Appendix 3

GENERAL RULEBOOK (GEN)

*In this attachment underlining indicates new text and striking through indicates deleted text.

...

3.3.32 (1) An Authorised Person must inform the Regulator about any material outsourcing arrangements.

...

Guidance

1. An Authorised Person's outsourcing arrangements should include consideration of:

   a. applicable guiding principles for outsourcing in financial services issued by the Basel Committee on Banking Supervision, IOSCO or any other international body promulgating applicable standards for outsourcing by Financial Institutions; or

   b. any equivalent principles or regulations the Authorised Person is subject to in its home country jurisdiction.

2. An outsourcing arrangement would be considered to be material if it is a service of such importance that weakness or failure of that service would cast serious doubt on the Authorised Person's continuing ability to remain fit and proper or to comply with the Regulator's administered Regulations and Rules.

3. Rule 3.5 contains additional requirements that apply to an Authorised Person that receives services directly from a third party or a subcontractor of a third party which involve accessing the Authorised Person's IT Systems or Networks or accessing or processing its data.

...

3.3.~~3~~4~~1~~A (1) This Rule applies to:

(a) Banks

...

3.5 Cyber Risk Management

This Rule 3.5 takes effect on [6 months from the date of publication].

Cyber Risk Management Framework

3.5.1 (1) An Authorised Person must establish and maintain a Cyber Risk Management Framework to identify, assess and manage Cyber Risk effectively.

(2) An Authorised Person must ensure the Cyber Risk Management Framework is in writing and is approved by its Governing Body.

(3) The Cyber Risk Management Framework must:

(a) include systems and controls which are appropriate to the nature, scale and complexity of the activities conducted by the Authorised Person; and

(b) have clearly defined roles and responsibilities, including accountability for decision making during business-as-usual operations and stressed situations.

(4) The systems and controls in Rule 3.5.1(3)(a) must include one or more systems for the purposes of:

(a) identifying and assessing Cyber Risk which enables the Authorised Person to implement the requirements in Rule 3.5.4;

(b) protecting ICT Assets in accordance with Rules 3.5.5 to 3.5.13;

(c) monitoring and testing the effectiveness of such systems and controls in accordance with Rule 3.5.14; and

(d) managing Cyber Incidents which enables the Authorised Person to comply with the requirements in Rules 3.5.15 to 3.5.17.

(5) An Authorised Person must review its Cyber Risk Management Framework to ensure that it remains appropriate, effective and up-to-date .

(6) An Authorised Person must carry out the review required under (5) regularly, and at least annually.

(7) An Authorised Person must integrate its Cyber Risk Management Framework within its overall risk management framework established under Rules 3.3.4 to 3.3.6.

Guidance

1. An Authorised Person's Cyber Risk Management Framework may be based on, or informed by, other relevant guidance and regulations published by the Regulator and other competent UAE federal authorities, as well as standards prepared by international organisations or recognised professional institutions, including the following:

a. The UAE Telecommunications and Digital Government Regulatory Authority: UAE Information Assurance (IA) Regulation (2020);

b. International Organisation for Standardisation: Information technology – Security techniques – Information security management systems – Overview and vocabulary (ISO standard no. 27000:2018);

c. National Institute of Standards and Technology (NIST): Framework for Improving Critical Infrastructure Cybersecurity (2018);

d. Center for Internet Security: Critical Security Controls (2024);

e. Committee on Payments and Market Infrastructures and the International Organisation of Securities Commissions: Guidance on cyber resilience for financial market infrastructures (2016);

f. Cloud Security Alliance: Cloud Controls Matrix and CAIQ (2024);

g. Risk assessment methodology: NIST SP800-30: Guide for Conducting Risk Assessments (2012);

and subsequent versions thereof.

2. The systems and controls referred to in Rule 3.5.1(4)(b) should enable an Authorised Person to protect its ICT Assets in accordance with the requirements in Rules 3.5.5 to 3.5.14 in a way that minimises the likelihood and impact of a successful Cyber Incident on ICT Assets as identified under Rule 3.5.4(1). They should be commensurate with the outcome of the Cyber Risk assessment under Rule 3.5.4(2) and the Authorised Person's Cyber Risk tolerance determined under Rule 3.5.3(2)(c).

3. An Authorised Person may need to apply additional controls, depending on its nature, scale or complexity.

4. An Authorised Person may also rely on Group-wide policies on Cyber Risk when developing its policies, procedures or controls.

5. An Authorised Person should tailor any standards or policies it chooses to adopt to its needs. Not all elements of the standards or policies may be applicable. Additional policies, procedures and controls may be required to address idiosyncratic risks.

6. Systems and controls put in place pursuant to Rule 3.5.1 may include supporting policies and procedures.

3.5.2 (1) An Authorised Person must manage Third-Party Cyber Risk as part of its Cyber Risk Management Framework established under Rule 3.5.1. This must include:

(a) undertaking due diligence to ensure that where it chooses suitable third-party providers of ICT Services they comply with appropriate Cyber Risk standards;

(b) ensuring that the terms of the contractual arrangements with a third-party provider of ICT Services require the third party to:

(i) comply with the Authorised Person's Cyber Risk requirements;

(ii) notify the Authorised Person about all Cyber Incidents that may affect the Authorised Person;

(iii) work with the Authorised Person in remediating the impact of a Cyber Incident on the Authorised Person;

(iv) allow the Authorised Person to verify that the third party continues to meet the Authorised Person's Cyber Risk requirements; and

(c) supervising effectively the provision of ICT Services by third parties.

(2) An Authorised Person that relies on the provision of ICT Services by a third party remains fully responsible for compliance with, and the discharge of, all obligations under this Rule 3.5.2.

Guidance

1. This Rule supplements the overarching requirements that govern the outsourcing of functions and activities under Rules 3.3.31 and 3.3.32 by an Authorised Person. The scope of this Rule is wider than the scope of those outsourcing requirements as it applies to the provision of all ICT Services that may affect the provision of Regulated Activities by an Authorised Person, including the provision of cloud services and the maintenance of the servers of an Authorised Person.

2. The supervision of the provision of ICT Services by a third party under Rule 3.5.2(1)(c) should include regular and appropriate verification that the third party complies with the Authorised Person's security requirements. Verification may be achieved, for example, through a review of the third party's control environment or using independent audit reports. The frequency, scope and independence of the verification or other review(s) should be determined based on the criticality of systems and the sensitivity of information contained in them. In certain circumstances, it may not be appropriate to allow the third party to undertake such review or verification itself.

3. The Regulator expects an Authorised Person to apply adequate controls on the use of subcontractors by a third party. An Authorised Person should be aware of the scope of services that are carried out by subcontractors and what actions were undertaken to mitigate Cyber Risk by both the third party and all of its subcontractors.

4. A contract with a third-party provider of ICT Services should set out appropriate requirements for the deletion or return of an Authorised Person's information at the end of the contract.

Governance

3.5.3 (1) An Authorised Person must ensure that its Governing Body and senior management are ultimately responsible for ensuring that its Cyber Risk Management Framework is implemented and followed and that Cyber Risk is managed effectively.

(2) Without limiting the operation of (1), the responsibilities of an Authorised Person's Governing Body and senior management in respect of Cyber Risk include:

(a) ensuring that Cyber Risk is adequately identified, assessed and managed in accordance with the Authorised Person's Cyber Risk Management Framework;

(b) establishing and maintaining a senior management structure for the management of Cyber Risk and for ensuring compliance with the Authorised Person's Cyber Risk Management Framework;

(c) defining the Authorised Person's Cyber Risk tolerance, which must be in line with its business objectives, strategy and overall risk tolerance; and

(d) ensuring that relevant personnel have the necessary expertise to manage Cyber Risk.

Guidance

1. The Regulator expects the Governing Body of an Authorised Person to demonstrate a thorough understanding of all Cyber Risk to which it is or might be exposed. The Governing Body should be regularly updated on current global cyber trends and be included in Cyber Risk training, cyber awareness campaigns and similar activities conducted by the Authorised Person.

2. Management information on Cyber Risk and mitigation measures should be presented to the Governing Body in a way that can be easily understood and analysed. It should include information on current and emerging Cyber Risks and the efficacy of existing mitigation measures. For example, the Regulator expects the Governing Body to be informed where a performance indicator signals that a Cyber Risk control may be underperforming or failing, leading to the Cyber Risk exposure approaching the Authorised Person's risk tolerance.

Identification and assessment of Cyber Risk

3.5.4 (1) An Authorised Person must identify and maintain a current inventory of its ICT Assets and classify them in terms of their confidentiality and how critical they are to the support of its business functions and processes.

(2) An Authorised Person must carry out an assessment of Cyber Risk associated with the assets identified in (1) regularly and no less than annually.

(3) When carrying out the assessment in (2) an Authorised Person must:

(a) identify threats from Cyber Incidents, including cybercrimes;

(b) assess the Cyber Risk resulting from those threats and the effectiveness of relevant controls, including the outcomes of ongoing monitoring and testing undertaken in accordance with Rule 3.5.14, to arrive at the residual Cyber Risk;

(c) analyse and quantify the potential impact and consequences of the residual Cyber Risk on its overall business and operations.

Guidance

1. The purpose of this Rule is to ensure that an Authorised Person understands which of its ICT Assets, critical operations and supporting information should be protected against Cyber Incidents, in order of priority.

2. An Authorised Person's assessment of the Cyber Risk it faces or may potentially face should be accurate, up-to-date and reviewed regularly and no less than annually.

3. The assessment should include, at a minimum:

a. an assessment of the interconnections and dependencies between the Authorised Person's ICT Assets and its business functions and processes;

b. consideration of the results of the Authorised Person's most recent risk self-assessment, where applicable, and testing of its business continuity arrangements under Rule 3.3.33;

c. consideration of Cyber Risk that third parties pose to the Authorised Person; and

d. a review of the inventory of ICT Assets.

4. The Regulator expects an Authorised Person to have well-defined processes and clearly assigned responsibilities for maintaining its ICT Asset inventory and assessing Cyber Risk. The ICT Asset inventory should record where each asset is stored and what it is used for. It should also include ICT Assets belonging to third parties upon which Authorised Person depends, including software as a service and cloud-hosted applications.

5. An Authorised Person should consider participating in industry forums relating to Cyber Risk that provide an opportunity for intelligence sharing.

Protection of ICT Assets against Cyber Incidents

3.5.5 An Authorised Person must use and maintain up-to-date anti-malware software and ensure that regular updates are applied to its anti-malware signature files.

Guidance

The Regulator expects an Authorised Person to use anti-malware software to conduct regular automatic scanning of its ICT Assets, in particular servers and workstations, and to scan all files received over networks (including email attachments and files downloaded from websites) and files kept on storage media before use. The anti-malware software should be used to detect and block malware, potentially malicious links in emails and malicious websites.

3.5.6 (1) An Authorised Person must implement network security controls, including appropriate network architectures, protocols and network security devices, to protect the perimeters of its Networks.

(2) An Authorised Person must implement network security monitoring procedures to facilitate prompt detection of unauthorised or malicious activities.

Guidance

An Authorised Person should consider installing security devices at critical junctures in its Networks (e.g., firewalls, web application firewalls, intrusion detection and prevention systems, virtual private network gateways) to protect the perimeters of its Networks. The rules and configurations of the network security devices should be backed up and reviewed regularly to ensure they remain appropriate and relevant.

3.5.7 (1) An Authorised Person must ensure that access rights and permissions to its IT Systems and Networks are properly managed.

(2) For the purposes of (1), an Authorised Person must:

(a) establish a user access management process for the approval of a user's request for access or permission which ensures that:

(i) the user is only granted the minimum access or permissions needed to perform that user's tasks or functions; and

(ii) the user's access and permissions are immediately revoked if the conditions for granting approval are no longer met.

(b) perform regular reviews of users' access rights and permissions to verify that they remain appropriate.

Guidance

1. The principle set out at Rule 3.5.7(2)(a)(i) is known as the "least privilege principle". This is a recognised information security concept that provides that only the minimum access necessary to perform an operation or task should be granted and that the access should be granted only for the minimum amount of time necessary. Its purpose is to reduce risk by limiting the number of individuals with access rights or privileges. In line with this principle, the Regulator expects an Authorised Person to base access rights and privileges, including access rights and privileges of Employees, Customers and third-party service providers, on a user's requirements and responsibilities and to revoke those rights and privileges as soon as they are no longer required, in particular when an employment, customer or contractual relationship comes to an end, or there is a change in a user's requirements or tasks.

2. Privileged access rights or permissions (i.e. rights and permissions to perform security related functions that ordinary users are not authorised to perform, including rights and permissions to administrator accounts) should be limited to the extent possible and assigned to user credentials different from those used for regular business activities. Regular business activities should not be performed using privileged user credentials.

3. Robust Identity and Access Management Practices should be adopted. These policies, procedures and systems outline which users have access to specific systems, data or functionality and the circumstances under which access is granted, reviewed and revoked.

4. The process of performing regular reviews of access and permissions should facilitate the identification of dormant and redundant accounts as well as the detection of unauthorised access rights or permissions.

5. Access rights and permissions for users may also include those for applications and programmes that are automated.

3.5.8 An Authorised Person must ensure that access to its IT Systems and Networks is properly secured, including by implementing:

(a) strong password authentication requirements;

(b) multi-factor authentication or equivalent protection for its IT Systems and Networks that may be accessed from the internet;

(c) multi-factor authentication or equivalent protection for privileged access rights or permissions; and

(d) encryption techniques to secure communication between a user and the Authorised Person's IT System and Network.

Guidance

1. The Regulator expects that an Authorised Person's strong password controls require, at a minimum, a change of password upon initial logon, minimum password length and history requirements, password complexity, maximum validity periods and lockout thresholds after a number of unsuccessful logon attempts.

2. For mobile devices, access controls and encryption techniques should address threats raised by their use away from the Authorised Person's premises.

3. Users with administrative or privileged access should use a designated device that is dedicated to carrying out approved privileged tasks and activities on sensitive systems.

3.5.9 (1) An Authorised Person must have a comprehensive change management process that considers Cyber Risk before and during a change to its IT Systems and Networks and any new Cyber Risk created after the change.

(2) The process in (1) must include systems and controls that ensure changes to its IT Systems and Networks are:

(a) adequately tested;

(b) approved before their implementation; and

(c) implemented promptly if needed to resolve material Cyber Incidents or security vulnerabilities.

Guidance

1. The purpose of the change management process is to ensure that changes and patches to production systems and hardware devices are adequately assessed, tested, approved and implemented.

2. The Regulator expects an Authorised Person to establish a separate physical or logical environment for the development, testing and production of systems or patches. The Regulator expects an Authorised Person to ensure a clear segregation of tasks so that no single individual develops, tests and implements any change.

3. While emergency changes should be implemented in a controlled manner, the Regulator recognises that the process requires swift actions and decisions. In such cases, where necessary and justifiable and on an exceptional basis, some aspects of an Authorised Person's change management process such as change

documentation or testing may be completed after a change has been implemented.

3.5.10 (1) An Authorised Person must establish a process for the management of software updates that addresses security vulnerabilities in the Authorised Person's ICT Assets.

(2) The process in (1) must ensure that:

(a) software updates are identified and classified by how critical they are to mitigate Cyber Risk;

(b) software updates are applied in a timely manner; and

(c) the implementation of critical software updates is prioritised.

(3) An Authorised Person must implement software updates in accordance with the process required under Rule 3.5.9.

Guidance

1. As part of its Cyber Risk Management Framework, an Authorised Person should establish a vulnerability management process for an up-to-date understanding of security vulnerabilities.

2. An Authorised Person may wish to consider using automated vulnerability scanning systems to assist in effectively identifying and assessing vulnerabilities resulting from new and evolving threats.

3.5.11 (1) An Authorised Person must implement appropriate encryption techniques to protect the confidentiality and integrity of information in transit, at rest, and at end of life.

(2) The encryption techniques implemented for the handling of information must be commensurate with the sensitivity of that information.

Guidance

1. The Regulator expects encryption techniques to be used to protect the confidentiality and integrity of sensitive information. In particular, encryption techniques should be used where such information is stored on workstation memory drives, external drives such as USB pen drives, external hard discs, mobile phones, tablets and other electronic equipment used to store or process critical and sensitive information.

2. Appropriate measures should also be taken when exchanging sensitive information. These encryption measures could include sending information

through encrypted channels or encrypting the information using strong encryption with an adequate key length.

3.5.12 (1) An Authorised Person must limit physical access to its data centres and server rooms, if any, to individuals who have a legitimate business need.

(2) For the purposes of (1), the Authorised Person must establish a process for:

(a) the approval of an individual's request for physical access; and

(b) the immediate revocation of such access if the conditions for granting approval are no longer met.

(3) An Authorised Person must implement appropriate security measures to prevent unauthorised physical access to its data centres and server rooms.

Guidance

The Regulator expects that:

a. where physical access is granted to individuals who are not members of an Authorised Person's staff, they will be accompanied by a staff member at all times during such access; and

b. an Authorised Person will monitor and record the activities that take place inside its data centres and server rooms.

3.5.13 (1) An Authorised Person must establish and maintain a comprehensive Cyber Risk management training programme and adequate awareness arrangements.

(2) The programme and arrangements in (1) must ensure that all relevant Employees:

(a) receive training, at least annually, on the Authorised Person's Cyber Risk policies and standards;

(b) develop and maintain appropriate awareness of, and competencies for, detecting and reporting Cyber Incidents; and

(c) understand their individual responsibilities.

Guidance

1. An Authorised Person should regularly review and, where necessary, update its training programme to ensure that it remains current and relevant. The review should take into consideration the evolving nature of technology as well as emerging Cyber Risks.

2. A relevant Employee would include any member of staff with access to an Authorised Person's IT System or Network or any other Employee who might otherwise be exposed to, or targeted by, a Cyber Incident.

3. New Employees should receive training within a reasonable period of joining the Authorised Person.

4. The Regulator expects Employees with privileged access rights to receive targeted security training that reflects their rights and responsibilities.

Monitoring and Testing

3.5.14 (1) An Authorised Person must implement a system to conduct ongoing monitoring of the effectiveness of the systems and controls that form part of its Cyber Risk Management Framework.

(2) An Authorised Person must ensure that:

(a) it has in place a comprehensive programme to test the resilience of its IT Systems and Networks and its processes and controls implemented to comply with Rules 3.5.5 to 3.5.13;

(b) testing under the programme is carried out regularly, and in the case of internet-facing systems, at least annually; and

(c) it has in place a process to prioritise and remedy adverse testing outcomes.

(3) An Authorised Person should ensure there is regular reporting to senior management on the results of the monitoring and testing it undertakes to satisfy its obligations under (1) and (2).

Guidance

1. An Authorised Person should use a range of methods to test its IT Systems and Networks and processes and controls, such as:

a. vulnerability assessments;

b. scenario-based testing;

c. penetration tests;

d. bug bounty programs;

e. red team exercises;

taking into account the Authorised Person's Cyber Risk assessment under Rule 3.5.4(2).

2. The frequency with which an Authorised Person should carry out testing will depend on the nature, scale and complexity of its business. It may be adequate to test annually for some Authorised Persons, for others more frequent testing may be required. The Regulator expects additional tests to be carried out whenever systems are updated or new systems are implemented, including when systems are changed to address any vulnerabilities that have been identified during testing.

Detection, response and recovery

3.5.15 (1) An Authorised Person must continuously monitor its IT Systems and Networks with a view to detecting:

(a) Cyber Incidents; and

(b) the occurrence of anomalies and events indicating a potential Cyber Incident.

(2) An Authorised Person must have a process for escalating actual or potential Cyber Incidents.

Guidance

1. An Authorised Person's ability to detect an actual or potential Cyber Incident is essential for strong cyber resilience. Early detection provides an Authorised Person with useful lead time to take appropriate measures to minimise any impact.

2. As part of its monitoring, the Regulator expects an Authorised Person to regularly review system logs, warnings, errors and security events to identify suspicious activities and system errors indicating a potential Cyber Incident.

3. The process for escalating actual or potential Cyber Incidents should define a point of contact for reporting incidents. All Employees should be made aware of their responsibility to report actual or potential Cyber Incidents as quickly as possible.

3.5.16 (1) An Authorised Person must establish and maintain a robust Cyber Incident Response Plan providing for measures to be taken by the Authorised Person to respond to and limit the consequences of a Cyber Incident.

(2) The Cyber Incident Response Plan must include appropriate conditions and procedures to ensure the timely implementation of response and recovery actions, including the actions required by Rule 3.5.17.

(3) The conditions and procedures in (2) must be regularly tested to ensure their effectiveness.

(4) An Authorised Person must ensure its Cyber Incident Response Plan is in writing and that it is reviewed regularly and no less than annually, and after the occurrence of a material Cyber Incident that is reportable pursuant to Rule 3.5.18, to ensure that it remains appropriate, effective and up-to-date.

Guidance

1. Rule 3.3.33 provides overarching requirements for an Authorised Person's business continuity arrangements. The Regulator expects the Cyber Incident Response Plan to be integrated into the Authorised Person's overall crisis management and disaster recovery plans, where applicable.

2. The Regulator expects an Authorised Person's Cyber Incident Response Plan to include a plan for communication with internal and external stakeholders using pre-approved communication templates relating to identified scenarios that may easily be adjusted, if necessary, and promptly sent to the relevant intended recipients if there is a Cyber Incident. The communication plans may be developed to address a range of possible scenarios taking into consideration experience gained from previous incidents.

3. An Authorised Person's test of its conditions and procedures under Rule 3.5.16(3) may be conducted in a variety of ways (for example by using table-top exercises or simulations) and the appropriate scope of testing should be determined each time a test is planned. While an Authorised Person may decide to test only selected procedures at one time, it should ensure that all aspects of the Cyber Incident Response Plan are tested regularly. Testing requirements should be specified in the Cyber Incident Response Plan.

4. The regular review required by Rule 3.5.16(4) should take into account current cyber threat intelligence as well as lessons learnt from previous events and be adjusted to account for new processes and services. Where the review is triggered by a material Cyber Incident (see Guidance item 1 under Rule 3.5.18), the Regulator expects an Authorised Person to assess whether established procedures were followed and whether actions taken were effective. It should also identify key lessons learnt with a view to improving future Cyber Incident response and recovery processes.

3.5.17 (1) If a potential or actual Cyber Incident is detected, an Authorised Person must carry out an investigation to determine its nature and extent.

(2) While the investigation in (1) is ongoing, the Authorised Person must, where applicable, take immediate action to contain the situation to prevent further damage and commence recovery processes based on its Cyber Incident Response Plan.

(3) An Authorised Person must take reasonable care to resume its operations responsibly, including taking the following steps, where applicable:

(a) eliminating all remaining harmful effects of the Cyber Incident;

(b) restoring the affected elements of its IT System and Network;

(c) recovering data affected by the Cyber Incident;

(d) identifying and mitigating all vulnerabilities that were exploited by the Cyber Incident;

(e) remediating vulnerabilities to prevent similar Cyber Incidents in the future; and

(f) communicating appropriately internally and externally.

Notification

3.5.18 An Authorised Person must notify the Regulator immediately, and in any event no later than 24 hours including weekends and public holidays, after it becomes aware, or has information which reasonably suggests, that a material Cyber Incident has occurred, using the prescribed incident reporting form available on the electronic portal.

Guidance

1. The Regulator considers any Cyber Incident that:

a. affects customer information or poses a risk to Client Assets;

b. may lead to material financial loss to the Authorised Person;

c. may have a material reputational impact on the Authorised Person;

d. disrupts critical business functions or information systems;

e. involves the disruption or downgrading of IT System functionality or Network space such as malware and Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks;

f. involves unauthorised intrusion into an Authorised Person's IT Systems or Networks, such as hacking; or

g. involves insider threats;

to be material.

2. In further determining whether a Cyber Incident is material, an Authorised Person should also take into account the extent to which the Cyber Incident:

a. is a crime under Federal legislation, including Federal Decree-law No. (34) of 2021 “On Countering Rumours and Cybercrimes”;

b. results in leakage or corruption of sensitive or confidential information; or

c. affects external stakeholders.

3. The Regulator expects an Authorised Person to consider the need to report Cyber Incidents to other appropriate authorities, such as law enforcement agencies, the FIU or the ADGM Data Protection Commissioner.

4. Rule 8.10.6 also sets out circumstances that require immediate notification to the Regulator.

...