CONSULTATION PAPER
NO. 3 OF 2025

PROPOSED ENHANCEMENTS TO CYBER RISK MANAGEMENT

30 April 2025

TABLE OF CONTENTS

Introduction

Why we are issuing this paper

1. The Financial Services Regulatory Authority ("**FSRA**") of the Abu Dhabi Global Market ("**ADGM**") has issued this consultation paper to invite public feedback on its proposal to introduce specific cyber risk management requirements for regulated firms ("**Cyber Risk Rules**").

2. The financial services industry is a primary target for cybercriminals. As financial institutions rely more heavily on technology, they face growing vulnerabilities to cyber risks, including those associated with financial crime. The varying levels of cyber resilience across firms have resulted in incomplete protection for the sector as a whole, due to its interconnected nature and reliance on outsourced services. To enhance overall cyber resilience, it is essential for all industry participants to establish a consistent baseline of security measures.

3. At a national level, the UAE is placing ever-increasing importance on combatting cyber threats. In January 2022, the UAE introduced federal cybercrime legislation, and measures to prevent cybercrime remain a key focus in the UAE's preparation for its Mutual Evaluation by the Financial Action Task Force in 2026.

4. The FSRA will continue to play a key role in contributing to the coordinated national efforts to combat financial crime, including preventative measures against the growing risk of cybercrime. Financial crime prevention is a strategic priority for the FSRA, in line with its objectives of ensuring that financial markets in the ADGM are supported by secure and efficient infrastructure, promoting and enhancing the integrity of the ADGM Financial System, and providing adequate protection for users of the system[1].

5. Capitalised terms contained in this consultation paper have the meanings attributed to them in GLO, unless otherwise defined in this paper.

Who should read this paper

6. This paper will be of interest to Authorised Persons and Recognised Bodies, potential applicants for a Financial Services Permission, and their respective professional advisors.

[1] Section 1(3) of the Financial Services and Markets Regulations 2015

How to provide comments

7. All comments should be made in writing and sent to the mail address or email address specified below. If sending your comments by email, please use the consultation 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

8. The deadline for providing comments on this proposal is 11 June 2025. When we receive your comments, we will consider whether any modifications are required to the proposed amendments described in this paper. The FSRA will then proceed to enact the proposed amendments. You should not act on the proposed amendments until the relevant regulations and rules are issued and we will publish a notice on our website when that happens.

Comments to be* addressed *to:

Consultation Paper No. 3 of 2025
Abu Dhabi Global Market
ADGM Square
Al Maryah Island
PO Box 111999
Abu Dhabi, UAE
Email: fsra.consultation@adgm.com

Background

1. Technology and data are essential drivers for today's financial institutions. Advanced technology is relied upon to streamline operations, achieve business goals, and deliver superior services to customers and clients. Data plays a pivotal role in supporting decision-making, operations and service delivery. By harnessing the power of technology and data, modern financial institutions can offer more efficient, effective, and customer-focused service.

2. As technology continues to transform financial services, robust IT and cyber risk management becomes increasingly critical. The FSRA is committed to ensuring that the ADGM financial markets are supported by secure infrastructure that safeguards the integrity of the ADGM Financial System. The ecosystem of innovative firms that choose to operate from our international financial centre demonstrates the FSRA's progressive approach to financial services regulation and support for technological advances in the financial services industry.

3. In November 2020 the FSRA issued guidelines on the mitigation of cyber threats and crimes ("**Guidelines**")[2] and in 2023 published a Discussion Paper on Information Technology Risk Management ("**Discussion Paper**")[3]. In the Discussion Paper the FSRA was clear that it considers IT risk management to be a key part of a firm's management of its overall risk profile. More recently, the FSRA released its Information Technology Risk Management Guidance to provide firms with a set of desired outcomes and best practices on the sound management of information technology risks ("**Guidance**")[4]. The Guidance identifies what the FSRA considers to be best practices for identifying and managing information technology risks and serves to support Authorised Persons and Recognised Bodies in their compliance with the existing, related binding legislative requirements.

4. These proposals for cyber risks in this consultation paper should also be seen as a component of the work that the FSRA is currently undertaking more generally in relation to operational resilience. The proposed amendments form part of the FSRA's phased approach to enhancing the operational resilience of Authorised Persons and Recognised Bodies.

[2] FSRA/FCPU/15/2020: *Governance Principles and Practices to Mitigate Cyber Threats and Crime*
[3] *Discussion Paper No. 1 of 2023: Information Technology Risk Management*, November 2023
[4] *Information Technology Risk Management Guidance*, November 2024

Proposed Cyber Risk Rules

5. The proposed Cyber Risk Rules build upon the recently issued Guidance by providing specific Rules for the management of cyber risks, as a natural step in the evolution of the FSRA's regulatory framework in this area.

6. The proposed Cyber Risk Rules would primarily be captured by adding a new cyber risk management section to Chapter 3 (Management, Systems and Controls) of the General Rulebook ("**GEN**"). An amendment would be made to the Market Infrastructure Rulebook ("**MIR**") to bring Recognised Bodies within scope alongside Authorised Persons. Other consequential changes would be made to the Conduct of Business Rulebook ("**COBS**"), the Prudential – Insurance Business Rulebook ("**PIN**"), the Captive Insurance Business Rulebook ("**CIB**"), the Prudential – Investment, Insurance Intermediation and Baking Rulebook ("**PRU**") and the Glossary Rulebook ("**GLO**").

Proposed Rulebook amendments

7. The proposed Cyber Risk Rules comprise the following.

   a. New Rules added to Chapter 3 of GEN (Management, Systems and Controls) under the heading of *Cyber Risk Management*. The Rules would require firms to:
      i. identify and assess their cyber risks;
      ii. establish and maintain a Cyber Risk Management Framework ("**CRMF**") that appropriately addresses those risks;
      iii. put in place appropriate governance and systems and controls as part of the CRMF;
      iv. undertake ongoing monitoring and reporting on the effectiveness of the CRMF; and
      v. manage and control cyber incidents, and notify material incidents to the FSRA, covered in more detail in paragraph 8).
   b. An amendment to MIR, to bring Recognised Bodies within scope.
   c. Minor amendments to COBS, PIN, CIB and PRU to align existing Rules or Guidance with the proposed Cyber Risk Rules.
   d. New definitions being added to GLO.

8. The proposed Cyber Risk Rules require that a firm's CRMF be integrated within its overall risk management framework as established pursuant to GEN 3.3.4-3.3.6. Additionally, the proposed CRMF applies a risk-based approach that is commensurate to the nature,

scale and complexity of the activities conducted by Authorised Persons and Recognised Bodies.

Transitional arrangements

9. The proposed Cyber Risk Rules do not require more than the expectations set out in the Guidelines issued in 2020. They do not extend to the adequacy of technology resources or operational resilience more generally and, as a result, the existing Rules and Guidance in that regard remain unaffected. Accordingly, the FSRA believes that it is appropriate to expect implementation by firms within three months of the Cyber Risk Rules coming into force.

Question 1

Are there any specific aspects of the Cyber Risk Rules that are likely to present material challenges for firms?

Question 2

Do you agree with the requirement for firms to establish and maintain a CRMF?

Question 3

Do you agree with the CRMF being integrated within a firm's overall risk management framework?

Question 4

Do firms need three months to effect compliance with the Cyber Risk Rules, or is an implementation period unnecessary? Do firms need longer than three months, and if so, why?

Notification of cyber incidents

10. The proposed Cyber Risk Rules include a requirement to notify material cyber incidents to the FSRA immediately, and in any event no later than 24 hours after the firm becomes aware of an incident, notwithstanding weekends or public holidays. Guidance in the Cyber Risk Management Rules sets out what the FSRA will consider to be 'material'. As GEN 8.10.6 already requires immediate reporting to the FSRA of material issues of this kind, an immediate notification requirement for significant cyber incidents will not create additional regulatory burden. Initial reporting will only need to cover preliminary information known at the time by the relevant firm. The FSRA considers that the 24-hour backstop to the immediate reporting requirement will:

a. facilitate faster mitigation of the incident, in turn potentially reducing its scope and impact;
b. support early coordination of resources by firms, potentially minimising potential contagion across systems and preventing (further) financial losses; and
c. enable reputational damage to be proactively addressed.

Question 5

Do you agree with the requirement to notify material cyber incidents to the FSRA immediately and in any event within 24 hours?

Post-implementation steps

11. The FSRA plans to undertake a review of firms' implementation of the Cyber Risk Rules. This may take the form of a thematic review or similar, with a view to providing the FSRA with the necessary information to further enhance its supervisory approach in this area. In the longer term, and informed by the outcomes of that review, the FSRA is contemplating introducing an obligation on firms to file an annual return. This reflects the heightened national focus on cybersecurity referred to earlier in this paper and the FSRA's preferred approach to cyber risk management prioritising risk mitigation, accountability, and transparency.

12. Publication of the Cyber Risk Rules will be followed by a program of awareness and outreach led by the FSRA.

Question 6

Do you agree with the introduction of an annual Cyber Risk Management Return in due course?

Question 7

Do you have any other comments on the proposals relating to cyber risk management as set out in this paper?

Miscellaneous amendments

13. In addition to our proposals in relation to the Cyber Risk Rules, we are taking the opportunity to correct some minor errors, omissions and typos in COBS, GEN and MIR. These have been integrated into the relevant Appendices to this paper.

Question 8

Do you have any comments on the proposed miscellaneous amendments included in Appendices 2, 3 and 5?

Conclusion

14. The detailed, proposed legislative amendments to the relevant Rulebooks are included in Appendices 1 to 7 to this paper. We believe that the proposed Cyber Risk Management Rules will align the FSRA with international best practices and ensure that we are clear that the management of cyber risk is a fundamental aspect of combatting financial crime.

Annexes, appendices and attachments

15. The draft, proposed legislative amendments to the relevant FSRA Rulebooks are set out as follows.

- **Appendix 1** - Proposed amendments to the Captive insurance Business Rulebook (CIB);
- **Appendix 2** - Proposed amendments to the Conduct of Business Rulebook (COBS);
- **Appendix 3** - Proposed amendments to the General Rulebook (GEN);
- **Appendix 4** - Proposed amendments to the Glossary Rulebook (GLO);
- **Appendix 5** - Proposed amendments to the Market Infrastructure Rulebook (MIR);
- **Appendix 6** - Proposed amendments to the Prudential - Insurance Business Rulebook (PIN); and
- **Appendix 7** - Proposed amendments to the Prudential - Investment, Insurance Intermediation and Banking Rulebook (PRU).