ECHELON
RISK +
CYBER

Managed Cloud Security Checklist

As organizations increasingly adopt cloud environments, securing these dynamic platforms is critical to maintaining a strong security posture. This checklist provides actionable steps to enhance cloud security, including logging and monitoring, network segmentation, and vulnerability management. Take control of your cloud security with best practices that mitigate risks and support compliance.

□ Enable logging and monitoring in cloud environments (e.g., AWS CloudTrail, Azure Monitor)

□ Implement network segmentation within cloud environments.

□ Regularly review and rotate access keys and credentials.

□ Perform regular cloud security posture assessments.

□ Apply Identity and Access Management best practices for users and roles including privileged account management.

□ Encrypt data at rest and in transit.

□ Conduct regular vulnerability scans of cloud resources.

□ Configure workload protection using native tools (e.g., AWS GuardDuty, Azure Security Center) or third-party provider (e.g., CrowdStrike Falcon Cloud Security, Palo Alto Networks Prisma Cloud, Wiz, etc.)

Protect your cloud investments with expert guidance—contact Echelon Risk + Cyber to learn more about our Managed Cloud Security services.

We defend the basic human right to security and privacy. echeloncyber.com