AWS Cloud Security Checklist

This checklist is designed to help you establish a secure and compliant environment in AWS.

Following these steps will strengthen your cloud security posture, protect sensitive data, and reduce the risk of unauthorized access or breaches.

# 1. Account and Identity Management

☐ Enable Multi-Factor Authentication (MFA) for root and IAM user accounts.
☐ Restrict the use of the root account; use it only for essential administrative tasks.
☐ Create IAM roles for administrative and service-level access instead of sharing credentials.
☐ Follow the principle of least privilege by assigning minimal permissions to users and roles.
☐ Regularly review and rotate IAM credentials, access keys, and API keys.
☐ Use AWS Identity Center (formerly SSO) for centralized user and role management.

# 2. Network Security

☐ Implement a Virtual Private Cloud (VPC) with subnets for isolated workloads.
☐ Use security groups and network access control lists (NACLs) to restrict inbound/outbound traffic.
☐ Set up bastion hosts for secure administrative access.
☐ Enforce end-to-end encryption for all data in transit using HTTPS, VPNs, or private links.
☐ Enable AWS Shield to protect against DDoS attacks.
☐ Regularly review open ports and IP ranges in security groups to ensure minimal exposure.

# 3. Data Protection

☐ Encrypt all sensitive data at rest using AWS Key Management Service (KMS).
☐ Enable S3 bucket encryption and restrict public access to buckets.
☐ Use CloudFront with SSL certificates to secure content delivery.
☐ Regularly back up critical data using AWS Backup or snapshots for disaster recovery.
☐ Enable Amazon Macie to identify and secure sensitive data stored in AWS.
☐ Ensure compliance with your organization’s data protection policies and regulations (e.g., GDPR, PCI).

# 4. Logging and Monitoring

☐ Enable AWS CloudTrail for logging API calls and monitoring account activity.

☐ Use Amazon CloudWatch to set up alarms and monitor system performance.

☐ Enable AWS Config to track and audit resource configurations.

☐ Configure VPC Flow Logs to capture and monitor network traffic.

☐ Use AWS GuardDuty for continuous threat detection and security monitoring.

# 5. Application Security

☐ Use AWS Web Application Firewall (WAF) to protect against common web vulnerabilities.

☐ Regularly scan containerized applications using Amazon Inspector or third-party tools.

☐ Leverage AWS Secrets Manager to securely store and manage application secrets.

☐ Implement security best practices in your CI/CD pipeline for automated deployments.

# 6. Compliance and Governance

☐ Use AWS Organizations to manage multiple accounts with centralized billing and governance.

☐ Enable Service Control Policies (SCPs) to enforce security policies across accounts.

☐ Regularly perform security assessments using AWS Trusted Advisor or third-party tools.

☐ Implement tagging strategies to track and manage resources effectively.

☐ Ensure proper documentation of security configurations for compliance audits.

# 7. Incident Response and Recovery

☐ Create an incident response plan tailored to your AWS environment.

☐ Test your disaster recovery strategy using AWS Backup or failover simulations.

☐ Enable AWS Config Rules to detect and remediate misconfigurations.

☐ Use Amazon Detective to investigate and analyze potential security incidents.

Need a hand with the next step?

If you have a question about any of these steps, or need help setting up a more advanced or tailored solution, we're here for you!

Feel free to send us an email at contact@403bits.com.

For simpler queries, we'll gladly share advice or point you in the right direction — free of charge!

And if you're facing a more complex challenge or want to save time, our experts can take over and deliver a comprehensive setup that perfectly fits your needs.

We're here to help you build security and efficiency
so you can focus on growing your business!

If you liked this checklist or have improvement suggestions, - let us know contact@403bits.com.