February 2025

Navigating Kingdom of Saudi Arabia's Evolving Cybersecurity Landscape:

What NCA Regulations Mean for your Business?

FOREWORD

In an era of rapid technological advancements and escalating cyber threats, robust cybersecurity frameworks have become imperative for nations to safeguard their digital ecosystems. As part of its Vision 2030 agenda, Saudi Arabia, has demonstrated a profound commitment to establishing comprehensive cybersecurity measures, central to which is the National Cybersecurity Authority (NCA).

The NCA's regulations have significantly shaped Saudi Arabia's cybersecurity posture by setting standards that address the complexities of today's interconnected world. These directives aim to protect critical infrastructure, promote trust in digital transactions, and foster an environment conducive to innovation and economic growth. Drawing on global best practices, the frameworks emphasize robust risk management, governance, and compliance, thereby nurturing a secure and resilient technological landscape. As regulatory requirements continue to evolve, organizations must proactively evaluate their cybersecurity maturity to ensure alignment with the NCA's mandates. By doing so, they not only mitigate risks and bolster their security posture but also maintain a competitive edge in an increasingly connected global marketplace.

Our perspective aims to serve as a strategic guide for organizations navigating the NCA regulations, offering insights on compliance requirements, key challenges, and industry implications. We hope these insights support businesses in aligning their cybersecurity strategies with the Kingdom's vision for a secure and thriving digital economy.

We will be happy to participate in any discussions required to clarify our views, which are enclosed in the attached publication. We look forward to hearing from you.

Abhijit Varma
Partner, Global Head of Tech Consulting

Bharat Chadha
Partner, Tech Consulting

UNDERSTANDING THE NCA: BACKGROUND AND OVERVIEW

The National Cybersecurity Authority (NCA) was established in 2017 by royal decree as Saudi Arabia's central authority responsible for cybersecurity. Its creation was pivotal in the Kingdom's efforts to enhance national security, protect critical infrastructure, and enable a resilient digital economy. The NCA governs the Kingdom's digital landscape by setting policies, issuing frameworks, and enforcing compliance.

01 Roles and Responsibilities of NCA

As the governing body for cybersecurity in Saudi Arabia, its key responsibilities include:

- Developing and enforcing cybersecurity policies, frameworks, and standards to ensure a unified and resilient approach across sectors.
- Overseeing compliance and risk management for government entities, critical infrastructure, and key organizations to mitigate cyber threats.
- Enhancing national cybersecurity capabilities by promoting awareness, training, and skill development.
- Strengthening collaboration with international cybersecurity bodies to align with global best practices and address cross-border threats.
- Supporting innovation and the cybersecurity industry by encouraging local talent, research, and partnerships with the private sector.

02 Key Cybersecurity Regulations and Frameworks by NCA

To operationalize its cybersecurity mandate, the NCA has developed a comprehensive set of regulations and controls tailored to address the unique risks faced by various industries and technological environments. These regulations establish security standards, governance frameworks, and best practices to enhance cyber resilience across the Kingdom.

The key regulatory frameworks introduced by the NCA include:

- Essential Cybersecurity Controls (ECC-2:2024) – Foundation of KSA's cyber security strategy that outlines a comprehensive set of measures from access management to incident response
- Cloud Cybersecurity Controls (CCC) – Security controls for cloud services, focusing on data encryption, identity and access management, and compliance monitoring
- Critical Systems Cyber Security Controls (CSCC) – Prioritizing protection of critical infrastructure by focusing on network segmentation, intrusion detection, and real-time monitoring of critical systems
- Organizations' Social Media Accounts Cyber Security Controls (OSMACC-1:2021) - Safeguards for organizations' social media accounts to prevent unauthorized entry, data leaks, and social engineering exploits

- Telework Cyber Security Controls (TCC) - Guidelines for secure remote working environments covering protected VPN connections, endpoint security, and safe file transfer
- Operational Technology Cybersecurity Controls (OTCC) – Provides a framework for safeguarding industrial control systems from cyberattacks
- Data Cyber Security Controls (DCC) - Governs aspects of data encryption, access management, regular data audits, and data retention policies.

A DEEP DIVE INTO THE NCA ECC-2:2024 FRAMEWORK

The NCA Essential Cybersecurity Controls (ECC – 2:2024) framework provides a structured approach for organizations to safeguard their digital infrastructure while ensuring compliance with national cybersecurity standards.

As cyber threats evolve in complexity, organizations need a strong security foundation that addresses key areas such as governance, defense, resilience, and third-party/cloud security.

Structure of the NCA ECC-2:2024 Framework

The framework is structured into:

4 Main Cybersecurity Domains

28 Cybersecurity Subdomains

110 Cybersecurity Controls

90 Cybersecurity Subcontrols

Key Domains of the NCA ECC – 2:2024

01

Cybersecurity Governance:

Establishes policies, roles, and responsibilities while promoting security awareness and training to cultivate a cybersecurity-conscious culture.

02

Cybersecurity Defense:

Focuses on strengthening security controls and proactive defense mechanisms to safeguard against cyber threats and attacks.

Cybersecurity Resilience:

Enables organizations to maintain business continuity, manage disruptions, and restore critical systems after security incidents.

03

Third-Party and Cloud Computing Cybersecurity:

Ensures secure engagements with external service providers, minimizing risks associated with third-party vendors and cloud infrastructures.

04

WHY SHOULD YOU COMPLY WITH NCA REGULATIONS?

Adopting the updated NCA ECC – 2:2024 framework offers organizations several strategic advantages, including:

- A more assertive cybersecurity posture with enhanced risk management capabilities.
- Improved regulatory compliance with evolving national security mandates.
- Optimized security operations through streamlined processes and better resource utilization.
- Greater resilience against emerging cyber threats and faster incident response.
- Enhanced trust and reputation among stakeholders, partners, and customers.

The NCA ECC – 2:2024 framework underscores the NCA's commitment to aligning with global cybersecurity best practices while addressing the unique security needs of Saudi organizations. By embracing these enhanced controls, organizations can not only safeguard their critical assets but also gain a competitive advantage in the digital economy.

WHO NEEDS TO COMPLY WITH NCA REGULATIONS?

The NCA's Essential Cybersecurity Controls (ECC) and other regulatory frameworks apply to a wide range of entities across Saudi Arabia:

- **Government entities,** including ministries, authorities, institutions, and their affiliates or subsidiaries—both within and outside the Kingdom.
- **Private sector organizations** that own, operate, or host **Critical National Infrastructure (CNI)** and other essential services.

Additionally, the **NCA encourages all entities in Saudi Arabia** to adopt these controls as best practices to strengthen their cybersecurity posture.

While the NCA's core controls set a universal foundation, specific regulations are tailored to an organization's operational environment. For instance, entities leveraging cloud technologies must adhere to Cloud Cybersecurity Controls (CCC) to ensure secure data management. At the same time, those managing critical infrastructure must implement Critical Systems Cybersecurity Controls (CSCC) for real-time monitoring and intrusion detection.

By enforcing these regulations, the NCA ensures that cybersecurity remains a top priority across public and private sectors, protecting national interests and critical services from potential cyber threats.

WHAT ARE THE PENALTIES FOR NON-COMPLIANCE?

Organizations operating in Saudi Arabia must comply with the NCA's cybersecurity regulations, which are applicable based on the sectors in which they operate. Non-compliance can result in significant legal penalties designed to enforce strict adherence to national cybersecurity standards.

The NCA conducts routine audits and assessments to monitor compliance and identify vulnerabilities requiring action. Penalties may include:

- Warnings, Temporary/Permanent License Suspension, or Service Suspension
- Fines up to SAR 25,000,000 (approx. USD 6.66 million)
- Reputation Damage through public disclosure of violations
- Mandatory Remediation of violations with any gains deposited into the state treasury

If necessary, organizations can appeal decisions to the Administrative Court within 60 days. These penalties highlight the critical need for compliance, ensuring organizational integrity and national cybersecurity.

(Source for penalties: https://www.lexology.com/library/detail.aspx?g=797020a8-810e-4ab0-9229-2a512af2120b)

HOW TO PREPARE FOR NCA COMPLIANCE?

Organizations should take proactive measures to strengthen their cybersecurity posture to ensure compliance with NCA cybersecurity regulations. Key steps include:

- Establish a robust Governance Framework: Develop guidelines by defining clear roles, responsibilities, policies, and procedures to ensure accountability, risk management, and compliance.
- Conduct Regular Risk Assessments: Identify and address potential cybersecurity risks before they become threats.
- Implement Robust Security Controls: Limit access to sensitive data by restricting access, enforce cybersecurity governance, deploy cybersecurity defense controls, and strengthen cybersecurity resilience by periodic risk assessment and third-party & cloud computing cybersecurity controls , reducing the risk of unauthorized access and mitigate misuse to critical data.
- Deploy SIEM Systems: Monitor network traffic in real-time, enabling early detection of malicious activity and faster incident response.
- Provide Cybersecurity Training: Educate employees on best practices and raise awareness about potential threats to reduce human error.
- Develop and Test Incident Response Plans: Prepare for cyberattacks by having a clear and tested plan to respond quickly and effectively.
- Stay Informed About Emerging Threats: Regularly update security protocols by staying informed on the latest cybersecurity threats and vulnerabilities.

By implementing these steps, organizations can not only comply with NCA regulations but also create a robust defense against evolving cyber threats.

COMMON CHALLENGES ORGANIZATIONS FACE IN NCA COMPLIANCE

Complying with the NCA's cybersecurity regulations presents several challenges for organizations, particularly in a rapidly evolving digital landscape. Key obstacles include:

- Complexity of Regulations: Organizations often struggle to interpret and implement evolving NCA requirements across multiple controls and frameworks.
- Resource Constraints: Many lack the expertise, tools, or dedicated teams needed for full compliance, particularly in specialized areas like cloud security and third-party risk management.
- Integration with Existing Systems: Adapting new cybersecurity controls to existing systems can be difficult, especially with legacy infrastructure or complex IT environments.
- Evolving Threat Landscape: The rapid pace of cybersecurity threats makes it challenging to keep security practices up to date.
- Employee Awareness and Training: Ensuring organization-wide cybersecurity training and awareness remains a hurdle, particularly in large, diverse teams.
- Ongoing Monitoring and Auditing: Continuous monitoring, auditing, and testing demand significant resources and effort to maintain compliance.

Overcoming these challenges requires a proactive approach, strategic planning, and, often, external expertise to ensure compliance while strengthening cybersecurity resilience.

HOW WE CAN HELP YOU NAVIGATE NCA REGULATIONS

At Uniqus, we specialize in helping organizations navigate the complexities of cybersecurity risk and compliance. Our unique value comes from leveraging AI and digital solutions, enabling us to offer cutting-edge approaches beyond traditional practices. Our innovative methods are designed to drive efficiency, enhance insights, and provide actionable strategies aligned with the evolving landscape of NCA regulations. Here's how we can assist:

- Establishing a Robust Governance Framework: We help organizations define and implement clear roles, responsibilities, policies, and procedures to ensure strong cybersecurity governance and accountability, aligning with NCA regulations.
- Risk Assessments and Gap Analysis: We conduct thorough risk assessments to identify vulnerabilities and gaps in your cybersecurity posture, aligning your practices with NCA's requirements.
- Implementing Robust Access Security Controls: We assist in designing and implementing cybersecurity controls, governance frameworks, and third-party & cloud computing security policies, ensuring that only authorized personnel have access to critical systems and data.

- Customized Compliance Roadmaps: Our team develops clear, actionable compliance roadmaps to help you ully adhere to NCA regulations, ensuring a seamless integration into your business operations.
- Cybersecurity Framework Implementation: We assist in implementing the NCA ECC – 2:2024 framework, customizing it to your organization's unique needs, whether it is cloud security, access controls, or incident response.
- Deploying SIEM Systems for Real-Time Monitoring: We provide Security Information and Event Management (SIEM) solutions, allowing organizations to monitor network traffic in real-time, detect anomalies, and respond to security threats promptly.
- Employee Training and Awareness Programs: We offer cybersecurity training to upskill your team on the latest threats and best practices, empowering your workforce to support your compliance goals.
- Incident Response and Resilience Plans: We help develop, test, and optimize your incident response and business continuity plans to ensure you're prepared for any cybersecurity threats.
- Ongoing Monitoring and Auditing: Our team provides continuous monitoring and regular audits to ensure compliance and to identify areas for improvement.
- Staying Informed About Emerging Threats: Our team provides ongoing cybersecurity monitoring and auditing, keeping you updated on emerging threats, regulatory updates, and evolving cybersecurity best practices to maintain compliance with NCA standards.

By partnering with us, you'll experience a consulting approach that blends traditional expertise with digital innovation, helping you navigate NCA's regulatory complexities while ensuring your cybersecurity posture remains resilient and future-proof.

CONCLUSION: BUILDING A RESILIENT CYBERSECURITY FUTURE

As Saudi Arabia continues to strengthen its cybersecurity ecosystem, organizations must prioritize compliance with NCA regulations not just as a legal requirement but as a strategic imperative. By adopting a proactive approach, addressing key challenges, and leveraging expert guidance, businesses can enhance their security posture, protect critical assets, and build long-term resilience against cyber threats.

In an era of constantly evolving digital risks, compliance is not a one-time task but an ongoing commitment. Organizations that embrace robust cybersecurity frameworks will not only meet regulatory requirements but also gain a competitive edge in a secure and trusted digital economy.

A TEAM THAT
YOU CAN TRUST TO DELIVER

Abhijit Varma
Partner, Global Head of Tech Consulting
av@uniqus.com

Bharat Chadha
Partner, Tech Consulting
bharatchadha@uniqus.com

Mitushi Pitti
Partner, Tech Consulting
mitushipitti@uniqus.com

Tarandeep Bindra
Associate Partner, Tech Consulting
tarandeepbindra@uniqus.com

Ellen C. Heister
Managing Director
ellenheister@uniqus.com

Anupreet Kaur
Director, Tech Consulting
anupreetkaur@uniqus.com

Hammad Malik
Director, Tech Consulting
hammadmalik@uniqus.com

Janmin Shah
Director, Tech Consulting
janminshah@uniqus.com

Kunal Gandhi
Director, Tech Consulting
kunalgandhi@uniqus.com

To know more about us, please visit *www.uniqus.com*