Dubai Financial Services Authority

REGTECH LIVE

16 June 2021

Justin Baldacchino, Managing Director, Supervision

The DFSA's Supervisory Priorities

Good afternoon and welcome to this 3rd edition of RegTech Live: Driving Compliance through innovation. As a principles-based regulator with a risk-based approach, our primary goal is to reduce risk and that is why we began hosting RegTech Live. The objective of this series is to drive awareness of the RegTech solutions that are available to assist Firms in mitigating risk.

Today, in addition to seeing demonstrations from a number of third-party providers, you will hear about some of the areas that are within the focus of DFSA's 2021-2022 supervision risk lens, and our priorities in addressing these risks. In the few brief moments I have with you, and understanding this is a session focused on technology-enabled services, I'll share our views on supervision in the context of innovative financial technologies.

Before I begin, I'll make one very important point. No matter the technologies deployed or the products or services offered, our core regulatory objectives continue to be to maintain financial stability, the integrity of the market, and the protection of clients. Technology may change how we view risk, but no amount of technological innovation will change our underlying objectives. It is this view of risk that drives our supervisory priorities. I will touch on a few key aspects of technology risk and our supervisory priorities in this area.

Over the next 10 minutes, you will hear me say the word "risk" many times. It's not because I particularly like the word, though I did spend most of my career managing risk on the private side, it's because assessing risk is the core of the work we do at the DFSA.

New technologies bring many promises. Some promise to disintermediate conventional capital market models; some promise to bring more speed and transparency to payment and transaction flows; some promise simple operational efficiencies. Technological innovations in compliance processes promise to reduce false positives in transaction monitoring and manage compliance with cross-border regulations; and others promise to reduce and manage risk more efficiently. The promise to reduce and more efficiently manage risk is music to a regulator's ears. But I would be remis if I didn't turn the music down and remind everyone that for every risk a new technology mitigates, a new risk is created. And that is where we will focus our efforts going forward - where an institution implements a new technology or innovative product or service, we will look to ensure the risks associated with that new technology, product, or service are effectively identified, assessed, mitigated, and continually monitored. And where an organisation outsources its

Level 13, The Gate, PO Box 75850, Dubai, UAE
Telephone: +971 (0)4 362 1500
Fax: +971 (0)4 362 0801

technology needs to a third-party provider, we will look to see that the Authorised Firm takes appropriate steps to mitigate the risks of the third-party vendor.

Third party risk is steadily moving higher on our risk register and we are steadily increasing our focus on how well Firms manage and monitor third party risk. Unfortunately, we all too often find that Firms outsource a function to a vendor under the belief that the vendor has now taken the responsibility for that function and all of the processes and controls that go with it. That's not exactly how it works. You can outsource the function, but you always maintain the responsibility for it and you hold responsibility for the actions of the third-party vendor. Therefore, we will look to see that Firms conduct proper due diligence on their vendors. We will look to see that Firms understand how their service providers control their own technology and cybersecurity risk. And we will look to see that Firms have processes in place to conduct ongoing monitoring and periodic reviews of their vendors' cybersecurity controls.

You don't have to look too far into history to understand the risk third party providers present to your organisation. Last week, the cloud computing services provider, Fastly, caused a 49-minute shutdown of the websites of PayPal, The Financial Times, the Guardian, The New York Times, the BBC, as well as the UK Government website, and two major U.S. retailers Amazon and Target, to name a few. Eight weeks ago, SolarWinds was attacked and malicious code was injected into the systems of 18,000 of the businesses that use its services. These included government agencies, Microsoft, cybersecurity vendors, and numerous Fortune 500 companies. What made this hack unique was that the malicious code was embedded in a software update that was distributed to SolarWinds's clients. Installing updates is one of the most basic ways in which we better protect our systems; so, what do you do when the updates become the delivery mechanism for the attack? That's a very good question! And we will be looking to see how Firms address this risk.

A key point about this. The SolarWinds attack was not an attack vector that was widely contemplated. But now that we know how such an attack can happen, we expect Firms to learn from it and we do expect it to be something that is more widely contemplated going forward.

We are seeing increased adoption of a number of enabling technologies such as APIs, cloud computing, biometrics, big data analytics and artificial intelligence, and distributed ledger technologies. Each of these technologies carries unique risks and each requires bespoke risk controls.

In response to this rapid adoption, and in collaboration with the UAE Central Bank, The Securities and Commodities Authority, and the ADGM FSRA, we recently issued "Guidelines for Financial Institutions adopting Enabling Technologies." The Guidelines consist of high-level principles and best practices for Firms that are considering adopting, or have already adopted, enabling

technologies. The Guidelines were produced to encourage the safe and appropriate adoption of these technologies so that risks arising from their adoption are appropriately addressed and managed. We expect firms to apply the Guidelines in a proportionate manner that reflects the size and complexity of their business, and the nature, scope, complexity and materiality of the activities undertaken. That said, the Guidelines do not create new obligations for Firms. However, Firms should expect the DFSA to refer to the Guidelines when discussing relevant issues and when conducting risk assessments. In due course, the DFSA may include some, or all of the Guidelines, in its Rulebook, in which case the obligations created would need to be adhered to in the same way Firms would adhere to any other DFSA administered Law and/or Regulation.

I encourage all Authorised Firms to read and familiarise themselves with the Guidelines. And although we have already published the Guidelines, Authorised Firms have the opportunity, until the end of June, to review the Guidelines and submit comments to the CBUAE. You can view the SEO Letter of the 2nd of June on the DFSA website for details on how to submit comments.

I'll now mention a couple of specific risks.

The first is cyber risk. You can't use technology without exposing your business to cyber risk. For that reason, over the past two years, we have put a great deal of time and effort into driving cyber risk awareness and setting expectations for how Firms should be managing this risk. In September 2019, we activated the cyber incident notification mechanism on the DFSA ePortal; in January 2020, we launched the DFSA cyber threat intelligence platform (TIP); in June 2020, we published the findings report from the cyber risk thematic review; in December 2020, we published Cyber Risk Management Guidelines; we've held several cyber risk focused roundtables; and two days ago, we held our third cyber threat intelligence workshop.

I'll touch for a moment on the Cyber Risk Guidelines. The Guidelines explain our expectations regarding the governance, hygiene, and resilience measures firms should have in place to manage cyber risk and we will us these Guidelines to guide our cyber risk reviews. This publication should be considered a first step. We will issue more enhanced guidance as the scale of activity and the overall cyber maturity of the centre grows. For the past two years, we've focused on generating awareness and setting expectations. Now we are shifting our focus to monitoring and testing Firms' cyber risks and controls. This year we began conducting cyber-focused risk assessments of a group of Authorised Firms. Each year, we will select a different group of Firms for the purpose of assessing how well firms have responded to the findings of the thematic review and have begun to implement the Cyber Risk Management Guidelines.

Consistent with the Cyber Risk Management Guidelines, we will be looking at the Firms' cyber risk governance arrangements and the involvement of senior management, hygiene practices, and most importantly, we will review how well each Firm is prepared to identify, respond to, and

recover from a cyber incident. You have heard us say this every time we talk about cyber risk, and you will continue to hear us say it…a cyber incident is not a matter of "if," it's a matter of "when." As technologies advance, so do the criminals committed to attacking them; therefore, your organisation's defences will likely always be catching up (now you understand the struggle of the regulator). The most important thing you can do is make sure you have the response mechanisms in place to ensure operational resilience in the event your organisation falls victim to a cyber-attack.

The second area is suitability. Many of the new digital asset products (e.g. cryptocurrencies, utility tokens, stablecoins) are targeted primarily at the retail market and raise new concerns about the suitability of such products. Suitability is an issue that is often misunderstood and not appropriately applied to the circumstances of each Client. We will be looking to see that Firms that offer these products conduct, where required, proper suitability checks before offering the product to individual clients. We will look to ensure that you have appropriately assessed the risk of the product in the context of each Client's experience, knowledge, and risk appetite.

This year, we've concluded a thematic review focused on suitability and expect to publish the findings report in Q4 of this year. I encourage you to read the report to understand our expectations in this regard.

Last but certainly not least is AML/CFT. This remains at the top of our risk list and will likely stay there for a long time to come. New technologies, in particular, cryptocurrencies offer new mechanisms for clients to transact in more transparent and less costly ways. But at the same time, they can be a mechanism for criminals to transact in less transparent ways and support the secret movement of illicit funds. Some blockchain technologies offer the promise of transparency in transaction flows; others offer the promise of secrecy. You have to understand which one you are dealing with and we will expect you to have the appropriate tools to conduct effective monitoring. We will watch to see that Firms in fact adopt appropriate tools to manage the risk. You will see demonstrations of a couple of relevant tools later in this session.

I will finish with an update on our Innovation Testing Licence Programme (ITL), the core of our innovation supervision programme. The ITL is now in its fifth year and since its launch in May 2017, we have received 105 formal applications and invited 51 innovative companies to join the programme. These have included companies offering AI-supported SME funding; digital debt issuances (conventional & Islamic), AI-supported wealth management; robo-advisory; InsurTech; token crowdfunding; payroll solution applications; escrow solutions; payments & cross-border money transfer, and E-wallets.

The programme has proven invaluable in supporting the safe offering of innovative technology-enabled products and services and we intend to continue to offer the programme for the

foreseeable future. We are now preparing to launch our 8th cohort in July. For this cohort, we will entertain applications related to security token offerings. That said, I encourage you to read Consultation Paper 138, before submitting your application, to make sure your proposed business model is consistent with what is in the consultation paper. You can find CP-138 on the DFSA website in the section for Consultation Papers.

Level 13, The Gate, PO Box 75850, Dubai, UAE
Telephone: +971 (0)4 362 1500
Fax: +971 (0)4 362 0801