# DORA series episode 1:

## Implications for financial entities

Heenal: Welcome to the first episode in the Allen & Overy podcast series on the European Union's Digital Operational Resilience Regulation, known as DORA. Our two-part series looks at the implications of DORA for both financial institutions and technology providers. I'm Heenal Vasu, a Senior Professional Support Lawyer in Allen & Overy's Financial Regulatory Practice, and in this first episode I'm joined by Nikki Johnstone, a Senior Associate in our practice, and Tom Anderson, an Executive Director at A&O Consulting. We're going to discuss the changes that DORA will bring to the financial sector across Europe, and some of the practical steps that firms can take to prepare. But first, Tom, digital operational resilience should already be a familiar concept to those firms operating in the financial services arena, isn't that right?

Tom: You're absolutely right. Digital operational resilience is, at its core, about how firms manage the risks inherent to their IT systems and use of third party service providers, and how they respond to IT incidents in order to protect themselves and their customers. DORA is intended to be the single source of digital operational resilience rules for all financial institutions in the EU. It consolidates disparate existing rules and guidance already applicable to some firms, such as banks, payment institutions and insurers. Others, like those in the investment funds sector, financial market infrastructures and cryptoasset service providers, may not have been subject to any such rules until now. So whilst it's important for all firms to understand what DORA requires, some will have more work to do than others to establish compliant systems and processes.

Nikki: Yes, and what this consolidation does is bring together not only different segments of the financial sector under a single regime, but it also dovetails with the separate sets of rules governing outsourcing, ICT risk management and incident reporting that many firms are currently subject to.

Heenal: Thanks very much, Nikki and Tom. So with firms already having to grapple with a large number of complex rules and guidelines, maybe DORA will make life easier for some firms, or am I being too optimistic?

Tom: Well, the rules might be easier to find, but DORA will require all firms to make changes to their approach to digital operational resilience, including IT operations and contractual arrangements. DORA is concerned with all ICT services, which it defines broadly to mean "digital and data services provided through the ICT systems to one or more internal or external users". So this covers data entry, storage, processing, monitoring and reporting services, as well as data-based business and decision support services. The range of a firm's activities which will be governed by DORA could also be expansive.

Heenal: So, Nikki, which activities and operations does DORA cover?

Nikki: Well, DORA is split into roughly four parts; it has obligations on IT risk management, reporting of IT-related incidents, digital operational resilience testing and, finally, managing third party IT risk. There are also obligations for certain critical IT service providers, but we'll talk about those in episode two.

Heenal: Thanks, Nikki. So, Tom, let's start with IT risk management. What do firms need to do in this regard?

Tom: Well, all financial institutions will now need to implement an IT risk management framework, and DORA sets out requirements on how these must be documented, implemented and supervised, and it also requires audits and reviews. So the framework should perform a number of functions – it should identify the firm's IT-related business functions and overall exposure to IT risk, set out how the firm will prevent IT incidents from occurring and detect any that do, and plan for how such incidents will be responded to and learned from. DORA requires most firms either to employ a dedicated IT risk officer, or designate a member of senior management, to be responsible for overseeing implementation of the IT risk management framework.

Heenal: Thanks, Tom. This is a particularly interesting development. Nikki, may you expand upon what the IT risk officer will be responsible for.

Nikki: Sure. This appointment will be responsible for the firm's contracting with IT service providers; that's a topic we'll address shortly, but also for reporting IT-related incidents. Now all firms will now have to report major IT-related incidents to their competent authority, and DORA sets out a template for how these reports should be made. Reports should include all the information necessary for the competent authority to determine the significance of the incident and assess possible cross-border impacts. Now some firms, like banks or payment service providers, will already be familiar with the obligations to file initial incident-related notifications within the same business day on which the incident occurs, followed by intermediate reports weekly, update notifications if there are any relevant developments, and then a final report with root cause analysis of the incident. Even stricter requirements are going to apply in relation to major ICT-related incidents which occur very near to the end of the business day; this means you'd have to make a report within four hours of the next business day. Less familiar, however, may be the obligation in DORA that firms inform any clients and service users if the incident has or may have an impact on the financial interests of service users and clients without undue delay following the incident. This looks quite similar to the types of obligations which firms have under GDPR to notify customers of a breach impacting their personal data.

Tom: Yeah, and an important point here is that reporting properly is as important as managing the IT risks in the first instance. So when we see significant fines given by the FCA for IT breaches, for example, it's common for the justification to refer to the firm's failure to report in good time alongside its failure to detect the incident itself. So the obligation to inform clients and service users without undue delay could, for many firms, involve a significant communications operation, so being ready for this in advance is really important.

Heenal: Thanks very much, Tom and Nikki. But, as we know, of course, prevention is always better than cure, so let's talk a little about DORA's provisions on digital operational resilience testing. Nikki, may you explain in a little detail what these provisions cover and the key elements which firms need to be aware of.

Nikki: Yes, sure. DORA requires all firms to test their digital operational resilience at least annually, and lists the appropriate tests which you can use. Now testing should be conducted by an independent party, although that can be an independent unit within the regulated firm as well as a third party provider. A firm's IT risk management framework should ideally set out which tests will be carried out and explain why these tests are proportionate to the firm and its IT risk exposure. There is a strong emphasis from the ESAs (European Supervisory Authorities) on ensuring that this proportionality principle is embedded throughout DORA's implementation.

Tom: Absolutely, Nikki. This proportionality principle should mean that firms identify and address the IT risks that are most relevant and pertinent to their business type, without requiring them to shoulder an excessive compliance burden. It also means that larger financial services firms will have to ensure that their governance, risk management, business continuity testing and response and recovery plans meet DORA's expectations. Further, there is an additional requirement for significant financial institutions to incorporate threat-led penetration testing as part of their programme. DORA requires the relevant European supervisory authorities to develop regulatory technical standards setting out exactly what threat-led penetration testing should involve, so we can expect these to follow DORA's passage into law.

Heenal: Thanks very much, Tom. So, Nikki, another important area of DORA, and one that many firms will be more familiar with, is outsourcing. Turning to this, may you explain the obligations on firms in relation to their third party IT risk?

Nikki: Yes, thanks, Heenal. There are essentially two limbs to firms' obligations in relation to their third party IT risk. The first limb requires firms to document, implement and report on an IT third party risk strategy. Again, employing the proportionality principle, this strategy should set out the firm's sources of IT third party risk, the functions it can outsource and those it will not. Firms will have to report annually to their competent authority on their use of third party IT services, and will also need to maintain a central register of information on all their contractual information and arrangements related to outsourced IT services. We can also expect regulatory technical standards, with standard templates for the register of information.

Tom: Absolutely, Nikki, and an interesting new obligation in DORA is that, before a firm contracts with any service provider for IT services, it must now assess the risks that sub-contracting could pose to its effective oversight of the service provision, as well as the possible concentration risk of outsourcing to certain providers. So concentration here means contracting with a service provider that cannot easily be replaced in the market, as well as having multiple contracts for different services with the same provider or closely connected providers.

Nikki: Yes, that's right. The Commission is clearly now concerned that many financial institutions across the EU are relying on a relatively small number of IT service providers to deliver parts of their operations. An associated concern is that IT services are being contracted outside the Union. To that end, DORA requires that firms' assessment of IT service providers in third countries include the jurisdiction's rules on data protection and insolvency, the effective enforcement of law and any constraints there could be on urgently recovering data. Finally, DORA prohibits outsourcing to third country service providers that would, if they were located in the EU, be subject to DORA's designation as a critical IT service provider. But that designation, and its implications for service providers, is the subject of our next episode!

Heenal: Thanks very much, Nikki. And, Tom, how about the second limb of a firm's obligations on third party IT risk; may you expand on this.

Tom: Well, this concerns the form and content of outsourcing contracts. For each IT service contract that a financial institution enters into, it must have a single written document describing the services, including full service level descriptions, stating when any sub-outsourcing will take place, where the services will be performed and where data will be processed. It should set out the IT security measures that will be in place, and how personal data will be accessed, recovered and returned to the firm. The contract must include monitoring rights for the financial institution and its competent authorities, as well as robust termination provisions in the event that things go wrong.

Nikki: It's important to note at this point that these contractual requirements apply to any third party IT service provisions. The European Banking Authority guidelines on outsourcing, which credit institutions, payment institutions and others must currently comply with, do require that all outsourcing be governed by a written agreement. But they set out prescriptive rules on outsourcing only where a critical or important function is concerned. DORA applies an equivalent set of prescriptive rules, but to all contracts involving provision of IT services.

Heenal: So, Nikki, what does this mean for firms in practice? Are these contracting requirements forward-looking or do they apply to existing arrangements?

Nikki: That's a good question. DORA isn't explicit on this point, but there's no indication that the rules apply only to new contracts. So, in practice, financial institutions will need to review their existing contracts with IT service providers to ensure they include the stipulated content. Given the breadth of the definition of IT services that DORA adopts, firms may have to reassess contracts that they hadn't previously regarded as 'outsourcing', and renegotiate them to address any gaps. They'll, of course, have the bargaining power, in that there'll be a clear regulatory imperative which drives their negotiating positions, but this could clearly have other commercial implications.

Tom: And that might not be the only contractual cost. Again the point isn't addressed explicitly, but DORA sets an expectation that firms may not appoint third country IT service providers from outside the EU if those providers would be designated as critical were they established in the EU. Subject to the views of the ESAs this could mean that firms would be forced to bring to an end their relationships with some third country providers.

Heenal: Thanks, Tom, that's absolutely correct, although presumably firms might be able to novate their IT contracts so that they're delivered by the services provider's EU entity instead. But of course they'll still need to carry out the concentration risk assessment you mentioned, so they may need to go back to the market for some services, or deliver them in-house instead. But, Tom, what other practical issues should firms be thinking about?

Tom: DORA isn't likely to become law for at least another year or so but, in my experience, it's impossible for any complex organisation to know how long a compliance-led build-out will take definitely until they start identifying the gaps in their existing framework. So, unfortunately, the gap analysis can also take significant effort, and DORA, as we discussed, will have different implications for different firms and different types of firms, so this is largely dependent on the rules they current comply with and their own risk appetite. AIFMs and ManCos, for example, may have a lot of work to do given they aren't currently subject to heavy IT risk management or outsourcing rules. Depending on the size of the firm's compliance function, this extra work may fall on a few staff and therefore take longer to drive through to completion.

Nikki: Yes, that's a good point, and it's relevant really to those younger financial services firms and cryptoasset service providers who are sometimes just contemplating the idea of becoming regulated who may be at an early stage in the development of their compliance procedures but may have more limited resource to update those procedures and contract to these new standards.

Heenal: And what happens if they fail to do so?

Tom: So the question likely to be on everyone's mind is "Will my form have to pay a fine for not meeting all these new requirements?" Well, recent EU directives, such as GDPR, have mandated penalties for non-compliance by reference to a percentage of global revenue, but DORA isn't so precise when it comes to non-compliance by financial entities. The ESAs will have the power to impose financial penalties, and we've seen from a joint letter on 9 February that they are keen to have far greater involvement in follow-ups and enforcement at an EU level in relation to critical third party providers. DORA also allows them to order firms to cease and desist from certain conduct or business practices, take data traffic from telecoms operators in order to investigate breaches and to issue public warning notices about firms and the individuals who manage them. All this is without prejudice to domestic regulators' own powers to issue administrative or criminal penalties to firms and individuals. So as to the size of financial penalties…well, we'll have to wait for more guidance on that. But why don't we think of ending on a positive note?

Nikki: Yes, OK. Well, one final provision of DORA that we haven't mentioned requires financial institutions to share data amongst themselves if it contains cyber threat information and intelligence. The balance between their data protection obligations and the need to prevent cyber-attacks has been a tricky one for financial institutions to strike, but hopefully DORA will enable firms to share more data and strengthen their resilience to these attacks.

Tom: Yes, that's an area in which we may see very positive developments in the near future, I'm sure.

Nikki: Exactly!

Heenal: Nikki, Tom, thank you both very much. That brings us to the end of this episode. As ever, if those listening have any questions about DORA, or any questions on what you would like us to cover in future podcasts, then please do contact us by phone or email. And do please also tune in for episode two, which will cover the obligations in DORA for certain critical IT service providers. So all that remains to be said is thanks very much for listening.

# Speakers

**Tom Anderson**
Executive Director
A&O Consulting
Tel +44 20 3088 6435
tom.anderson@allenovery.com

**Heenal Vasu**
Senior PSL
Fintech & Payments
Tel +44 20 3088 1447
heenal.vasu@allenovery.com

**Nikki Johnstone**
Senior Associate
Fintech & Payments
Tel +44 20 3088 2325
nikki.johnstone@allenovery.com