CONCEPT

Saudi NCA Cloud Cybersecurity Controls (CCC-2:2024) and Cloud First Policy Compliance

Saudi NCA Cloud Cybersecurity Controls (CCC-2:2024) and Cloud First Policy Compliance

Technical depth: Practitioner · **Practical mode:** Case study

Introduction

Saudi government entities and critical infrastructure operators are moving workloads to the cloud under the KSA Cloud First Policy, while the National Cybersecurity Authority NCA requires them and their providers to meet the Cloud Cybersecurity Controls, CCC-2:2024. Teams often misread which controls fall to the tenant, rely on provider claims without evidence and misjudge classification and localisation rules. This coreconcept KSA course shows practitioners how to apply NCA CCC alongside ISO/IEC 27017 and the CSA Cloud Controls Matrix, and participants leave with an NCA CCC Compliance and Cloud Security Plan for their own environment.

Course Objectives

- Explain how the KSA Cloud First Policy, CST cloud regulations and NCA CCC-2:2024 apply to an entity's cloud adoption decisions
- Map NCA CCC-2:2024 tenant and provider controls to ECC-2:2024, ISO/IEC 27017 and the CSA Cloud Controls Matrix v4.1
- Determine the controls that apply to each workload from its data classification level and service model
- Configure and verify identity, encryption, logging and secure configuration controls for cloud workloads
- Assess cloud service providers and contracts against NCA CCC and CST registration requirements
- Produce an NCA CCC Compliance and Cloud Security Plan with a prioritised remediation roadmap

Target Audience

- Cloud and infrastructure engineers building and operating workloads for government and critical infrastructure clients
- Cybersecurity officers responsible for NCA ECC and CCC compliance in their entity
- Governance, risk and compliance specialists preparing NCA self-assessments and evidence
- Compliance and security staff at cloud service providers serving in-scope tenants
- IT procurement and contract specialists sourcing cloud services

Course Outline

Day 1: Cloud Adoption Context in Saudi Arabia

- NIST SP 800-145 Service and Deployment Models in Government Cloud Adoption
- KSA Cloud First Policy: SaaS, PaaS and IaaS Priority and Data Centre Restrictions
- CST Cloud Computing Service Provisioning Regulations and CSP Registration Classes
- Shared Responsibility Matrix by Service Model
- Cloud Workload Inventory for a Current-State Assessment

Day 2: NCA CCC and Related Standards

- NCA CCC-2:2024 Structure: Four Domains, Provider Controls and Tenant Controls
- NCA ECC-2:2024 as the Baseline for CCC Compliance
- Data Classification Levels and Control Applicability under NCA CCC and NDMO Rules
- ISO/IEC 27017:2026 and ISO/IEC 27018:2025 Cloud Security and Privacy Controls
- CSA Cloud Controls Matrix v4.1 Crosswalk to NCA CCC-2:2024

Day 3: Implementing Tenant Controls

- Cloud Identity and Privileged Access Management with Multi-Factor Authentication
- Encryption and Key Management: Customer-Managed Keys and Hardware Security Modules
- Cloud Logging and Monitoring Integrated with Security Event Management
- Secure Configuration Baselines Using CIS Benchmarks
- Cloud Service Provider Due Diligence and Contract Security Clauses

Day 4: Risks, Gaps and Edge Cases

- Misconfiguration Detection with Cloud Security Posture Management
- Data Residency Decisions after the NCA CCC-2:2024 Localisation Changes
- Cloud Incident Response and Forensic Evidence Collection
- Exit Strategy, Portability and Backup Controls for Tenants
- Multi-Cloud and SaaS Sprawl Risk Assessment

Day 5: Case Work and the NCA CCC Compliance Plan

- Government Entity Case Study: Migration to a Commercial Government Cloud
- Critical Infrastructure Case Study: SaaS Adoption Review
- NCA CCC Tenant Control Self-Assessment for an Own Environment
- NCA CCC Compliance and Cloud Security Plan Drafting
- Peer Review Panel and Remediation Roadmap Defence

Skills You Will Gain

- Cloud Regulatory Interpretation
- Cloud Control Mapping
- Cloud Data Classification
- Cloud Identity and Key Management
- Cloud Security Configuration Review
- Cloud Provider Assurance
- Cloud Compliance Evidence Preparation

Why Attend This Course

- Return with an NCA CCC Compliance and Cloud Security Plan built on your own workloads and providers
- Distinguish clearly what your entity must evidence from what your cloud provider must evidence
- Avoid the classification, localisation and configuration errors behind many failed cloud assessments
- Compare approaches with practitioners from government, critical infrastructure and provider organisations

Conclusion

Cloud adoption under the KSA Cloud First Policy is sustainable only when each workload meets the NCA controls that apply to it and the evidence is ready. This course moves from the national cloud policy and regulatory context, through NCA CCC-2:2024 and the international standards that sit alongside it, to implementing tenant controls and handling the gaps that assessments expose. The final day produces an NCA CCC Compliance and Cloud Security Plan that participants take back to their entity as a working remediation roadmap.