Understanding Cybersecurity Regulation and Compliance in Saudi Arabia: A Practical Guide to ECC-2

Post-Event Report: SBJBC x CRMG Cyber Series Webinar, 30 April 2026

Preface

The third webinar in the series will focus more closely on the risk-based approach to cybersecurity, which Rycroft identified as central to all of the Saudi regulations covered in this session. Members interested in registering should consult the events page on the SBJBC website. Those wishing to discuss CRMG's services or explore aspects of Saudi cyber regulation in greater depth are encouraged to contact CRMG through the links on the event webpage.

Summary

The Saudi British Joint Business Council (SBJBC), in partnership with Cyber Risk Management Group (CRMG), hosted the second webinar in a cybersecurity series on 30 April 2026. Led by Simon Rycroft, Co-Founder and CEO of CRMG, the session offered a practical guide to cybersecurity regulation in Saudi Arabia, with particular attention to the National Cybersecurity Authority's (NCA) Essential Cybersecurity Controls version 2 (ECC-2).

Robert McNamara, Head of Research at SBJBC, opened the session and introduced Simon Rycroft, who has spent around thirty years in cybersecurity, specialising in governance, risk, and compliance. Rycroft set the framing at the outset, treating cybersecurity risk and compliance as a business issue requiring board-level engagement and pragmatism, addressed within available resources rather than treated as purely technical work.

The International Context

To frame the Saudi position, Rycroft set out the international standards that have long shaped cybersecurity regulation worldwide. The de facto standard for many years has been ISO 27001, supported by ISO 27002 and structured around the concept of an information security management system, holistic in reach across the best-practice principles relevant to enterprise operations.

Alongside ISO sits the NIST Cybersecurity Framework, now in its second version, addressing similar territory but with a different balance, placing heavier emphasis on detection, response, and recovery. Other authoritative reference points include the Centre for Internet Security Controls and the Information Security Forum's Standard of Good Practice. Together, those broader frameworks remain the principal influences on Saudi regulation.

Newer regulation in the EU and the UK is focused more pointedly on resilience, equipping organisations to weather a serious cyber event and emerge from it, identifying critical suppliers, and reporting systemically important suppliers to regulators where they fall under direct oversight. The forthcoming UK Cybersecurity and Resilience Bill, currently progressing through Parliament, reflects this emerging theme. Resilience-focused thinking is not yet visible to the same degree in the Saudi regulatory environment, which still aligns more closely with the older holistic frameworks.

Beyond the general cybersecurity standards, AI regulation is rising, with the EU AI Act acting as a trailblazer, supported by ISO 42001 and the NIST AI Risk Management Framework. On data protection, EU and UK GDPR continues to exert wide influence, while IEC 62443 remains the principal point of reference for operational technology and industrial control systems. Even with this expanding ecosystem, the older and broader ISO and NIST frameworks remain the greatest influence on regulation emerging in the Kingdom.

The Saudi Regulatory Architecture

Saudi Arabia's cybersecurity regulatory architecture is led by the NCA and a suite of standards, all of which carry the suffix "CC" for cybersecurity controls. These include the Essential Cybersecurity Controls (ECC), the Telework Cybersecurity Controls, the Organisational Social Media Cybersecurity Controls, the Cloud Cybersecurity Controls, the Critical Systems Cybersecurity Controls, the Data Cybersecurity Controls, and the Operational Technology Cybersecurity Controls.

Beyond the NCA suite, the Personal Data Protection Law (PDPL) is owned by the Saudi Data and AI Authority (SDAIA). The Capital Markets Authority (CMA) maintains its own cybersecurity guidelines. The Saudi Arabian Monetary Authority (SAMA) issues its Cybersecurity Framework. The Communications, Space and Technology Commission (CST) maintains both the Cybersecurity Regulatory Framework and a Cloud Computing Regulatory Framework.

At the heart of this architecture sits the ECC, and although the Saudi authorities present it and the related standards as aligned with ISO 27001 and NIST, in practice little of the DNA of those international frameworks is visible in the Saudi standards, which are noticeably different on closer reading. The PDPL, by contrast, is heavily influenced by GDPR, though with a lighter touch on subject access requests and the rights of the individual, while the SAMA and CMA frameworks reflect more visible influence from ISO and NIST. The CST frameworks are light touch for non-critical organisations, although for critical organisations they refer authority back to the NCA. Most other authorities defer to the NCA at some point, reinforcing its position as the central regulator for Saudi cybersecurity.

A further point of complexity is the difference in structure, terminology, and assessment method. The SAMA framework, for instance, is assessed against a maturity scale, with level three of five generally regarded as the appropriate target. The NCA standards are assessed against control applicability: whether a control applies, and whether it is not implemented, partially implemented, or fully implemented.

A New Standard for the Wider Economy

Until recently, the NCA standards applied strictly only to two categories of organisation: government and government-related entities, and those supporting critical national infrastructure. The latter category itself covers a wide remit, including telecoms, food production and distribution, energy, oil and gas extraction and distribution, and transport. The NCA encouraged all other organisations to comply with the spirit of the standards even where they were not strictly required to.

That position has begun to shift with the publication of the Non-Critical National Infrastructure Cybersecurity Controls (NCNICC). At present, the regulation is available only in Arabic and is therefore still new to the market. It applies to organisations with more than six employees, using Class A and Class B controls to differentiate between sizes of entity. For smaller organisations the regime is relatively light touch, with similarities to the UK's Cyber Essentials scheme. The wider effect is to extend many of the principles already established in the ECC suite to a much broader segment of the Saudi economy.

Common Core Principles Across Frameworks

Despite the diversity of frameworks, terminology, and assessment methods, the underlying content of Saudi regulation is consistent. Across the standards, organisations are expected to demonstrate cybersecurity governance, including a defined strategy, board-level oversight, security policies communicated to staff, and a cybersecurity function with a Chief Information Security Officer separate from IT. The separation of powers between IT and information security has become an increasingly important principle.

Beyond governance, organisations are expected to perform cybersecurity risk assessment, understand continuity requirements when critical systems are unavailable, test business continuity plans, and know their compliance and legal obligations. Cybersecurity should be embedded across the employment lifecycle, including vetting and screening of staff in critical posts, ongoing reviews of access rights as staff move within the organisation, and prompt removal of access rights on departure. Security education and awareness programmes should be thorough and consistent.

Further core areas extend across the working environment and the supporting technology stack. They cover teleworking and remote access, physical environment controls, equipment handling for photocopiers, scanners, mobile devices and bring-your-own-device arrangements, information classification and lifecycle handling, and inventories of both physical and information assets. The technical foundations include secure systems development and acquisition, cloud configuration, protection against malicious code and intrusion, identity and access management with particular attention to privileged access reviews, encryption at rest and in transit, and immutable backups taken in as near real time as possible. Operational disciplines help build a fuller picture, and include aspects like technical vulnerability management and patching, disciplined change management, incident management and reporting, crisis management, and audit and assurance. The essential point Rycroft drew out was that, whether expressed through ISO 27001, the NIST Cybersecurity Framework, the SAMA Cybersecurity Framework, the CMA Cybersecurity Guidelines, or the NCA suite, all of these regulations address the same underlying disciplines. The differences lie in structure, terminology, and assessment approach, not in core content.

The NCA Suite in More Detail

The ECC sits at the hub of the NCA suite and represents the baseline for any relevant organisation, and layered on top of it are additional standards, each addressing a specific operational context. The Critical Systems Cybersecurity Controls apply to systems meeting a defined criticality threshold, including an impact threshold expressed as a small percentage of national GDP. The remaining standards address cloud services (split between tenant and provider controls), data, teleworking, organisational social media use, and operational technology.

A particular feature of the NCA suite is its common structural approach, since each standard uses the same set of headline domains and subdomains, covering governance, defence, resilience, and third-party supplier security. The principal exception is the Data Cybersecurity Controls, which omit the resilience domain on the basis that resilience is more concerned with structural recovery than with the flow of data. There are also occasional subdomains specific to certain standards, such as a subdomain in the Data Cybersecurity Controls for printers, scanners, and copying machines. With those exceptions, the consistency of structure across the suite allows the various sets of controls to be aggregated into a single repository for use during compliance assessments.

The internal structure of each subdomain follows a recognisable pattern across the NCA suite. The first control sets out the requirement for a programme covering the area in question, including documentation, approval, and communication of requirements, and the second control requires implementation. A series of supporting controls then specifies the content to be included, the audiences to be addressed, and other detail, with the final control requiring periodic review. Once the model is recognised, the structure of each subdomain becomes easier to interpret.

Two further structural features are also worth a mention, each adding a vertical dimension to the controls within particular standards. The Operational Technology Cybersecurity Controls distinguish between three levels of facility criticality, with each control applying to a different combination of levels and the NCA in some cases assigning the relevant level directly. The Data Cybersecurity Controls draw an equivalent distinction by data classification, with the classification levels themselves defined by SDAIA. In both standards, the practical effect is that controls apply across both a horizontal subject matter and a vertical dimension of system or data type.

Interpretation and Complexity

While the NCA suite is comprehensive and broadly well-structured, its drafting is at times difficult to interpret. Rycroft illustrated the point with a control from the ECC requiring cybersecurity requirements to be included in project management methodology and procedures, and in information and technology asset change management, in order to identify and manage cybersecurity risks across the technology project lifecycle. A further clause within the same control treats cybersecurity requirements as a key part of technology project requirements overall. Although the intent of such controls is generally discernible, the precise meaning is not always easy to extract in a single reading.

The NCA produces additional implementation guidance for most of its standards, but the guidance does not always align cleanly with the underlying intent of the core control. Updated requirements introduce further complexity. An earlier version of the ECC required multi-factor authentication for users accessing external web applications. The updated control instead requires user authentication methods, the relevant authentication factors and their numbers, and authentication techniques to be defined based on the result of an impact assessment of authentication failure and bypass. In practical terms, the requirement is to align authentication methods with risk assessment, but the wording does not make this immediately clear. These interpretive challenges are particularly relevant where compliance is ultimately tested through engagement with the regulator. Organisations approaching the standards for the first time should anticipate the need to interpret controls actively and be ready to defend their interpretations through audit.

Pragmatic Approaches to Compliance

Rycroft framed compliance as a question of circumstance, with organisations needing to understand whether they are regulated in the strict sense, their risk profile, the services they offer in Saudi Arabia, their wider compliance obligations, their cybersecurity maturity, and the resources available to them. Compliance, on this reading, is best understood as a journey rather than a binary status.

For organisations strictly within scope, the path is comparatively narrow and the work proceeds through a defined sequence of steps. Each applicable control must be identified, converted into actionable items, and assessed against current practice in a gap assessment, and an improvement programme then addresses the gaps and monitors progress. With well over six hundred controls across the NCA suite when all standards are taken into account, an organisation will be required to assess itself against the standards and to submit those self-assessments to the NCA, which reserves the right to audit. Penalty exposure reaches up to 25 million Saudi riyals where regulatory expectations are not met.

Where organisations are not strictly regulated, there is greater flexibility in the choice of starting framework. In Rycroft's view, the NCA suite is not necessarily the easiest starting point for a smaller business technically outside the regulated population. ISO 27001, the NIST Cybersecurity Framework, the CMA Cybersecurity Guidelines, or, for very small organisations, Cyber Essentials in the UK, offer more accessible drafting and the same underlying principles. Whichever starting point is chosen, the structure remains the same: identify controls, identify gaps, fill the gaps in a structured manner, and manage maturity uplift over time.

Across both regulated and unregulated routes, a consistent set of practices applies. A risk-based approach is required to identify applicable controls, and cyber strategy and compliance must be treated as a business issue rather than an IT issue. Everything should be documented: strategy, plans, policies, procedures, risk registers, agreed risk acceptances, contractual requirements, and service-level agreements. Evidence is critical, covering board minutes where cybersecurity is discussed, awareness training records, event logs, incident management processes, and post-incident reviews. Communications with staff, the public, the regulator, and emergency services should be planned and consistent, while compliance should be monitored over time, in the expectation of incremental improvement.

The Risk-Based Approach

A risk-based approach underpins both regulated and unregulated routes to compliance, since the Saudi regulations require organisations to understand their threat profile, recognise their systemic importance within their sector, identify risks, and shape their control structures accordingly. In Rycroft's view, the risk-based requirement in Saudi regulation sits somewhat lighter than in equivalent European regimes overall, although for organisations deemed critical to national infrastructure there is rather less wiggle room. The principle nevertheless holds: understanding what is critical, what is less critical, performing risk assessments, recognising the impact on the organisation if a critical system were to be compromised, and applying controls accordingly. The next webinar in the series will focus on this in greater depth.

Tools for Managing Compliance

Because the NCA standards share a common structure, the controls have been collected into a single repository, filtered by domain and subdomain, and translated into plain English. CRMG has performed this work, mapped each control to ISO 27001, captured the three OT levels and the data classification levels from the relevant standards, and filled certain gaps where ISO expresses a control the NCA suite does not.

For larger organisations and those carrying multifaceted compliance obligations, technology becomes important to the mechanics of the work, typically through a governance, risk, and compliance (GRC) platform able to support compliance at scale. CRMG works with Diligent, although alternatives exist. Where organisations face complex multi-jurisdictional requirements, including the Dubai Information Security Regulation, the NCA ECC, the NIST Cybersecurity Framework, DORA for financial entities in Europe, and the forthcoming UK Cybersecurity and Resilience Bill, the value of a unified control set increases. A harmonised approach reduces overlapping work and clarifies obligations through a common, principle-based control library aligned to multiple regulations.

AI in the Compliance Process

Asked whether AI would or could accelerate the harmonisation work itself, Rycroft was cautious about the current state of the technology. In his experience, and from his observation of attempts by other respected organisations, AI is not yet able to interpret controls reliably across regulatory contexts. Each control sits within a principle-based environment, and AI struggles to read this kind of context accurately when drawing equivalence with controls in another jurisdiction. The position will likely change in time, but at present AI is not the answer.

Closing Reflections

Saudi cyber regulation is broadly consistent with regulation in other jurisdictions in the disciplines it addresses, even where the NCA takes a non-typical approach in its drafting and structure. The Non-Critical National Infrastructure Cybersecurity Controls extend the NCA's reach substantially into the wider economy and deserve close attention as the English translation and supporting guidance become available. Compliance is not a binary state but a maturity journey that must be continually managed and revaluated like any other strategic initiative.

Pragmatism is essential, with efficiencies to be found by taking a unified approach, by consolidating and filtering controls, and by translating dense regulatory wording into plain, actionable points. Maturity will improve over time, and above all, organisations should document and evidence everything, since internal auditors, board members, and the regulator might at any point require evidence of compliance.