

Insights

WHEN COMPLIANCE CREATES FRICTION: NAVIGATING CYBERSECURITY REQUIREMENTS IN COMMERCIAL RELATIONSHIPS

Oct 27, 2026

Saudi Arabia's cybersecurity and data governance frameworks continue to shape how organizations procure technological solutions, engage service providers and manage third-party relationships. One practical consequence, and subject of this article, is that compliance with cybersecurity legal framework by a party may affect another party's ability to deliver contracted services and, in some cases, impact the ability of all contracting parties to fully benefit from those services. This may result in delays, additional compliance reviews, technical workarounds or operational constraints that were not anticipated at the outset of the contractual relationship. The issue is not necessarily that a particular service or arrangement is inherently prohibited, but rather that compliance controls may inevitably introduce restrictions or technical limitations which may, therefore, require careful navigation by all parties.

Compliance in practice

Saudi Arabia's Essential Cybersecurity Controls (ECC) apply to all government agencies and private sector entities owning, operating or hosting Critical National Infrastructure (CNI). CNI is defined in the ECC as:

"Essential elements of infrastructure (i.e. assets, facilities, systems, networks, processes, and key personnel who operate and process them) whose loss or compromise may result in

- *Significant negative impact on the availability, integration, or delivery of basic services, including services whose integrity could, if compromised, result in serious loss of property, lives, and/or injuries, taking into account significant national-level economic and/or social impacts.*
- *Significant impact on national security, national defense, and/or State economy or national capacities."*

The CNI ECC are expressly framed as minimum requirements, with entities in scope (i.e., owning, operating or hosting CNI) required to take continuous measures to ensure ongoing compliance. For

activity outside the context of CNI, the National Cybersecurity Authority (NCA) has issued a separate mandatory baseline — the Non-CNI Private Sector Entities Cybersecurity Controls (NCNICC-1:2025). This means that the determination of CNI and then determination of the applicable ECC or NCNICC is relevant across the private sector as a whole.

In practice, cybersecurity standards issued by the NCA — including the Critical Systems Cybersecurity Controls (CSCC) — require that network design and settings must not allow technical support from outside the Kingdom for critical systems, whether connected to the internet or not. In other words, a service that works everywhere else may still require adjustment before a customer's cybersecurity team clears it for use.

Early engagement is key

Cybersecurity compliance should therefore be viewed not only as a regulatory consideration, but also as a practical commercial issue that may influence how services are delivered and the associated cost. For customers and their Saudi service providers, this means recognizing that internal cybersecurity requirements can affect them at the procurement, bid and implementation stages. For service providers, it also means understanding that its legal compliance alone may not guarantee operational acceptance within a customer's cybersecurity environment.

Early engagement between legal, commercial, technical and cybersecurity stakeholders can help identify potential issues before implementation. This is not merely good practice — the NCA's own framework requires cybersecurity risk assessments at the early stages of technology projects and mandates that third-party contracts include the customer's cybersecurity requirements and the supplier's compliance obligations.

As cybersecurity governance continues to evolve, organizations that proactively address these issues — at the contracting stage, through appropriate due diligence, and by fostering open dialogue between technical and commercial teams — will be better positioned to deliver projects efficiently while maintaining compliance and managing risk.

Meet the team



Othman S. Alshmry

KSA Managing Partner, Al Khobar /
Riyadh

othman.alshmry@bclplaw.com

[+966 13 817 9335](tel:+966138179335)



Samuel E. Eversman

Partner, Al Khobar / Riyadh

sam.eversman@bclplaw.com

[+966 53 437 4777](tel:+966534374777)



Muhammad Hassan

Associate, Al Khobar

muhammad.hassan@bclplaw.co

[m](#)

+966 13 817 9335



Marcus Pearl

Partner and Global Practice Group
Leader – Technology, Commercial &
Data, London

marcus.pearl@bclplaw.com

+44 (0) 20 3400 4757

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.