NCA Cloud Compliance Checklist

42 Checkpoints Across 7 Compliance Domains

The Complete Guide for Enterprises Operating Cloud Infrastructure in Saudi Arabia

Why This Checklist Matters

The NCA Cloud Computing Controls (CCC-2) framework defines mandatory security requirements for all cloud service providers and consumers operating in Saudi Arabia.

Non-compliance can result in regulatory penalties, loss of government contracts, and reputational damage.

Use this checklist to assess your cloud provider against all 7 NCA compliance domains and identify gaps before your next audit.

Prepared by MomentumX

Sovereign Cloud Infrastructure for MENA | momentumx.cloud

Domain 1: Data Sovereignty & Residency

- [ ] All data classified per NCA Data Classification Policy
- [ ] Primary and backup data stored within KSA borders
- [ ] Data processing occurs exclusively within KSA jurisdiction
- [ ] Cross-border data transfer controls documented and enforced
- [ ] Data residency compliance verified with cloud provider SLA
- [ ] Sovereignty requirements included in vendor contracts

Domain 2: Access Control & Identity Management

- [ ] Multi-factor authentication (MFA) enforced for all admin access
- [ ] Role-based access control (RBAC) implemented and documented
- [ ] Privileged access management (PAM) solution deployed
- [ ] Access reviews conducted quarterly with audit trail
- [ ] Identity federation complies with NCA identity standards
- [ ] Service account credentials rotated per policy

Domain 3: Encryption & Key Management

- [ ] Data encrypted at rest using AES-256 or equivalent
- [ ] Data encrypted in transit using TLS 1.2+
- [ ] Encryption key management under customer control
- [ ] HSM or equivalent key protection mechanisms in place
- [ ] Key rotation policy defined and automated
- [ ] Encryption standards meet NCA cryptographic requirements

Domain 4: Network Security & Isolation

- [ ] Network segmentation between tenants verified
- [ ] Virtual private cloud (VPC) isolation configured
- [ ] Intrusion detection/prevention systems (IDS/IPS) active
- [ ] DDoS protection mechanisms in place
- [ ] Network traffic monitoring and logging enabled
- [ ] Firewall rules reviewed and documented quarterly

Domain 5: Business Continuity & Disaster Recovery

- [ ] BC/DR plan documented and aligned with NCA requirements
- [ ] Recovery Time Objective (RTO) defined and tested
- [ ] Recovery Point Objective (RPO) defined and tested
- [ ] Backup systems located within KSA borders
- [ ] Annual DR testing conducted with documented results
- [ ] Incident escalation procedures defined and communicated

Domain 6: Audit, Logging & Monitoring

- [ ] Comprehensive audit logging enabled for all cloud services
- [ ] Log retention meets NCA minimum requirements (12 months)
- [ ] Security Information and Event Management (SIEM) deployed
- [ ] Real-time alerting configured for critical security events
- [ ] Log integrity protection mechanisms in place
- [ ] Regular log review process documented and followed

Domain 7: Compliance Governance & Vendor Management

- [ ] Cloud governance framework documented and approved
- [ ] Vendor risk assessment completed for all cloud providers
- [ ] SLA compliance monitoring process established
- [ ] Regular compliance assessments scheduled (min. annually)
- [ ] Incident response plan specific to cloud services documented
- [ ] Staff security awareness training conducted annually
- [ ] Regulatory change management process in place
- [ ] Third-party audit reports (SOC 2, ISO 27001) obtained and reviewed
- [ ] Compliance exceptions documented with compensating controls
- [ ] Executive oversight and reporting structure defined
- [ ] Contract exit strategy and data portability plan documented
- [ ] Compliance dashboard or reporting mechanism operational