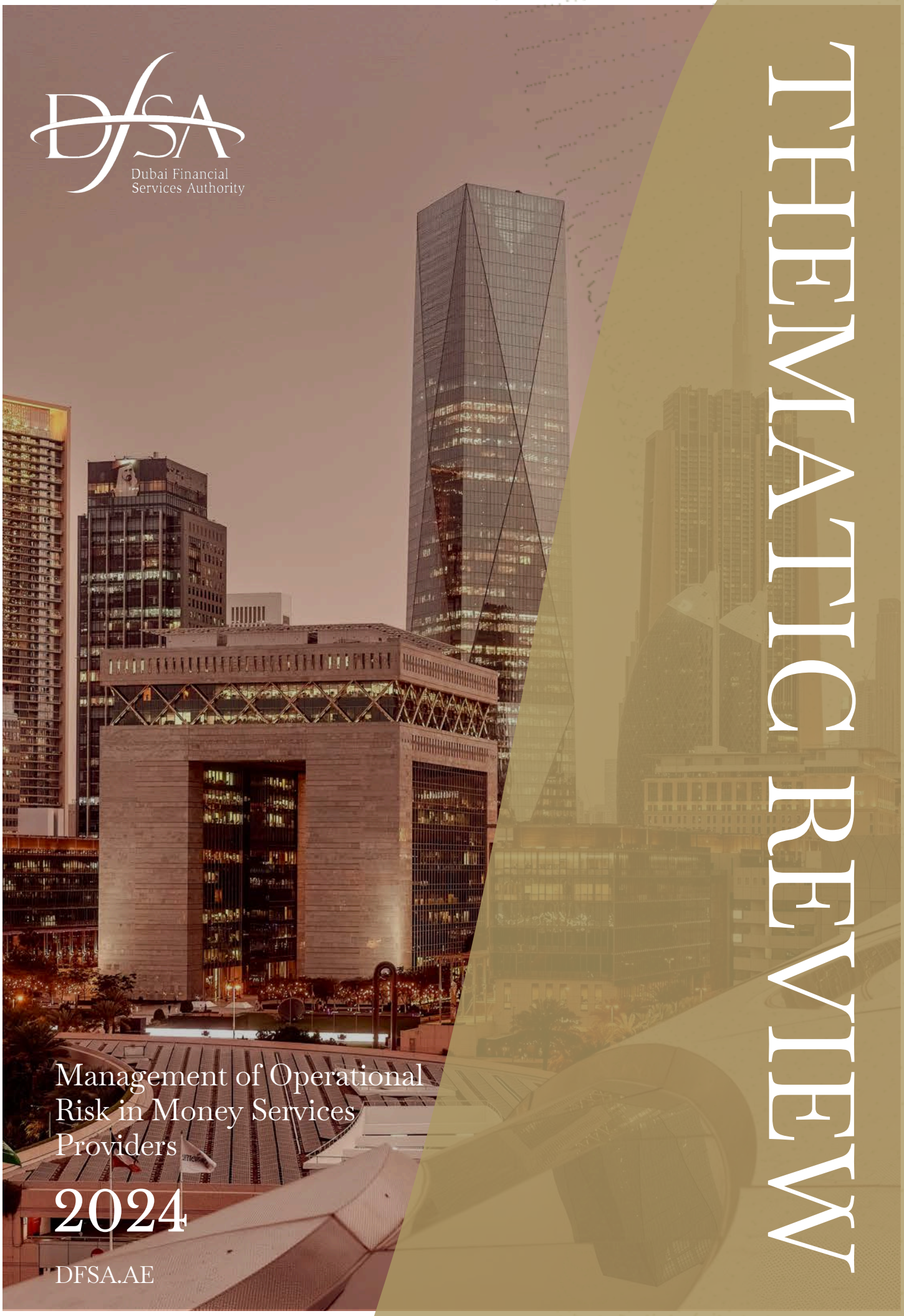

Dubai Financial Services Authority

THEMATIC REVIEW

Management of Operational Risk in Money Services Providers

2024

DFSA.AE

BACKGROUND

In line with our regulatory objectives, and our 2024 supervisory priorities, the Dubai Financial Services Authority (DFSA) conducted a Thematic Review (Review) on Money Services Providers (MSPs).

From 2021 to date, there has been a significant growth of MSPs in the Dubai International Financial Centre (DIFC), resulting in increases in clients' services and transactions conducted in or from the DIFC. Therefore, the DFSA considers it appropriate to assess MSPs regulatory compliance and vulnerabilities to mitigate any potential integrity issues in the DIFC Money Services sector, including the possibility of fraudulent online transactions.

The Review focused on MSPs' management of Operational Risk, specifically, the level of regulatory compliance with Chapter 6 the Prudential – Investment, Insurance Intermediation and Banking Business (PIB) Module of the DFSA Rulebook. MSPs are required to implement systems and controls to identify and report fraudulent transaction attempts and must apply strong customer authentication to verify transactions initiated via web or application-based digital channels.

During March 2024, the DFSA contacted MSPs requesting information concerning their Operational Risk policies and procedures to assess their level of regulatory compliance.

The following areas were assessed via a desk-based review and subsequent interviews with key senior operations and compliance personnel:

1. relevant operational policies and procedures;
2. Strong Customer Authentication (SCA) and user security measures;
3. exceptions applied to SCA measures and implementation of technical standards;
4. systems and controls to detect fraud; and
5. reporting of information about transactions and rates of fraud.

The DFSA expects all MSPs in the DIFC to consider the key themes and findings in this Review in the context of their specific activities and obligations, and, where appropriate, consider further enhancements to their systems and controls.

We also remind MSPs of their continuing obligations to ensure that the DFSA is promptly informed of any significant events or anything else relating to the firm of which we would reasonably expect to be notified.

SCOPE AND METHODOLOGY

The Review assessed MSPs' compliance of Management of Operational Risk. It also provided an insight on whether fraud reporting obligations by these firms are adhered to.

It aimed to:

- assess MSPs' compliance with Management of Operational Risk, specifically, the level of regulatory compliance with Chapter 6 the PIB Module of the DFSA Rulebook; and
- highlight areas of non-compliance for further action by the MSPs.

The Review was undertaken in three phases:

PHASE ONE

Information request

MSPs were requested to provide copies of Operational Risk management policies and procedures and a complete checklist outlining how operational risk as prescribed in Chapter 6 of the DFSA PIB Rulebook are met.

PHASE TWO

Desk-based review and firm interviews

A desk-based review was undertaken based on the information provided by MSPs. Desk-based review was followed by interviews with MSPs to seek clarification and enhance understanding of the process and procedures applied.

PHASE THREE

Report and action plan

All the observations and findings were consolidated in this Review while specific areas of non-compliance were addressed on a bilateral basis with each MSP directly.

KEY THEMES AND FINDINGS

1. Risk management framework and governance

Governing Body is defined in the DFSA Rulebook as the board of directors, partners, committee or management of an MSP.

It is important to evidence that an MSP's Governing Body has approved the MSP's Operational Risk policy. This ensures that there is an appropriate level of oversight with regards to the MSP's processes and this is documented for audit purposes.

We observed that most assessed MSPs were able to provide evidence of operational risk information in the form of a policy or document. However, these MSPs were unable to evidence the document or policy being reviewed and approved by the MSP's Governing Body, nor compliance with the Governing Body's approval process.

Action Required:

MSPs must ensure their Governing Body approves their Operational Risk Policy in accordance with PIB 6.2.2.

2. Strong Customer Authentication and User security measures

Strong Customer Authentication (SCA) is defined in PIB 6.13.2 as:

1. authentication that is based on the use of two or more elements that are:
   a. independent, in that breach of one element does not compromise the reliability of any other element; and
   b. designed in such a way as to protect the confidentiality of the authentication data.
2. the elements must consist of two or more of the following:
   a. something known only by the User ('knowledge');
   b. something held only by the User ('possession'); or
   c. something inherent to the User ('inherence').

What we expect of a MSP, in maintaining the integrity of SCA:

1. no element of 'knowledge', 'possession' or 'inherence' can be derived from the disclosure of the authentication code cover;
2. it is not possible to generate a new authentication code based on an old one;
3. the authentication code cannot be forged;
4. where the authentication through a remote channel has failed to generate an authentication code, it is not possible to identify which of the SCA elements was incorrect;
5. a maximum of 5 failed consecutive authentication attempts within a given period result in the account being temporarily or permanently blocked;
6. the duration and number of retries for a temporary block should be linked to the service offered and trigger a fraud risk alert; and
7. the User is alerted before the block becomes permanent and a secure procedure is established to regain the use of the blocked payment instrument.

We observed that most MSPs were able to discuss and evidence SCA with the User Security Credentials (USC). However, implementation of the specific security measures and the associated processes were not documented.

Action Required:

Per PIB 6.13.3(4), MSPs are required to maintain adequate security measures to protect the confidentiality and integrity of Users' personal security credentials. MSPs should maintain and document these security measures in their policies and procedures.

3. Technical standards

Under PIB 6.13.5, MPSs must develop, implement and document in the firm's Operational Risk Policy, technical standards relating to:

1. the implementation of the requirements for strong customer authentication referred to in PIB 6.13.3;
2. procedures for applying the exclusions in PIB 6.13.4;
3. common and secure standards of communication for the purpose of identification, authentication, notification, and sharing information with Users and other service providers; and
4. if applicable, procedures, systems and controls that ensure the reliability and continuity of the interface made available by a payment account provider.

MSPs can apply exclusions to SCA as defined in PIB 6.13.4 when:

1. the User accesses its own payment account information unless:
   a. it is the first time the account is accessed; or
   b. the account has not been accessed for 90 days or more;
2. the User makes a payment of a small amount;
3. the User makes a payment to a specified beneficiary on a list created by the User, or under a standing order, where strong customer authentication was applied when the list or standing order was created; or
4. a transfer is made between accounts held by the same User.

We observed that various MSPs had Operational Risk management policies which did not specify how and where the technical standards were documented, including appropriate measures to demonstrate compliance with PIB 6.13.5.

Action Required:

MSPs must develop, implement, and document in the MSP's Operational Risk Policy, the technical standards which address all four requirements mandated by PIB 6.13.5.

4. Systems and controls to detect fraud

MSPs must have in place transaction monitoring systems and controls to detect and prevent unauthorised or fraudulent Payment Transactions.

These systems and controls must be designed taking into account the following risk factors:

1. compromised or stolen authentication elements;
2. the amount of each payment transaction;
3. known fraud scenarios in the provision of the particular Payment Service;
4. analysis of Payment Transactions typical of the type of Users;
5. signs of malware infection in any sessions of the authentication procedure; and
6. if the firm provides the access device or software (the Payment Instrument), a log of the use of the access device or software and abnormal use.

We observed that not all MSPs were able to demonstrate or provide documentation evidencing:

a. their transaction monitoring systems and controls; and
b. that all the required risk factors had been considered.

Action Required:

MPSs must have in place appropriate transaction monitoring systems and controls designed with the relevant risk factors in mind.

FINAL COMMENTS

The DFSA would like to extend its thanks to staff at the MSPs who participated in the Review by providing quality data and thorough responses to the information request and follow-ups. The DFSA and participant MSPs acknowledge the importance of a robust Operational Risk framework, implementation to mitigate risk, and sound systems and controls to identify and report fraudulent transactions.

About the DFSA

The Dubai Financial Services Authority (DFSA) is the independent regulator of financial services conducted in and from the Dubai International Financial Centre (DIFC), a purpose-built financial free zone in Dubai. The DFSA's regulatory mandate covers asset management, banking and credit services, securities, collective investment funds, custody and trust services, commodities futures trading, Islamic finance, insurance, crowdfunding platforms, money services, an international equities exchange and an international commodities derivatives exchange.

In addition to regulating financial and ancillary services, the DFSA is responsible for administering Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) legislation that applies to regulated firms and Designated Non-Financial Businesses and Professions in the DIFC.

www.dfsa.ae