	MEDIUM
Systems Manager Parameter Store			
☐	**Use SecureString for Sensitive Parameters**	KMS-encrypted at rest. Use CMK not default SSM key for critical params.	HIGH
☐	**Separate Parameter Paths by Environment**	/prod/app/db-password vs /dev/app/db-password.	MEDIUM
☐	**Audit Parameter Access via CloudTrail**	GetParameter calls logged. Alert on access outside normal patterns.	MEDIUM
Secret Hygiene			
☐	**Scan Codebase and Repositories for Hardcoded Secrets**	Run git-secrets or truffleHog on all repos. Block commits with secrets.	HIGH
☐	**Rotate Immediately if a Secret Is Exposed**	Treat any exposed credential as compromised. Rotate before investigating.	HIGH
☐	**Enable GitHub Secret Scanning (or Equivalent)**	Auto-detect secrets pushed to version control in real time.	HIGH
☐	**Delete Old Versions of Secrets After Rotation**	Previous versions should be cleaned up after a safe rotation window.	LOW

✓	Checklist Item	Details / Notes	Priority
9 | DEVSECOPS & SECURE DELIVERY			
Infrastructure as Code			
☐	**All Infrastructure Defined as Code**	CloudFormation, CDK, Terraform, or Pulumi. No manual console deployments to prod.	HIGH
☐	**Store IaC in Version Control with PR Reviews**	Every infrastructure change reviewed before merge. No direct commits to main.	HIGH
☐	**Scan IaC Templates Before Deployment**	Checkov, tfsec, or cfn-nag in CI pipeline. Block CRITICAL findings.	HIGH
☐	**Enforce Encryption and Tagging via IaC Policies**	OPA or Sentinel policies that reject templates missing required controls.	HIGH

✓	Checklist Item	Details / Notes	Priority
☐	**Test IaC Changes in Non-Prod Before Prod**	Staging environment mirrors production configuration exactly.	HIGH
☐	**Maintain Drift Detection**	Alert when live infrastructure diverges from its IaC definition.	MEDIUM
	CI/CD Pipeline Security		
☐	**Scan Container Images in CI Before Push**	Fail pipeline on CRITICAL CVEs. Warn on HIGH. Allow LOW/MEDIUM.	HIGH
☐	**Use OIDC for CI/CD AWS Authentication**	GitHub Actions, GitLab CI, and CircleCI all support OIDC. No static keys.	HIGH
☐	**Least-Privilege IAM Roles for CI/CD**	Deploy role can only deploy. It cannot read secrets or modify IAM.	HIGH
☐	**Run SAST in Pull Request Pipelines**	Static analysis catches insecure code patterns before code review.	MEDIUM
☐	**Run Dependency Scanning in CI**	Detect vulnerable open-source packages at build time.	MEDIUM
☐	**Sign Container Images and Verify Signatures**	Use AWS Signer or Cosign to verify image provenance before deployment.	MEDIUM
☐	**Audit All Pipeline Execution Logs**	Keep CI/CD logs in centralized logging for 12 months.	LOW

✓	Checklist Item	Details / Notes	Priority
	10 | INCIDENT RESPONSE & RECOVERY		
	Preparedness		
☐	**Write Runbooks for Top 5 Incident Scenarios**	Compromised key, public S3 exposure, GuardDuty HIGH finding, DDoS, data loss.	HIGH
☐	**Store Runbooks Outside Primary AWS Environment**	Use a separate tool (Confluence, Notion, Google Docs) with offline backup.	HIGH
☐	**Define Incident Severity Levels and Escalation Paths**	Who gets called at 2 AM for a CRITICAL finding? Written, tested, agreed.	HIGH
☐	**Conduct Tabletop Exercises Quarterly**	Simulate incidents with the full response team. Identify gaps before they're real.	MEDIUM
☐	**Run Annual Game Day with Simulated AWS Compromise**	Test the entire response chain end-to-end in a non-production environment.	MEDIUM
	Detection & Response Tooling		
☐	**Integrate All AWS Security Findings into SIEM**	Security Hub, GuardDuty, Config, Inspector findings → centralized SIEM.	HIGH
☐	**Set Up EventBridge Rules for Auto-Response**	Auto-isolate EC2 instances, revoke credentials, or notify on critical events.	HIGH
☐	**Maintain Forensic Investigation Capability**	Pre-built Forensics account with access to take EBS snapshots and memory images.	MEDIUM

✓	Checklist Item	Details / Notes	Priority
☐	**Pre-Approve Incident Response IAM Roles**	Break-glass roles with elevated access. Locked, audited, time-limited access.	MEDIUM
☐	**Enable AWS Systems Manager Session Manager for Access**	No open SSH/RDP ports. All instance access through SSM with full session logging.	MEDIUM
Backup & Recovery			
☐	**Use AWS Backup for All Critical Workloads**	Centralized backup policies across RDS, EFS, DynamoDB, EC2, and EBS.	HIGH
☐	**Test Backup Restores on a Monthly Schedule**	A backup you've never tested is a file you hope contains what you think it does.	HIGH
☐	**Enable Cross-Region Backup Replication**	Primary region outage should not prevent restoring from backup.	HIGH
☐	**Set Backup Vault Lock (Immutable Backups)**	Ransomware cannot delete backups protected by Vault Lock.	HIGH
☐	**Define and Test RTO and RPO for Critical Workloads**	Recovery Time Objective and Recovery Point Objective must be documented and verified.	HIGH
☐	**Enable Point-in-Time Recovery for RDS and DynamoDB**	Allows restore to any second within the retention window.	MEDIUM

✓	Checklist Item	Details / Notes	Priority
11 | COMPLIANCE & GOVERNANCE			
Compliance Automation			
☐	**Map Security Controls to Compliance Framework**	SOC 2, ISO 27001, PCI DSS, HIPAA — document the AWS service for each control.	HIGH
☐	**Use AWS Audit Manager for Evidence Collection**	Auto-collect evidence from Config, CloudTrail, and Security Hub.	MEDIUM
☐	**Enable Relevant Security Hub Compliance Standards**	CIS AWS Foundations, PCI DSS, NIST CSF — enable the one(s) that apply.	HIGH
☐	**Conduct Well-Architected Security Pillar Review Annually**	Formal workload review using AWS WA Tool. Track remediation as work items.	MEDIUM
☐	**Document Accepted Risks Formally**	Every suppressed finding or known gap must have a written risk acceptance.	MEDIUM
Access Reviews & Governance			
☐	**Quarterly IAM Access Review for All Production Accounts**	Review all roles, users, policies, and trust relationships.	HIGH
☐	**Annual Third-Party Penetration Test**	External perspective on your AWS environment. Required for most compliance frameworks.	MEDIUM
☐	**Maintain Asset Inventory via AWS Config**	Every resource tracked, tagged, and associated with an owner.	MEDIUM

✓	Checklist Item	Details / Notes	Priority
☐	**Enforce Mandatory Tagging via SCP and Config Rules**	Owner, Environment, Application, and CostCenter tags on all resources.	MEDIUM
☐	**Publish Internal Security Baseline Documentation**	Teams should know what security standards they're building to.	LOW

This checklist is based on AWS Well-Architected Security Pillar guidance, CIS AWS Foundations Benchmark v3.0, and NIST CSF 2.0 controls as of February 2026. Controls evolve — review this document quarterly.

For implementation support, security audits, or SIEM/DLP integration: **sales@bithost.in | +91 911-336-6525**