

Virtual Get Togethers A Series Summary

DQ Advocates
April 2020

Introduction

This paper has been produced by the Regulatory & Compliance Advisory team of DQ Advocates Limited to provide a summary of the recently held “virtual get together s” (VGTs).

The VGTs were held by DQ as a forum for Compliance professionals across the Isle of Man. The forum was designed to encourage discussion on the compliance challenges presented by the Covid-19 global pandemic. Over April 2020, six VGTs were held using video conferencing, engaging 80 compliance professionals. A variety of topics were discussed, including several best practice points.

Contact points for the team in case of queries on this paper are:

Sinead O’Connor – sinead@dq.im

Kathryn Sharman – Kathryn.sharman@dq.im

Mike Nudd – Michael.Nudd@dq.im

Interaction with the Regulator

All meetings discussed attendees’ interaction with the FSA. Some of the bigger firms represented were experiencing frequent communication, while smaller firms did not report the same the same level of interaction. This led to the conclusion that, in the first instance, the FSA is focusing its direct communication with licenceholders on those which pose a more systemic risk to the Island. For those entities which had not contact from the FSA, a proactive approach was encouraged. Firms should reach out to the FSA and communicate any concerns or issues as well as any changes to their business practices. Where licenceholders had taken a proactive approach, attendees reported that the communication received a positive response, reflecting well on the licenceholder.

Risks and the Risk Management Framework

It was recognised across the meetings that the pandemic presents increased risks, both known and unknown. Risks identified during the discussions included increased fraud and working from home (WFH). WFH presents risks around CDD collection, non face to face business and data security. It was appreciated that identifying risks remotely may be difficult. To mitigate this, all aspects of the business should be engaged to effectively identify risks and changes in order to mitigate against them. All risks must be included into the regulated entity’s risk management framework, including the Business Risk Assessment required by the AML/CFT Code and the Technology Risk Assessment, particularly as technology plays such a key part in working from home and liaising with clients in different ways.



Any exceptions made to standard processes should be clearly documented. One recommended best practice point was the use of a decision log to record exceptions, the mitigation for them and the thinking behind the decision.

Working from home – “A new way of working”

The lockdown has resulted in an unprecedented increase in WFH. All meetings discussed how WFH has impacted attendees. It was agreed that the way on which a business adapted to WFH may be the focus of a supervisory visit in the future so the importance of documenting decisions and exceptions arising from WFH is critical.

Across the meetings, several concerns were raised about WFH. One concern included the long term impact. Businesses should be aware of potential fatigue and the impact of sick leave on key processes and controls as well as considering how policy changes can be communicated to staff in a remote environment.

Another best practice point which was shared was the implementation of a WFH policy, detailing specific requirements. Some attendees noted they had already implemented such a policy with success. Some suggestions for what might be included in a WFH policy were the need for people to be located in different rooms, where possible, if various members of the household are WFH and a WFH conflict register to record measures taken to manage such situations. This was in addition to normal WFH security measures such as locking computers and keeping material confidential. The policy may also cover expenses and data confidentiality, for example shredding processes while WFH. One attendee advised they have a cost centre for purchases relating to WFH. Such purchases may include equipment. Another attendee advised that their policy included regular breaks and other steps for staff welfare.

An attendee raised that the WFH policy should cover the process for suspicious activity reporting. The current environment may pose difficulties for secure communication or following the traditional policy. For some attendees, WFH had led to a noticeable decrease in suspicious reporting. One suggestion was for employees to have access to THEMIS so that any report could be saved there as a draft which the MLRO can then access if encrypted emails cannot be used. Firms should ensure that employees are aware of their surroundings and the impact this may have on security. Any challenges with reporting should be reported to the FIU.

FIU Communication

It was noted that the FIU continues to function as normal and THEMIS remains the reporting portal. Businesses should advise the FIU if they are experiencing issues that may delay or prevent the timely reporting of STRs. The FIU is to be advised if WFH impacts on an MLRO’s ability to work effectively. It was also mentioned that the FIU



is conducting a risk assessment in relation to the pandemic and its impact on financial crime which it is planning to publish.

Data Protection

Across all meetings, no attendees noted any particular pandemic related reason to engage with the Information Commissioner. It was noted that WFH may increase the risk of a potential breach and attendees were encouraged to consider including measures to mitigate against breaches in the WFH policy.

Data protection areas for focus include complying with data security and privacy while WFH. It was also raised that remote access can provide a control measure as it should not result in data being used outside of the office.

The use of a Data Protection Impact Assessment (DPIA) in relation to WFH was discussed across several meetings. A DPIA has scope for use when a new technology or process is implemented. The impact of the pandemic could necessitate a DPIA to encompass new ways of working, variations to the processing of data and even new data collection such as asking employees more detailed questions about their health or that of family members. In addition to the use of a DPIA, the privacy policy and all privacy notices should be reviewed and updated to reflect the current processing undertaken.

Business Continuity Plan (BCP)

BCPs were discussed across several meetings in relation to a variety of matters. Consideration should be given to identifying critical workers within the business (workers who may still work or attend the office) within the BCP as it is unlikely that the BCP was written with a lockdown situation in mind. In light of police checks, if a key person is required to travel to the office, a letter from the business might assist. A template is available from any of the team whose contact details are at the start of this document.

Businesses should ensure that their BCP is robust and reflects the reality they now find themselves working in. This may also be a focus area of future supervisory visits and it is important that the FSA can see that the business updated its BCP in light of the pandemic and the associated restrictions.

Documentation for Assurance

The rationale for any changes made during the pandemic should be clearly documented across the business. It is important to be aware of how changes taking place in one area may impact other aspects of the business including risk assessments



and governance. Risk assessments should be regularly reviewed to ensure they reflect the current environment and the processes used.

It is expected in future supervisory visits that the FSA will look for references in the risk management framework to the pandemic, how it was managed and any changes or exceptions that took place. Effective documentation provides future assurance if scrutinised.

Technical issues

Issues and concerns regarding technology were raised by a number of attendees across the meetings. It was identified that poor internet or phone connection is a risk which should be reflected accordingly in risk management frameworks. Issues with diverting phones was also identified as a potential risk. Overreliance on the internet should also be recorded as a risk.

It was agreed that DQ Advocates would feedback technology issues and concerns discussed to the relevant areas, including the Chamber of Commerce.

Audit

The issue of conducting audits was also identified. It is expected that there will be future pressure on auditors which may affect their ability to undertake a timely audit. Businesses were encouraged to proactively engage their auditors to ensure there is no extreme delay in the undertaking of required audits. One attendee commented that lots of audit based work can still be undertaken if the auditors are engaged and effectively communicated with. Some aspects such as transactional testing may prove more difficult.

The recent website communication from the IOM FSA regarding the submissions of Audited Financial Statement and Annual Compliance Returns was highlighted and a link to this is provided at the end of this document.

Electronic CDD

The collection of electronic CDD was a key topic of discussion in most meetings. Concerns raised included the processes used or ability to collect electronic CDD and the acceptance of electronic CDD by third parties such as banks. A banking representative in one meeting advised that their firm were reviewing acceptability on a case by case basis because there currently is no formal agreement on the acceptance of electronic CDD. Firms were advised to contact their banks directly regarding accepted forms of CDD if it is a concern. In another meeting, an attendee noted that



they were aware that one bank is working closely with the FSA on creating guidance regarding e-signatures and e-documentation.

Firms were also advised to investigate using the delayed verification of identity concession provided in the AML/CFT Code. If the concession is used, it was recognised that this must be clearly documented with adherence to the associated requirements in the Code.

In some meetings, attendees discussed their approaches to the use of electronic CDD such as passport selfies and practical pitfalls that may arise. One practical issue raised was the cost and difficulty of implementing any new system or new technology used for CDD collection. Other issues included achieving board buy in for such a system and also risk rating such a process. One mitigation provided for electronic CDD was the later provision of standard CDD when possible.

Another issue raised was how to ensure an e-document is tamper proof when arguably nothing is tamper proof. It was also noted by some attendees that clients themselves may be wary of using such processes. If electronic CDD processes are to be used, they should be effectively communicated to clients along with any intention if this CDD is to be supplemented at a later date.

CPD

It was noted in all meetings that the FSA's view is that compliance with the CDP requirements remains in place. It was advised that webinars should be used where possible to continue to demonstrate CPD. If this poses an ongoing issue, dialogue with the FSA or the relevant industry association may be beneficial. A community approach was encouraged, through the sharing of webinar links on LinkedIn for example. Internal training could potentially be conducted using video conferencing technology.

Compliance Monitoring

Compliance monitoring should continue to be undertaken where possible. A risk based approach should be exercised, with businesses focusing on key elements, the current situation and the arising risks. Where full monitoring cannot be undertaken, this too should be documented with rationale and explanation. The challenge of Compliance Officers being remote from the Board/Senior Management in the current working environment was discussed in relation to monitoring and governance. It was noted that Compliance Officers should ensure that appropriate measures are implemented to ensure that governance is maintained at all times.



One attendee noted that due to the working situation, they still had one employee in the office able to undertake monitoring. Other attendees noted that as they were paperless, they were able to undertake monitoring as normal.

Jersey Guidance

Several key points from recent Jersey guidance were noted. These included ensuring board resilience, fulfilling critical functions and separation of functions. Consideration should also be given to mind and management requirements. In light of travel restrictions and remote working, licence holders should document how they will fulfil these obligations. Documentation should demonstrate mind and management, for example recorded virtual board meetings.

Another observation raised by the JFSC related to situations where material outsourcing is in place. It is recommended that these contracts and arrangements are reviewed to ensure that the appropriate controls are still evident and so that there is an understanding of any changes in how the outsourced provider is operating.

Economic Substance

Consideration should be given to economic substance and if this is still being met. Travel restrictions may impact the ability to conduct board meetings on Island. Steps taken in regard to substance should be clearly documented.

PI Insurance

Further consideration should be given to the business' PI insurance. Working from home may change the business model and impact on insurance terms. Businesses should contact their insurer to determine if their PI insurance is affected.

Risk Appetite

One challenge of the current pandemic is the potential reduction of new business. This may lead to a change in the risk appetite of the business, leading to the acceptance of higher risk business. Compliance should be aware of Board decisions that may affect risk appetite and reflect this accordingly in the customer risk assessment and other relevant risk assessment documentation.



Liquidity and Capital

Over several meetings, attendees were reminded that Directors and Boards have a duty to maintain liquidity and capital in order to comply with the financial resources and reporting requirements. Compliance should be aware of any steps that may be taken that would affect liquidity or capital such as dividend payments.

Compliance should also focus on ensuring that financial resources and reporting requirements are fulfilled. It is appreciated that in a remote environment this may be difficult.

Best Practice

A decision log. This is being used by some businesses to record and document the consideration of risks and other issues before their inclusion in risk assessments. This is a useful way to document considerations and discussions on key areas and provide a future aide memoire.

A working from home conflicts log. This is being used to record potential conflicts that may arise. Examples given include working near a partner that may work at another financial organisation or rival firm.

Exception Form. This is used to document exceptions made to processes such as scanned CDD. The form should highlight the risks of the exception, the mitigating steps taken and the expected outcomes.

FAQ sheets. This can be used to clearly communicate to staff processes for contacting other members of staff or third parties as well as other policies or processes. Examples include social media communication or the removal of the ability to print from home.

Governance flowchart. A flowchart which outlines the appropriate person or team to contact and helps to facilitate governance changes remotely.

Useful links:

DQ Article on Covid-19 in the regulated sector:

<https://dq.im/coronavirus-covid-19-in-the-regulated-sector/>

DQ Article on Digital Identity:

<https://dq.im/digital-identity-in-a-digital-world-the-fatf-guidance/>

IOM FSA AML Covid-19 specific guidance:

<https://www.iomfsa.im/media/2677/covid-19-amlcft-faqs.pdf>



IOM FSA delay to audits update:

<https://www.iomfsa.im/fsa-news/2020/apr/arrangements-for-submission-of-audited-financial-statements-and-annual-compliance-returns-in-response-to-covid-19/>

IOM Information Commissioners Office Covid-19 FAQ's:

<https://www.inforights.im/media/1787/coronavirus.pdf>

IOM Information Commissioners Office Direct Marketing guidance:

<https://www.inforights.im/media/1047/direct-marketing-technical-guidance.pdf>

UK National Cyber Security Centre Working from Home Guidance:

<https://www.ncsc.gov.uk/guidance/home-working>

UK ICO Covid-19 Guidance:

<https://ico.org.uk/for-organisations/data-protection-and-coronavirus/>

Jersey FSC Covid-19 information update:

<https://www.jerseyfsc.org/news-and-events/more-information-for-businesses-in-response-to-covid-19/>

Guernsey FSC Covid-19 increased Fraud risk Guidance:

<https://www.gfsc.gg/news/article/commission-warns-licensees-increased-risk-fraud-arising-covid-19>

FATF Digital identity Guidance (including risks of electronic CDD gathering and suggested mitigation):

<https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf>

FATF Covid-19 statement:

<http://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-covid-19.html>

