

Cloud security audit checklist (AWS)

Week 10. Audit only your own practice account (AWS Free Tier). Set a billing alarm before you start. Tools such as ScoutSuite or AWS Security Hub can automate many checks; confirm each finding yourself.

Account and identity

- ☐ Root account has MFA and no access keys; not used day to day
- ☐ Every person has their own IAM user or SSO identity with MFA
- ☐ No IAM policies with "Action": "*" on "Resource": "*" except break-glass
- ☐ Access keys rotated; unused keys and users removed
- ☐ Billing alarm and budget configured

Storage (S3)

- ☐ Block Public Access on at account level
- ☐ No buckets readable by everyone unless intentionally public
- ☐ Default encryption on; versioning on for important data
- ☐ Access logging enabled for sensitive buckets

Network

- ☐ Security groups don't allow 0.0.0.0/0 on SSH (22), RDP (3389) or databases
- ☐ Databases in private subnets, not publicly accessible
- ☐ Default VPC reviewed or removed in unused regions

Compute and data

- ☐ Instances patched; IMDSv2 required
- ☐ EBS volumes and RDS databases encrypted
- ☐ Snapshots not shared publicly
- ☐ Secrets in Secrets Manager or Parameter Store, not in code or user data

Logging and detection

- ☐ CloudTrail on in all regions, logs protected
- ☐ GuardDuty enabled
- ☐ Alerts for root login and IAM changes

Shared responsibility

- ☐ List what AWS secures (the cloud) and what you secure (in the cloud) for each service you use