Operational Efficiency and resilience in the UAE (Critical Data Management) – DFSA / DIFC

Overview of **Dubai Financial Services Authority** (DFSA) Expectations

Introduction

The DFSA expects Authorised Firms to understand their Operational Risk exposures and take necessary steps to effectively mitigate the risks. The DFSA does not require Authorised Firms to follow any particular Operational Risk framework. However, Authorised Firms are expected to establish an appropriate and effective Operational Risk management framework to identify, assess, monitor, report and control or mitigate Operational Risk. The framework should be consistent with the Firm's risk appetite and the nature, scale, and complexity of the Firm's business activities.

There are three oversight bodies that prescribe minimum standards for the Banking, Insurance, and Securities sectors in the UAE: **the Basel Committee on Banking Supervision (BCBS)**, the International Association of Insurance Supervisors (IAIS), and the International Organisation of Securities Commissions (IOSCO).

"From time-to-time, international standard setting and oversight bodies, conduct assessment of the DFSA's regulatory regime. Our aim is to create an environment that is on par with international standards of regulation and represents a best-of-breed of best practices."

Part. 1 Regulators' overview in the UAE

1. **Securities and Commodities Authority** (SCA)

   The SCA regulates and supervises the securities and commodities market in the UAE. It sets rules and regulations for companies, brokers, and financial intermediaries operating in the capital markets.

2. **Central Bank of the United Arab Emirates** (CBUAE)

   The CBUAE is the central bank of the UAE. It is responsible for monetary and financial stability, including regulating banks, financial institutions, and payment systems within the country.

3. **Dubai Financial Services Authority** (DFSA)

   The DFSA is the independent regulator of the Dubai International Financial Centre (DIFC). It regulates and supervises financial services, including banking, insurance, securities, and asset management within the DIFC.

4. **Abu Dhabi Global Market (ADGM) Financial Services Regulatory Authority** (FSRA)

   The FSRA is the regulatory authority of the ADGM, a financial free zone in Abu Dhabi. It regulates and supervises financial services activities, including banking, insurance, securities, and asset management within the ADGM.

Part. 2 Regulators in the onshore of UAE

1. **The Central Bank of the UAE**

2. **The Emirates Securities and Commodities Authorities (ESCA)**

   The ESCA IT department has initiated the implementation of the Information Security Management System (ISMS) in alignment with the ISO 27001:2013 standard to support the strategic vision of the SCA IT Department and ensure that the information security practices are

in line with the industry-wide best practices for information security. This project assists SCA IT **to improve the information availability, integrity and confidentiality** and put in comprehensive approaches to assess information risks and define a comprehensive treatment plan. As part of this journey, the SCA IT Department also intends to achieve the ISO/IEC 27001:2013 Certification, the only auditable standard available for information security.

Part. 3 Dubai Financial Services Authority (DFSA) – Laws & Rules

Legal Framework: Article 121 of the UAE Constitution enabled the Federation to create Financial Free Zones in the Emirates, and most importantly, to exclude the application of certain Federal laws in these Financial Free Zones. A number of laws created the DIFC and the necessary centre bodies, which include the DFSA. These laws set out the objectives, powers and functions of the centre bodies. They also contain important exemptions and prohibitions in the DIFC.

Federal Law No. 8 of 2004 on “The Financial Free Zones in the United Arab Emirates” (the Financial Free Zone Law). This means that the DIFC would mostly have its own regulatory and legal framework.

Part. 4 Data-related Regulations in the UAE

Regulation	Description
UAE Data Protection Law	The UAE introduced the Data Protection Law (Federal Law No. 2 of 2019) to govern the processing of personal data. This law aims to protect individuals' privacy rights and imposes certain obligations on organizations that collect and process personal data.
National Electronic Security Authority (NESA)	The NESA was established to enhance cybersecurity in the UAE. It issues guidelines and regulations to protect critical information infrastructure and systems, ensuring their resilience against cyber threats.
Dubai Data Law	Dubai implemented its own data protection law known as the Dubai Data Law (Law No. 26 of 2015). It governs the management of data within the emirate of Dubai, including the protection, sharing, and utilization of data.
Critical Infrastructure and Information Protection (CIIP) Regulations	The UAE has implemented CIIP regulations to safeguard critical infrastructure and information from potential threats. These regulations apply to both public and private entities operating critical infrastructure, such as energy, telecommunications, transportation, and finance.
Cloud Computing Regulatory Framework	The UAE Telecoms Regulatory Authority (TRA) has issued guidelines and regulations for cloud computing services. These regulations address issues such as data sovereignty, data protection, and data storage within the country.

Telecommunications Regulatory Framework	The TRA oversees the telecommunications sector in the UAE. It establishes regulations related to data protection, data retention, and data management for telecom operators and service providers.
Dubai International Financial Centre (DIFC) Data Protection Law	The DIFC, a financial free zone in Dubai, has its own data protection law called the DIFC Data Protection Law. It sets out data protection obligations for organizations operating within the DIFC.

Part. 5 Macro data management comparison insights between the EU, CH, and the UAE

Item	European Union (EU)	Switzerland (CH)	United Arab Emirates (UAE)
Data Protection Regulation	General Data Protection Regulation (GDPR)	Federal Act on Data Protection (FADP)	Data Protection Law (Federal Law No. 2 of 2019)
Data Transfer	GDPR allows for data transfers within the EU and to countries with an adequacy decision or appropriate safeguards in place. Additional measures may be required for transfers outside these provisions.	Switzerland allows for data transfers within Switzerland and to countries with adequate data protection levels or with appropriate safeguards in place.	UAE imposes restrictions on international data transfers and requires data transfers to meet adequacy or other conditions determined by the UAE authorities.
Critical Infrastructure Protection	EU Directive on Security of Network and Information Systems (NIS Directive) sets requirements for the security of critical infrastructure sectors, including data protection measures.	Switzerland has specific regulations and guidelines for the protection of critical infrastructure, including data protection measures.	UAE National Electronic Security Authority (NESA) issues regulations and guidelines for the protection of critical information infrastructure, including data protection measures.
Risks and Operational Resilience (Critical Data)	Basel Committee on Banking Supervision, Principles for Operational Resilience	Circular 2023/1 Operational risks and resilience – banks	The DFSA Rulebook, Authorised Market Institutions (AMI), Ch. 5., CM 5.5 Operational efficiency and resilience

Part. 6 Operational efficiency and resilience (AMI)

Key concepts

Concept	Description	Chapter ref. (AMI)
Systems and controls	Authorised Market Institution must ensure that its systems and controls are: (a) adequate to ensure that its operations are conducted at all times in accordance with the applicable requirements, including legislation; (b) sufficiently flexible and robust to ensure continuity and regularity in the performance of its functions relating to the operation of its facilities; and (c) appropriate to the nature, scale and complexity of its operations.	5.5.1.
Risk management	Provide sufficient and reliable information to Key Individuals and, where relevant, the Governing Body of the Authorised Market Institution.	5.5.2, 3, (d)
Outsourcing	Authorised Market Institution must, before entering into any material outsourcing arrangements with a service provider, obtain the DFSA's prior approval to do so. In assessing the adequacy of an Authorised Market Institution's systems and controls for identifying, assessing, and managing risks arising from functions which are outsourced, the DFSA will have regard to: (a) the business continuity and disaster recovery arrangements of the Authorised Market Institution's service provider. (b) whether the security and confidentiality of information provided to the service provider of the Authorised Market Institution is guaranteed in accordance with the applicable legislation.	5.5.3
Technology resources	For the purposes of meeting the requirement in (1), an Authorised Market Institution must have adequate procedures and arrangements for the evaluation, selection, and on-going monitoring of information technology systems. Such procedures and arrangements must, at a minimum, provide for: (a) problem management and system change (b) testing information technology systems before live operations in accordance with the requirements in Rule 5.5.6	5.5.5 (4)

	(c) monitoring and reporting on system performance, availability and integrity; and (d) adequate measures to ensure: (i) the information technology systems are resilient and not prone to failure (ii) business continuity in the event that an information technology system fails (iii) protection of the information technology systems from damage, tampering, misuse or unauthorised access; and (iv) the integrity of data forming part of, or being processed through, information technology systems **Guidance** In assessing an Authorised Market Institution's systems and controls used to operate and carry on its functions, the DFSA recognises that an Authorised Market Institution is likely to have significant reliance on its information technology systems. In assessing the adequacy of these systems, the DFSA will consider: a. the organisation, management, and resources of the information technology department of the Authorised Market Institution b. the arrangements for controlling and documenting the design, development, implementation and use of technology systems; and c. the performance, capacity and reliability of information technology systems.	

Sources

DFSA Website, July 2023, Operational & Technology Risk Supervision
https://www.dfsa.ae/what-we-do/supervision/operational-technology-risk-supervision/summary

DFSA Website, July 2023, Regulatory Laws and Rules
https://www.dfsa.ae/your-resources/regulatory/laws-and-rules

DFSA Website, July 2023, Rulebook
https://dfsaen.thomsonreuters.com/rulebook/ami-55-operational-efficiency-and-resilience?highlight=resilience&phrase=false

Securities & Commodities Authority Website, July 2023, Policies
https://www.sca.gov.ae/en/about-us/all-policies.aspx

Disclaimer

The information presented in this paper is based on official sources and publicly available data as of the time of writing. While every effort has been made to ensure the accuracy and reliability of the content, Alydium SA cannot guarantee the completeness or suitability of the information for any particular purpose. The content is provided for informational purposes only and does not constitute legal or professional advice. Readers are advised to consult official sources, seek legal counsel, or professional expertise to obtain the most up-to-date and accurate information regarding data management regulations in the United Arab Emirates (UAE), the European Union (EU), and Switzerland. Alydium SA assumes no liability for any errors, omissions, or consequences arising from the use of the information provided.

July 2023