Cloud Security Assessment Checklist

1. Assessment Scope

- [ ] Assessment scope is clearly defined (environments, cloud providers, accounts, regions)
- [ ] Compliance requirements are documented (SOC 2, ISO 27001, PCI DSS, HIPAA, etc.)
- [ ] Assessment type and frequency are identified (configuration review, compliance, penetration testing; point-in-time or continuous)

2. Asset Inventory

- [ ] All known cloud assets are cataloged (compute, storage, networking)
- [ ] Asset discovery to identify shadow IT is completed
- [ ] Asset owners, criticality levels, and dependencies are documented

3. Threat Modeling

- [ ] Crown jewel assets are identified
- [ ] Potential attack paths and threat categories are documented (misconfiguration, privilege abuse, lateral movement, API abuse)

4. Network Security

- [ ] Security groups and firewall rules follow least privilege (IaaS)
- [ ] No unnecessary ports are open to the internet (0.0.0.0/0) (IaaS)
- [ ] Network segmentation exists between critical workloads (IaaS)
- [ ] Public endpoints are intentional and justified (all models)
- [ ] Network access controls and IP whitelisting are configured appropriately (PaaS/SaaS)

5. Storage Security

- [ ] No storage buckets or objects are publicly accessible (unless intentional)
- [ ] Encryption at rest is enabled for all sensitive data
- [ ] Encryption in transit is enforced
- [ ] Backup and versioning are configured and work as expected
- [ ] Storage access permissions follow least privilege

6. Access Management

- [ ] IAM policies follow least privilege principle
- [ ] MFA is enforced for all privileged accounts
- [ ] No unused or stale accounts exist
- [ ] Root/admin account usage is monitored and restricted
- [ ] Secrets are stored in proper vaults (not hardcoded)

Attaxion

7. Platform-Specific Services

- [ ] Container images are scanned for vulnerabilities
- [ ] Databases are not publicly accessible (unless required)
- [ ] Database encryption and backup are enabled
- [ ] API gateways have authentication and rate limiting configured

8. Vulnerabilities and Configuration

- [ ] Known vulnerabilities are identified and prioritized
- [ ] Everything that needs patching is catalogued and prioritized
- [ ] Third-party dependencies are current and scanned for vulnerabilities

9. Logging and Monitoring

- [ ] Cloud audit logs are enabled
- [ ] Logs are centralized and retained per policy
- [ ] Security alerts are configured and tested
- [ ] Incident response procedures are documented and up to date

10. Compliance and Governance

- [ ] Security controls map to required compliance frameworks
- [ ] Security policies are documented and enforced
- [ ] Audit trails are complete and protected

11. Post-Assessment

- [ ] All findings are risk-scored based on likelihood, severity, and business impact
- [ ] Remediation plan exists with clear ownership and timelines
- [ ] Continuous monitoring is configured for ongoing posture management
- [ ] Next assessment date is scheduled

Assessment Date: _____

Completed By: _____

Next Assessment: _____

Attaxion