Cloud Application Security Audit Checklist

1. Authentication & Access Control

☐ Multi-factor authentication (MFA) is enabled for all users ☐ Access rights are reviewed regularly and based on least privilege ☐ Role-based access control (RBAC) is implemented ☐ Default accounts are disabled or secured ☐ Inactive user accounts are removed or disabled promptly

2. Data Security

☐ Data is encrypted at rest ☐ Data is encrypted in transit ☐ Sensitive data is masked or tokenized where appropriate ☐ Backups are performed regularly and tested ☐ Access to sensitive data is logged and monitored

3. Application Security

☐ Regular vulnerability assessments are conducted ☐ Web application firewall (WAF) is in place ☐ Security patches are applied in a timely manner ☐ Third-party libraries are tracked and updated ☐ Secure coding standards are enforced

4. Logging & Monitoring

☐ Centralized logging is enabled ☐ Logs are reviewed for suspicious activity ☐ Security incidents are documented and investigated ☐ Alerts are configured for critical security events

5. Compliance & Governance

☐ Application complies with relevant regulations (e.g. GDPR, HIPAA) ☐ Data retention policies are defined and enforced ☐ Privacy policies are communicated to users ☐ Security policies are documented and reviewed regularly

6. Audit Summary

Section	Total Checks	Completed	Notes
Authentication & Access Control	5		
Data Security	5		
Application Security	5		
Logging & Monitoring	4		
Compliance & Governance	4		