ABU DHABI GLOBAL MARKET
سوق أبوظبي العالمي

DISCUSSION PAPER
NO. 1 OF 2023

INFORMATION TECHNOLOGY RISK MANAGEMENT

29 November 2023

CONTENTS

CONTENTS 2

INTRODUCTION 3

Why we are issuing this paper 3

Who should read this paper 3

How to provide comments 4

What happens next 4

Comments to be addressed to 4

OVERVIEW 5

A. IT Risk Management Guidance 5

B. Review of Existing IT-Related Rules 8

C. IT Incident Reporting Requirements 8

D. Regulatory Technologies (“RegTech”) for Authorised Firms 10

CONCLUSION 11

INTRODUCTION

Why we are issuing this paper

1. The Financial Services Regulatory Authority ("**FSRA**") of Abu Dhabi Global Market ("**ADGM**") is issuing this discussion paper (“**Discussion Paper**”) to seek views on its initiatives to enhance information technology (“**IT**”) risk management practices in authorised firms, where this term covers both Authorised Persons and Recognised Bodies in this Discussion Paper.

2. IT is present and vital in all aspects of financial services and effective IT risk management is therefore a key factor in ensuring that business operations and services to customers are resilient against internal and external threats, thereby allowing them to operate when faced with such threats.

3. In order to support the ongoing, rapid digital transformation of the financial services sector, the FSRA has requirements governing the management of IT risks and has incorporated the review of IT risk management in its supervisory activities for authorised firms. This Discussion Paper sets out initiatives that the FSRA is building on to enhance its supervisory oversight of IT risk management practices in authorised firms. These include issuing comprehensive and holistic “IT Risk Management Guidance” that brings together the FSRA’s observations on best practices across a range of IT domains, including guidance for the adoption of algorithm-driven and decentralized infrastructure solutions.

4. In conjunction with this, the FSRA is considering the following, further steps to reinforce good IT risk management practices in authorised firms:

   a. reviewing existing rules relating to IT risk management to incorporate core requirements that would strengthen authorised firms’ practices;

   b. requiring authorised firms to report material IT incidents to the FSRA in a standardised format within a prescribed timeframe; and

   c. making regulatory technologies available to authorised firms to navigate the FSRA’s Rulebooks and guidance relating to IT risk management.

5. Capitalized terms contained in this Discussion Paper have the meanings attributed to them in the FSRA’s Glossary (“**GLO**”), unless otherwise defined in this paper.

Who should read this paper

6. This Discussion Paper should be of particular interest to authorised firms, potential applicants seeking to operate within ADGM, and their respective professional advisors.

7. The FSRA also welcomes feedback from other stakeholders, whether based in ADGM or beyond, regulated firms in other jurisdictions with IT risk management experience, think tanks and industry groups.

How to provide comments

8. All comments must be made in writing and sent to the mail address or email address specified below. If sending your comments by email, please use the Discussion Paper number in the subject line. If relevant, please identify the organisation you represent in providing your comments. The FSRA reserves the right to publish, including on its website, any comments you provide, unless you expressly request otherwise at the time of making any comments. Comments supported by reasoning and evidence will be given more weight by the FSRA.

What happens next

9. The deadline for providing comments on this Discussion Paper is 9 February 2024, after which we will consider whether any modifications are required to the proposals.

Comments to be addressed to

Discussion Paper No. 1 of 2023
Financial Services Regulatory Authority
Abu Dhabi Global Market, ADGM Square
Al Maryah Island
PO Box 111999
Abu Dhabi, UAE
Email: consultation@adgm.com

OVERVIEW

10. The FSRA considers IT risk management to be a key part of authorised firms' management of their overall risk profile, with "risk posture" being the appropriate term for that component of their overall risk profile. In this respect, binding requirements relating to IT risk management and controls have been issued in the form of regulations and rules by ADGM and the FSRA respectively. These regulations and rules specify the standards that authorised firms must meet to maintain a robust and resilient IT environment as an inherent part of their business activities.

11. As part of our ongoing regular engagement with industry stakeholders, including authorised firms, the FSRA has received feedback on the need for specific regulatory guidance on IT risk management against the backdrop of an increasingly digitalised financial services landscape, to help authorised firms implement best practices in relation to a broad set of IT practices and domains. Additionally, in early 2023 the FSRA conducted a survey of authorised firms and concluded that there is room for them to strengthen their IT risk management culture in authorised firms as well as provide tools for them to further develop their existing risk management capabilities.

12. The following sections detail a number of initiatives that the FSRA believes will help authorised firms enhance their practices in this area.

A. IT Risk Management Guidance

13. The FSRA proposes issuing IT Risk Management Guidance ("**ITRMG**"), contained in **Attachment 1**, to cover an extensive range of best practices across a variety of IT domains. The ITRMG will complement existing requirements and guidance by being relevant to all authorised firms regardless of the Regulated Activities they undertake. By issuing the ITRMG, the FSRA intends to communicate its views on how a consistent and risk-sensitive approach might be employed by authorised firms in managing their IT risk.

14. In formulating the ITRMG, the FSRA has considered the work in this area by international standard setting bodies and financial services regulatory authorities, as well as leading industry standards on information technology and security.

15. In order to put the ITRMG in context with existing regulations, rules and guidance, the table below illustrates the set of IT-related material relevant to firms authorised by the FSRA.

Regulations and Rulebooks containing IT-related content	**ADGM Regulations**	• Data Protection Regulations • Electronic Transactions Regulations
	FSRA Rules (activity-agnostic)	• General Rulebook • Anti-Money Laundering and Sanctions Rules and Guidance
	FSRA Rules (activity-focused)	• Conduct of Business Rulebook • Prudential – Investment, Insurance Intermediation, and Banking Rules • Prudential – Insurance Business • Market Infrastructure Rulebook
Guidance containing IT-related content	**FSRA Guidance (thematic)**	**Activity/Topical-Focused** • Digital Securities • Digital Investment Management ("Robo-advisory") • Private Financing Platforms and Multilateral Facilities • Virtual Assets • Cybercrime Mitigation
		Technology-Focused • Application Programming Interfaces (APIs) • Emerging Technologies (Joint-issuance with CBUAE, SCA, and DFSA)
	FSRA Guidance (activity-agnostic)	IT Risk Management Guidance (ITRMG)

16. The ITRMG comprises four sections, each with a number of chapters that set out the FSRA's expectations in those areas:

    A. Establishing a Culture of Effective IT Risk Management: overall governance and controls for IT risk, including the management of IT third parties;

    B. Managing an IT Environment: how authorised firms should manage IT assets, infrastructure, systems lifecycle, resilience and cyber events;

    C. Interacting Securely: how authorised firms should manage access to their systems, cryptographic keys and online transaction services; and

    D. Leveraging Business Embedded Technologies: how authorised firms that use specific technologies should address the IT risks associated with those technologies.

17. Each chapter of the ITRMG begins with desired outcomes that summarise the FSRA's expectations for authorised firms. For each of these desired outcomes, the FSRA has set out best practices for authorised firms. For example, Desired Outcome 3.2 in chapter 3 of the ITRMG states that an authorised firm should closely

monitor and review its IT third parties' performance and risk posture. This is followed by best practices on conducting due diligence, developing contractual agreements, monitoring the performance of IT third parties and putting termination arrangements in place.

Section	Chapter	Desired Outcomes
A. Establishing a Culture of Effective IT Risk Management	1. Governance and Oversight 2. Risk Management 3. Third Party Management 4. Compliance and Audit	15
B. Managing an IT Environment	5. System Lifecycle Management 6. Information Technology Asset Management 7. Operational Infrastructure Management 8. Data Lifecycle Management 9. Resilience 10. Cyber Event Management	19
C. Interacting Securely	11. Access Management 12. Online Transaction Security 13. Cryptography	8
D. Leveraging Business Embedded Technologies	14. Algorithm-Driven Solutions 15. Decentralised Infrastructure Solutions	4

18. While the ITRMG is relevant to all authorised firms, it is neither a binding set of rules nor a standard of care owed by authorised firms to their customers. Authorised firms are expected to adapt the ITRMG in a manner that is commensurate with the nature, scale and complexity of their business activities carried out in ADGM.

19. The FSRA is also cognisant of international developments in IT risk management and will endeavour to harmonise, where appropriate and practical, its expectations and requirements to those published by regulatory and industry standard setting bodies.

20. Upon the formalisation and launch of the ITRMG, the FSRA will refer explicitly to the ITRMG when assessing applications for authorisation and during supervisory reviews of firms. In this way, the ITRMG will provide transparency to applicants and authorised firms of the expectations of the FSRA in this area.

21. Additionally, the ITRMG will be updated as and when the FSRA identifies new IT best practices or as mitigation strategies against threat actors are publicised. This approach aims to ensure that the ITRMG keeps pace with the fast evolving IT landscape and updates to the ITRMG will be published on the FSRA website.

ISSUES FOR CONSIDERATION

1. Do you agree with the content covered by the proposed ITRMG?
2. Do you have any concerns with or feedback on specific desired outcomes or best practices outlined in the proposed ITRMG?

B. Review of Existing IT-Related Rules

22. The FSRA has IT-related rules across multiple Rulebooks. For example, in the Conduct of Business Rulebook, there are sections relating to technology governance for Virtual Assets and authentication mechanisms for Payment Services. Similarly, in the General Rulebook there are rules relating to outsourcing and business continuity and disaster recovery.

23. It is timely for the FSRA to review its existing suite of IT-related rules and, where appropriate, strengthen the requirements that authorised firms are to comply with in key areas, e.g. IT risk awareness training, IT audit, independent security testing.

24. The FSRA is cognisant, however, of balancing between being overly prescriptive and not having the tools it needs to ensure authorised firms maintain a robust IT control environment, especially given the rapid evolution of IT in financial services. The above-mentioned proposed areas reflect the need for more specific rules on IT risk management while not confining compliance to a narrow subset of IT controls that may not be applicable to all authorised firms.

25. As a result, the FSRA will conduct a review of existing IT-related rules, to be followed by a separate consultation exercise in 2024 to solicit specific feedback on the final set of proposed rules for IT risk management.

ISSUES FOR CONSIDERATION

3. What additional IT areas should the FSRA consider for the revision of its rules?

C. IT Incident Reporting Requirements

26. Many financial services regulators globally have implemented incident reporting requirements for IT, in such areas as IT security and cyber security incidents. Such reporting keeps regulators aware of emerging threats to authorised firms, thereby allowing regulators to take prompt action to prevent any potential systemic impact.

27. While Rule 8.10.6 of the General Rulebook requires authorised firms to advise the FSRA immediately where they become aware of any significant failure in their systems or controls, there is currently no specific guidance on what constitutes a

significant failure in relation to IT incidents or on how authorised firms should report such events. Given the increasing importance of IT to financial services, it is opportune for the FSRA to provide further guidance to authorised firms to improve the consistency and timeliness of responses, alongside a formal requirement to report all material incidents.

28. The FSRA therefore proposes to require authorised firms to report IT-related incidents that have a material impact on a firm's business operations or the provision of services to customers, in the form of a specified incident report template. The FSRA does not intend to narrow the scope of reportable incidents to only IT security or cyber incidents as IT-related incidents may arise due to actions by external threat actors, e.g. ransomware attack, denial-of-service[1], or through internal lapses, e.g. system misconfiguration, inadequate system capacity planning.

29. In designing the incident report template, the FSRA will consider several reference points, including existing notification templates published by regulators globally and international standard setting bodies, such as the report from the FSB on the public feedback received on a framework for common cyber incident reporting[2]. The FSRA proposes that the incident reporting template should include the following items:

a. Details of the reporting entity and primary point of contact;

b. Date and time the incident was discovered;

c. Nature of the incident, e.g. system outage, cyber-attack, data leak, and its impact, e.g. financial loss, service disruption;

d. Steps taken to mitigate impact, respond to, and recover from the incident; and

e. Shareable intelligence, e.g. virus signature, indicators of compromise, in the event of an attack from external actors.

30. The FSRA intends to set the period for the assessment of and reporting requirement for material IT incidents to be no longer than two hours from an authorised firm's discovery of an IT incident.

31. The FSRA also intends to require that authorised firms submit a post-incident report. The post-incident report should contain a root-cause analysis of the incident and the appropriate remediation actions taken to address the root cause(s). Furthermore,

[1] Per the FSB's Cyber Lexicon (updated in 2023), a ransomware is malware that is used to commit extortion by impairing the use of an information system or its information until a ransom demand is satisfied. A denial of service attack is one where the prevention of authorised access to information or information systems; or the delaying of information system operations and functions, with resultant loss of availability to authorised users occurs.
[2] https://www.fsb.org/2023/04/format-for-incident-reporting-exchange-fire-a-possible-way-forward/

the FSRA will propose that the post-incident report would need to be submitted no later than fourteen calendar days after the incident was discovered by the firm.

32. Following its review of existing IT-related rules, the FSRA will conduct a separate consultation exercise in 2024 to solicit specific feedback on the final set of proposed rules for incident reporting.

ISSUES FOR CONSIDERATION

4. Do you agree that the FSRA should provide specific requirements for the IT incident reporting?

5. Do you have any views on the proposed content for IT incident reports?

6. Do you have any views on the proposed IT incident reporting timeline?

7. Do you have any views on the proposed post-incident report submission timeline?

D. Regulatory Technologies ("RegTech") for Authorised Firms

33. In November 2021, the FSRA published a case study on digital regulation as part of its RegTech Report[3]. The case study described the use of artificial intelligence ("**AI**") to make the FSRA's Rulebooks more accessible to authorised firms and other stakeholders. Subsequently, in November 2022, the FSRA launched its Open Regulation initiative that provided a "training ground" where industry specialists, RegTech companies and the data science community could access that FSRA's AI models, data and research to allow them to create AI-enabled RegTech tools[4].

34. As part of the FSRA's ongoing efforts to innovate and explore the use of RegTech to help users navigate its Rulebooks and guidance documents, the FSRA has been undertaking research into the uses of AI models, specifically large language models ("**LLMs**") that have risen in prominence in the last 12 months.

35. Given that IT-related rules and guidance are contained in various Rulebooks and guidance documents, the FSRA will be trialling the use of LLMs to provide conversational-style interactions for interested parties to help them navigate relevant rules and guidance. The desired outcome is for users of the interface,

[3] The report is available here: https://www.adgm.com/media/announcements/fsra-issues-report-on-regulatory-technology

[4] The Open Regulation repository is available here: https://www.adgm.com/media/announcements/adgms-financial-services-regulatory-authority-launches-its-ai-initiative-on-open-regulation

whether authorised firms or other interested parties, to receive a tailored set of the rules and guidance relevant to them in response to a particular IT implementation.

36. The FSRA is of the view that the use of RegTech tools will not only provide authorised firms with greater clarity on the specific set of regulatory requirements that they must comply with, but also allow them to be able to demonstrate to the FSRA how they are meeting them, alongside encouraging voluntary adoption of a broader set of relevant risk management practices. The FSRA is also cognisant of the risks associated with the use of LLMs and will ensure that RegTech tools that use LLMs are rigorously tested to ensure that known risks associated with their use are treated effectively.

37. Based on the response to and efficacy of the tool, the FSRA may potentially expand the scope of rules and guidance beyond IT risk management.

ISSUES FOR CONSIDERATION

8. Do you have any views on whether the FSRA should provide RegTech tools to facilitate navigating its Rulebooks and guidance?

9. Do you have concerns on the FSRA's use of LLMs to provide RegTech tools?

CONCLUSION

38. Given that IT risk management is an ever-evolving discipline, both in the region and globally, the FSRA highly values stakeholders' feedback on the proposals in this Discussion Paper. The FSRA believes that these proposals will strengthen the risk posture of authorised firms, promote a robust IT ecosystem, and contribute to the achievement of ADGM's strategic goals.