CONCEPT

# NCA ECC-2:2024 Essential Cybersecurity Controls: Implementation and Compliance in KSA

**NCA ECC-2:2024 Essential Cybersecurity Controls: Implementation and Compliance in KSA**

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

## Introduction

Government entities, their companies and critical infrastructure operators in Saudi Arabia must meet the National Cybersecurity Authority's Essential Cybersecurity Controls, and the move from ECC-1:2018 to ECC-2:2024 has reset many compliance programmes. Too often, self-assessments are completed as paperwork while gaps in access, email protection and third-party controls stay open. This coreconcept KSA course equips cybersecurity and GRC managers to scope, implement and evidence ECC-2:2024 alongside ISO/IEC 27001 and NIST CSF 2.0. Participants leave with an ECC-2:2024 Gap Assessment and Compliance Roadmap.

## Course Objectives

- Determine the scope and applicability of ECC-2:2024 for an entity and its services in Saudi Arabia
- Interpret the four ECC-2:2024 domains and map their controls to ISO/IEC 27001:2022 and NIST CSF 2.0
- Implement governance and defence controls, including policies, access management, email protection and monitoring, to the ECC requirement
- Prepare a control-by-control self-assessment with evidence using the NCA assessment and compliance tool
- Prioritise remediation of gaps by cyber risk, effort and assessment exposure
- Produce an ECC-2:2024 Gap Assessment and Compliance Roadmap for approval by the authorising official

## Target Audience

- Heads of cybersecurity functions and cybersecurity managers responsible for ECC implementation
- GRC and compliance managers who prepare NCA self-assessments and evidence
- IT and infrastructure managers who own defence controls across networks, systems and identity
- Internal audit and assurance managers reviewing cybersecurity compliance
- Risk and business continuity managers linking cyber risk to enterprise risk and resilience
- Vendor and cloud service managers overseeing third-party cybersecurity obligations

# Course Outline

## Day 1: ECC-2:2024 Context and Scope in Saudi Arabia

- NCA Mandate and Regulatory Documents: ECC, CCC, OTCC and DCC
- ECC-2:2024 Applicability to Government Entities, Their Companies and CNI Operators
- ECC-2:2024 Structure: 4 Domains, 28 Subdomains, 108 Controls and 92 Subcontrols
- Changes from ECC-1:2018 and Transition Priorities
- Current-State Scoping with Asset and Service Inventory

## Day 2: ECC Domains and International Mappings

- Cybersecurity Governance Domain: Strategy, Policies, Roles and Risk Management
- Cybersecurity Defence Domain: Asset, Identity, Network, Data and Cryptography Controls
- Cybersecurity Resilience Domain and Business Continuity Aspects
- Third-Party and Cloud Computing Cybersecurity Domain
- ECC-2:2024 Mapping to ISO/IEC 27001:2022 Annex A and NIST CSF 2.0

## Day 3: Implementing the Controls

- Cybersecurity Policy and Procedure Set Drafting to ECC Requirements
- Cybersecurity Function Structure and Saudi National Staffing Requirements
- Identity and Access Management Controls: MFA, Privileged Access and Periodic Review
- Email Protection Controls Including DMARC, SPF and DKIM
- Vulnerability Management, Penetration Testing and Event Log Monitoring Cycles

## Day 4: Compliance Assessment, Evidence and Problem Cases

- NCA Self-Assessment with the ECC Assessment and Compliance Tool
- Evidence Pack Design and Control Implementation Status Ratings
- Cybersecurity Risk Assessment and Treatment per ISO/IEC 27005
- Cybersecurity Requirements in IT Projects and Change Management
- Recurring Field Audit Findings and Remediation Pitfalls

## Day 5: Case Work and the ECC Compliance Roadmap

- Government Entity Case: Control-by-Control Gap Assessment
- Utility Operator Case: Third-Party and Cloud Control Gaps
- Remediation Prioritisation Matrix by Risk and Effort
- ECC-2:2024 Gap Assessment and Compliance Roadmap Drafting
- Roadmap Defence Before a Mock Assessment Panel

## Skills You Will Gain

- Cybersecurity Control Implementation
- Compliance Gap Analysis
- Control Framework Mapping
- Evidence Management
- Cyber Risk Assessment
- Third-Party Cyber Risk Management
- Remediation Planning
- Audit Readiness

## Why Attend This Course

- Return to work with an ECC-2:2024 Gap Assessment and Compliance Roadmap for your entity, tested before a mock assessment panel
- Explain to leadership what changed from ECC-1:2018 and where the entity's effort must go first
- Reuse existing ISO/IEC 27001 and NIST CSF work instead of running a separate compliance programme
- Compare evidence approaches with managers from government entities, their companies and critical infrastructure operators

## Conclusion

ECC-2:2024 sets the minimum cybersecurity baseline that the NCA expects across Saudi government entities and critical infrastructure, and assessments now look for working controls rather than documents alone. This course moves from scope and structure, through the four control domains and their international mappings, to implementation, self-assessment evidence and the findings that recur in field audits. The final day turns that material into an ECC-2:2024 Gap Assessment and Compliance Roadmap that participants take back to their authorising official for approval and funding.