Saudi Arabia’s draft Cloud Cybersecurity Controls

Nick O’Connell - Partner, Head of Digital & Data - Saudi Arabia - Digital & Data
n.oconnell@tamimi.com - Riyadh

Saudi Arabia’s National Cybersecurity Authority (‘NCA’) is responsible for addressing the strategic and regulatory needs of the Kingdom in so far as cybersecurity is concerned. This includes aspects such as the development of policies, governance mechanisms, frameworks, standards, controls and guidelines.

The uptake of cloud services will continue to increase across the globe, and the popularity of cloud-based solutions in Saudi Arabia shows no signs of abating. As a result, the NCA has identified a pressing need to ensure that there are cloud-focussed mechanisms for addressing cybersecurity risks in a cloud computing context.

In mid-February 2020, the NCA issued the draft Cloud Cybersecurity Controls (CCC-1: 2020), as a proposed extension to the application of its Essential Cybersecurity Controls 2018 (ECC 2018). (One criticism of the ECC 2018 has been that it contains a general prohibition on the use of cloud services hosted outside the Kingdom, without any further nuance.) A public consultation period followed, inviting interested parties to make submissions. In this article, pending the outcome of the consultation process, we provide brief observations on the CCC-1:2020 in its originally published form.

Application

The CCC-1:2020 is intended to reduce cybersecurity risks for both cloud service providers and cloud customers.

As drafted originally, CCC-1:2020 will apply to Saudi government entities (including ministries, authorities, establishments, and others) and their companies and entities, as well as private sector entities owning, operating or hosting critical national infrastructure.

Cloud service providers and cloud customers that are subject to the ECC:2018 will be required to implement CCC-1:2020. This point raises some questions, as the ECC:2018 does not appear to apply directly to cloud service providers that are not government entities or critical national infrastructure providers.

The CCC-1:2020 is drafted to apply to cloud service providers, inside or outside the Kingdom, that provide cloud services to cloud customers who are subject to CCC-1:2020. (It does not apply to such cloud service providers in so far as they also provide cloud services to customers that are not subject to the CCC-1:2020).

Consistent with the more general ECC:2018, the CCC-1:2020 also contemplates other entities, not strictly subject to CCC-1:2020, complying with the CCC-1:2020 requirements as a means of adopting best practices and enhancing cybersecurity.

Cloud-specific Cybersecurity obligations

As defined in the draft CCC-1:2020, cloud computing is more than just operation of data centres. It includes Software as a Service (‘SaaS’), Platform as a Service (‘PaaS’) and Infrastructure as a Service (‘IaaS’); and it contemplates private, community, public and hybrid cloud models. A cloud service provider is defined as anyone who provides cloud services to the public (presumably this means ‘to others, on a commercial basis’, rather than to ‘members of the public’ per se), either directly or indirectly, through data centres (both inside and outside Saudi Arabia), and who manages them in whole or in part. A cloud customer is anyone who subscribes to cloud services provided by such a cloud service provider.

According to the original draft, cloud customers subject to CCC-1:2020 will be required to contract only with licensed cloud service providers. This could refer to cloud service providers holding a Saudi commercial registration, although we cannot rule out the possibility that it may refer (in limited circumstances) to local and foreign cloud services providers registered with the Communications and Information Technology Commission (‘CITC’) pursuant to the CITC’s Cloud Computing Regulatory Framework.

The provision of cloud services to cloud customers subject to CCC-1:2020, as drafted, will need to be governed by Saudi laws and regulations. Cloud service providers will need to consider all laws and regulations relating to cybersecurity in Saudi Arabia, and to comply with the applicable controls, guidelines, frameworks and regulations for cybersecurity at the relevant level; and cloud customers are required to verify such compliance.

Additionally, the draft contains a requirement to comply with the data classifications of the National Data Management Office (‘NDMO’). Exactly what this will entail is unclear at this point, as the NDMO has not yet (as far as we are aware) issued any such classifications.

Broad data classifications as contemplated in the draft CCC-1:2020 are as follows:

Level	Application
1	Applies to data classified as 'top secret', based on what is issued by 'the relevant government entity' (presumably, the NDMO).
2	Applies to data classified as 'secret', based on what is issued by the relevant government entity.
3	Applies to data classified as 'restricted', based on what is issued by the relevant government entity. (Level 3 is the lowest level for hosting sensitive systems and data).
4	Applies to data classified as 'open', based on what is issued by the relevant government entity.

According to the draft, cloud service providers will need to provide cloud computing services from within Saudi Arabia. This requirement extends to all systems used, including storage, processing, monitoring, support, and disaster recovery. The CCC-1:2020 also requires them, to the extent required by Saudi law, to use telecommunications infrastructure, including connectivity points, provided by operators licensed in Saudi Arabia. (The wording of this provision is unclear; rather than imposing an obligation, it could be read simply as highlighting the need to comply with any such requirements as may be imposed pursuant to other laws or regulations.)

Cloud service providers are prohibited from complying with any non-Saudi laws that may conflict with obligations imposed by Saudi laws with regard to cybersecurity and the treatment of data under their control. In the event of any direction apparently in conflict with this requirement, that might result in the disclosure of data held in Saudi Arabia, the cloud service provider is required to notify the Saudi authorities promptly.

Cloud service providers are required to provide, to the NCA, an annual report (updated in the event of material changes in the interim) reflecting the technology, features and controls related to the cloud service provider's ability to access or decrypt (directly or via a third party) any cloud customer data.

What next?

It is possible that the draft CCC-1:2020 will be revised as a result of feedback that CITC receives as part of its public consultation process. Cloud customers and cloud service providers need to monitor developments in this space, to ensure that they can accommodate the potential impact of these cloud-focussed cybersecurity requirements.

For further information, please contact Nick O'Connell (n.oconnell@tamimi.com).