CAPTAIN I.T.

CLOUD SECURITY ASSESSMENT CHECKLIST

As more businesses shift to the cloud, ensuring a secure and compliant cloud environment is essential. This Cloud Security Assessment Checklist helps identify vulnerabilities, enforce best practices, and protect sensitive data stored and processed in cloud platforms. Use this tool to evaluate your current cloud posture or prepare for an audit.

Identity and Access Management (IAM)

- [ ] Implement role-based access control (RBAC)
- [ ] Use multi-factor authentication (MFA) for all user accounts
- [ ] Review inactive or orphaned accounts regularly
- [ ] Set up conditional access policies
- [ ] Limit use of global/admin privileges

Data Security

- [ ] Ensure data encryption at rest and in transit
- [ ] Classify and tag sensitive data
- [ ] Apply rights management for confidential data
- [ ] Enable secure file sharing policies
- [ ] Use secure key management solutions

Configuration and Monitoring

- [ ] Use baseline security configurations for cloud resources
- [ ] Enable logging and monitoring (CloudTrail, Azure Monitor, etc.)
- [ ] Monitor for unusual login activity or access patterns
- [ ] Set up alerts for changes to configurations or access rights
- [ ] Perform regular cloud security posture assessments (CSPM)

Network Security

- [ ] Segment cloud networks using subnets and VNETs/VPCs
- [ ] Restrict inbound and outbound traffic using firewalls
- [ ] Use private endpoints where possible
- [ ] Limit use of public IP addresses and services
- [ ] Inspect traffic with intrusion detection/prevention systems (IDS/IPS)

Compliance and Governance

- [ ] Define and enforce data residency and retention policies
- [ ] Review compliance with HIPAA, GDPR, CMMC, PCI-DSS, etc.
- [ ] Conduct periodic security audits and penetration tests
- [ ] Maintain cloud asset inventory and audit trails
- [ ] Ensure vendor compliance and certifications (e.g., SOC 2, ISO 27001)

Backup and Disaster Recovery

- [ ] Verify cloud backup policies are in place and automated
- [ ] Test restore procedures regularly
- [ ] Ensure snapshots and backups are protected from deletion
- [ ] Define RTO and RPO for cloud workloads
- [ ] Use geo-redundant backup strategies for critical data

Need Help Securing Your Cloud Environment?

Captain IT specializes in securing cloud environments for small and mid-sized businesses. From Microsoft 365 to Azure and AWS, we help you meet compliance standards and protect critical data.

Contact us for a FREE consultation!

Hello@CaptainIT.com

(800) 834-9795