



RULE AND STATEMENT OF GUIDANCE

Cybersecurity and Incident Reporting for
Regulated Entities

October 2026

Table of Contents

List of Acronyms	3
1. Introduction	4
2. Statement of Objectives	4
3. Statutory Authority	4
4. Scope of Application	5
5. Definitions.....	5
6. The Cybersecurity Framework.....	7
7. Governance and Accountability Arrangements	8
8. Cybersecurity Risk Management	10
9. Cybersecurity Resources	13
10. Cybersecurity Awareness and Training	14
11. Outsourcing and Third-Party Risk Management	14
12. Managed Entities.....	17
13. Data Protection	18
14. Incident Response, Recovery, and Reporting	19
15. Technology and Information Systems Controls	22
16. Independent Review, Audit and Testing	25
17. Enforcement.....	25
18. Effective Date.....	25

List of Acronyms

CIMA	Cayman Islands Monetary Authority
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DDoS	Distributed Denial-of-service
DoS	Denial-of-service
DPA	Data Protection Act
IT	Information Technology
MAA	Monetary Authority Act
MFA	Multi-factor Authentication
MITMA	Man-in-the-middle attack
RSOG	Rule and Statement of Guidance
SaaS	Security as a Service
SOG	Statement of Guidance
WAFs	Web Application Firewalls

Rule and Statement of Guidance on Cybersecurity and Incident Reporting for Regulated Entities

1. Introduction

- 1.1. This document establishes the Cayman Islands Monetary Authority's (the "Authority" or "CIMA") *Rule and Statement of Guidance on Cybersecurity and Incident Reporting for Regulated Entities* (the "RSOG").
- 1.2. This RSOG should be read in conjunction with the following:
 - a) Rule and Statement of Guidance on Internal Controls for Regulated Entities;
 - b) Rule on Corporate Governance for Regulated Entities;
 - c) SOG for Corporate Governance for Mutual Funds and Private Funds
 - d) SOG for Outsourcing for Regulated Entities; and
 - e) any other relevant legislation issued by the Cayman Islands Government and regulatory instruments issued by the Authority from time to time.
- 1.3. References to any legislation or regulation shall be construed as references to those provisions as amended, modified, re-enacted or replaced from time to time. For the avoidance of doubt, this document applies to the legislation or regulations to the extent that such provisions in those acts or regulations are in force.
- 1.4. To highlight the Authority's rules within this document, a Rule is written in **light blue** and designated with the letter "R" in the right margin.

2. Statement of Objectives

- 2.1. The Authority acknowledges that technology presents innovation opportunities, greater efficiency and effectiveness, productivity and competitive advantages for Regulated Entities and their customers. However, inadequate management of technology risk may impair Regulated Entities' ability to meet overall business objectives or result in significant liability and reputational damage. Therefore, Regulated Entities must ensure that robust Cybersecurity measures are in place to effectively identify, protect, detect, respond to, and recover from Cybersecurity-related threats, incidents, and breaches.
- 2.2. This RSOG establishes minimum requirements and guidance for Cybersecurity and Incident Reporting for Regulated Entities.

3. Statutory Authority

- 3.1 This RSOG is consistent with the statutory objectives of the Authority as prescribed in Section 6(1)(b) of the Monetary Authority Act ("MAA"), which provides that the principal regulatory functions of the Authority are:
 - "(i) to regulate and supervise financial services business carried on in or from within the Islands in accordance with this Law and the regulatory laws;*
 - (ii) to monitor compliance with the anti-money laundering regulations; and*
 - (iii) to perform any other regulatory or supervisory duties that may be imposed on the Authority by any other law;"*

3.2 Section 34(1)(a) of the MAA provides that:

"After private sector consultation and consultation with the Minister charged with responsibility for Financial Services, the Authority may–

- (a) *issue or amend rules or statements of principle or guidance concerning the conduct of Regulated Entity's and their officers and employees, and any other persons to whom and to the extent that the regulatory acts may apply;"*

4. Scope of Application

- 4.1. This RSOG applies to all Regulated Entities, including controlled subsidiaries as defined in the Banks and Trust Companies Act, but excluding:
 - (a) Regulated Mutual Funds as defined in the Mutual Funds Act; and
 - (b) Private Funds as defined in the Private Funds Act.
- 4.2. Regulated Entities should implement this RSOG in accordance with the proportionality principles, that is, commensurate to the size, complexity, structure, nature of business and risk profile of their operations, following an appropriate assessment of their IT risks, including Cybersecurity.
- 4.3. Regulated Entities such as Class 'B', 'C' and 'D' insurers that are fully managed by a licensed insurance manager are only required to comply with Rules 12.1, 12.2 and 12.3. Insurance Managers must ensure that the cybersecurity framework implemented in respect of insurers that they manage is commensurate with the size, complexity, structure, nature of business and risk profile of the operations of the said insurers and meets their specific needs and risk tolerance.

5. Definitions

- 5.1. The following definitions are provided for the purpose of this RSOG:

- 5.1.1. **"Cloud Computing"** means a model for enabling on-demand network access to a shared pool of configurable computing resources, including networks, servers, storage, applications and services, that can be provisioned and released with minimal management effort or service provider interaction.
- 5.1.2. **"Criticality Classification"** means a method for identifying and prioritising information systems and components.
- 5.1.3. **"Cybersecurity"** is an approach or series of steps, methods, processes, tools or behaviours to protect computer systems, networks, digital devices or data to prevent or manage the risk of damage to, unauthorised use of, exploitation of and, as needed, to restore electronic information and communications systems, and the information they contain, to strengthen the confidentiality, integrity, and availability of these systems.
- 5.1.4. **"Cybersecurity Event"** is any observable occurrence or change within the digital/operational domain (e.g., systems, networks, data,

third-party services) that may indicate a Cybersecurity issue. When such an event is determined to have an adverse impact that requires a response and recovery, it becomes a Cyber incident for reporting purposes.

- 5.1.5. **"Cybersecurity Framework"** means the governance arrangements, policies and procedures, roles and responsibilities, processes and controls, practices, resources and technologies established to identify, assess, manage and mitigate Cyber Risks, and to protect against, detect, respond to and recover from Cyber-attacks.
- 5.1.6. **"Cybersecurity Incident"** means a Cybersecurity event that has been determined to have an impact on the organisation, prompting the need for response and recovery.
- 5.1.7. **"Cyber Resilience"** means the ability to anticipate, withstand and recover from Cybersecurity events; practically, it is measured by the combination of mean time to failure and mean time to recovery.
- 5.1.8. **"Cyber Risk"** means the potential for harm, loss, or disruption arising from the failure, breakdown, misuse, or malicious compromise of information systems, networks, digital technologies, or data of a Regulated Entity. It includes risks resulting from unauthorised access, use, disclosure, disruption, modification, or destruction of digital assets, whether originating from external threat actors, internal actors, system weaknesses, or third-party service providers.
- 5.1.9. **"Cybersecurity Threat"** means any circumstance or event with the potential to adversely impact operations (including its functions and reputation), assets, customers, or other parties, through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service of a Regulated Entity.
- 5.1.10. **"Governing Body"** means the Board of Directors, where the entity is a corporation, the General Partner, where the entity is a partnership, the Manager where the entity is a Limited Liability Company, and the Board of Trustees where the entity is a trust business, or any equivalent governing structure as appropriate, taking into account the nature, size, and legal form of the Regulated Entity.
- 5.1.11. **"Information Technology" ("IT")** means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. The term includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
- 5.1.12. **"Information System"** means a discrete set of electronic information resources organised for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic information, as well as any specialised system, such as industrial/process control systems,

telephone switching and private branch exchange systems, and environmental control systems.

5.1.13. **"Information System Assets"** refer to data, systems, network devices and other IT equipment.

5.1.14. **"Regulated Entity"** means a legal person, a natural person or a legal arrangement that is regulated or supervised by the Authority under the regulatory acts, as defined in the MAA.

5.1.15. **"Risk Management"** means the use of structures, processes and people that identify, assess, mitigate, and monitor all internal and external sources of risk that could have a material impact on operations.

5.1.16. **"Recovery Time Objective"** means the maximum time the components of an Information system can remain in the recovery phase before materially impacting the organisation's mission or business processes.

5.1.17. **"Risk Tolerance"** is the degree of risk of a negative event relating to Cybersecurity that a Regulated Entity is willing to accept.

6. The Cybersecurity Framework

- | | | |
|------|--|---|
| 6.1. | Regulated Entities must establish, implement, maintain and periodically review a documented Cybersecurity Framework commensurate with the size, complexity, structure, nature of business and risk profile of their operations. | R |
| 6.2. | The Cybersecurity Framework must form part of the broader governance, operational resilience and enterprise risk management arrangements of the Regulated Entity. It must support the confidentiality, integrity and availability of systems and data. | R |
| 6.3. | The Cybersecurity Framework must include, at a minimum: | R |
| | a) Governance and Accountability Arrangements; | |
| | b) Cybersecurity Risk Management; | |
| | c) Cybersecurity Resources; | |
| | d) Cybersecurity Awareness and Training; | |
| | e) Outsourcing and Third-Party Risk Management; | |
| | f) Managed Entities; | |
| | g) Data Protection; | |
| | h) Incident Response, Recovery and Reporting; | |
| | i) Technology and Information System Controls; and | |

j) Independent Review, Audit and Testing.

- 6.4. The requirements identified under section 6.3 are further expanded upon in sections 7 through 16 of this RSOG, which set out the Authority's detailed expectations, obligations, and supporting guidance relating to each component of the Cybersecurity Framework.

7. Governance and Accountability Arrangements

- | | | |
|------|--|---|
| 7.1. | Regulated Entities must establish governance arrangements to ensure effective oversight, accountability and management of Cybersecurity risks. | R |
| 7.2. | The Governing Body must approve the Cybersecurity Framework and oversee its effective implementation and ongoing operation. | R |
| 7.3. | Regulated Entities must appoint a suitably qualified senior officer with responsibility and accountability for oversight of the Cybersecurity Framework. | R |
| 7.4. | Regulated Entities must establish clearly documented reporting lines, escalation procedures and managerial responsibilities for Cybersecurity oversight and incident escalation. | R |
| 7.5. | The duties and responsibilities of the Governing Body and Senior Management relating to Cybersecurity should include, but not be limited to: | |
| | (a) Ensuring that a sound and robust Cybersecurity Framework is established and maintained; and taking accountability for and ownership of the Framework and the financial resources for the Framework, including oversight of outsourced Information Technology ("IT") services, cloud providers and any other applicable risks. They should also be involved in key IT decisions; | |
| | (b) Approving appropriate programmes, policies and procedures for Cybersecurity, Cyber Resilience and IT management; | |
| | (c) Ensuring that effective internal controls and Cybersecurity risk management practices are implemented to achieve ongoing security, reliability, resiliency and recoverability; | |
| | (d) Properly assessing cost-benefit issues, including factors such as reputation, customer confidence, consequential impact and legal implications, regarding investment in controls and security measures for computer systems, networks, data centres, operations and backup facilities. The costs of managing Cybersecurity risks should be balanced against the benefits, while maintaining operational and financial stability; | |
| | (e) Ensuring that management supports the senior officer accountable for Cyber Resilience by the creation, implementation, testing and ongoing improvement of Cyber Resilience plans, which are appropriately harmonised across the business; and | |
| | (f) Ensuring that a formal, independent Cybersecurity and Cyber Resilience review/audit of the organisation is carried out periodically, | |

commensurate with its size, complexity, structure, nature of business and risk profile of its operations.

The Role of the Governing Body

- 7.6. The Governing Body of a Regulated Entity must ultimately be responsible for Cybersecurity, and its duties must include, but not be limited to: R
- (a) approval of a written Cybersecurity risk management strategy aligned with the overall business strategy and risk tolerance, as well as approval of completed Cybersecurity risk assessments and Cybersecurity risk management as part of Regulated Entities' overall risk management strategies and programs;
 - (b) approval of a comprehensive Cybersecurity Framework;
 - (c) appropriate oversight of the Risk Management Framework to ensure that policies and processes are implemented effectively;
 - (d) periodic review of the Cybersecurity Framework; and
 - (e) approval of the Cybersecurity audit plan; and ensuring that any findings are addressed in a timely manner.
- 7.7. The Governing Body should also be responsible for:
- (a) Establishing a well-documented, comprehensive Cybersecurity training programme for the Governing Body to help ensure it has the requisite knowledge to competently exercise its oversight function and assess the adequacy and effectiveness of the overall Cyber Resilience programme.
 - (b) Overseeing Cybersecurity and Cyber Resilience. The Governing Body may, as necessary, delegate primary oversight to an existing committee (e.g., the risk committee) or to a new committee (e.g., a Cyber Resilience committee).
 - (c) Having a good command of Cyber risks and the Cybersecurity environment, including regular training in this regard. Governing Body members should receive orientation on joining the entity and receive regular updates on recent threats and trends.
 - (d) Holding management accountable for reporting a quantified and comprehensive assessment of Cyber risks, threats and events as a standing agenda item during its meetings.
 - (e) Ensuring that one senior officer is appointed who is accountable for reporting the capability to manage the implementation of the Cybersecurity Framework and Cyber Resilience programme of a Regulated Entity. The Governing Body should ensure that this officer has regular access to the Governing Body, sufficient authority, command of the subject matter, experience and resources to fulfil these duties.
 - (f) Ensuring that management integrates Cyber Resilience and Cyber risk assessments into the overall business strategy and enterprise-wide risk management, as well as budgeting and resource allocation.

- (g) Annually defining and quantifying the business risk tolerance relative to Cybersecurity and Cyber Resilience, and ensuring that this is consistent with the strategy and risk appetite.
- (h) Carrying out periodic reviews of its own performance in the implementation of the Cybersecurity Framework and Cyber Resilience, and/or seeking independent advice for continuous improvement.

The Role of the Senior Management

7.8. Senior Management should be responsible for:

- (a) Developing, implementing and monitoring the Cybersecurity Framework by documenting appropriate policies and procedures and controls relating to Cybersecurity, Cyber Resilience and IT system controls.
- (b) Ensuring that the appointed senior officer (e.g. CIO or CISO) has access to the Governing Body so that there is clear and ready communication to keep the Governing Body apprised of the Regulated Entity's potential Cyber risks, current threats, incidents or attacks that are deemed material, as well as any necessary changes to the Regulated Entity's Cybersecurity Framework and IT systems.
- (c) Establishing and overseeing programs to ensure employees receive regular Cybersecurity awareness training, including safe practices, phishing prevention, and incident reporting protocols.
- (d) Implementing clear escalation procedures for reporting Cybersecurity Incidents internally and to the Governing Body, ensuring timely communication based on severity and regulatory requirements.
- (e) Ensuring adequate financial, technological, and human resources are allocated to maintain and enhance the Cybersecurity Framework, including support for monitoring, testing, and incident response capabilities.
- (f) Ensuring that Cybersecurity procedures and controls are established, approved, implemented and maintained to support the Cybersecurity Framework and related policies approved by the Governing Body.

8. Cybersecurity Risk Management

- 8.1. The Cybersecurity Framework must be commensurate with the risk tolerance approved by the Governing Body and support the operational resilience objectives of the Regulated Entity. R
- 8.2. Regulated Entities must make reasonable efforts to strengthen Cyber Resilience and their ability to detect, respond to, contain and recover from Cybersecurity Incidents. R
- 8.3. A Regulated Entity's Cybersecurity risk management strategy should involve putting measures in place to ensure the confidentiality, integrity and availability of its data and systems.

- 8.4. The following key components should, at a minimum, be considered by Regulated Entities in their Cybersecurity risk management efforts:

8.4.1. Risk Identification:

- (a) Identification and Criticality classification of Information systems. Identify and maintain an up-to-date physical inventory of all assets, including, but not limited to, computers, servers, routers, and switches, as applicable;
- (b) Identification and assessment of current and emerging threats, risks, and vulnerabilities as well as the impact and likely impact on its IT environment, which comprises internal and external networks, hardware, software, applications, data, processes, systems interfaces, operations and human elements;
- (c) Maintenance of an inventory of Cybersecurity risks and applicable controls;
- (d) Classification of data based on its sensitivity (e.g., public, internal, confidential, highly confidential) and criticality to ensure appropriate protection measures are applied; and

- 8.4.2. Identification and assessment of risks arising from third-party relationships, including vendors, Cloud service providers, and other external partners. This should include evaluating their Cybersecurity posture, contractual obligations, and incident response capabilities.

8.4.3. Risk Assessment and Protection:

- (a) Establishment of an appropriate policy and processes to conduct regular and comprehensive Cybersecurity risk assessments that consider people (i.e. employees, customers and other external parties), processes, data, and technology across all its business lines and geographies, as applicable. Such assessments should be reviewed and updated periodically, and without undue delay, where material changes occur that may impact the Regulated Entity's Cybersecurity risk exposure;
- (b) Analysis and evaluation of the probability of and potential impact and consequences of the identified Cybersecurity risk exposure on Regulated Entities' overall business and operations should an adverse event occur;
- (c) The approach, and key assumptions made when measuring Cybersecurity risks should be clearly documented;
- (d) Establishment of Cybersecurity risk mitigation and control strategies that align with Regulated Entities' business strategy, value of their information assets, risk tolerance and client interests;
- (e) Assessment of Cyber threats to the continuity or operations of Regulated Entities resulting from internally managed functions, outsourced arrangements and critical IT service providers;

- (f) Consideration for securing insurance against various Cybersecurity risks, including recovery costs and compensation. Where a regulated entity determines that Cybersecurity insurance is not required, the basis for this determination should be supported by a documented risk assessment that demonstrates the decision is appropriate and commensurate with the entity's Cybersecurity risk profile;
- (g) A clear policy should be in place to detail the level of protection required based on the risk and criticality rating of the Information system. The policy should include appropriate safeguards to ensure critical products and services remain available and to enable the Regulated Entity to prevent, mitigate, or contain the impact of a potential Cybersecurity event. Risk or business impact assessments should support evidence of protection;
- (h) Conduct regular testing and validation of Cybersecurity controls (e.g., penetration testing, vulnerability assessments, and control effectiveness reviews) to ensure they operate as intended and remain effective against evolving threats;
- (i) Address human factor risks by implementing mandatory security awareness and training programs for employees and relevant stakeholders. Training should cover phishing prevention, safe data handling, password hygiene, and incident reporting protocols; and
- (j) A comprehensive risk assessment should be conducted before the adoption or material use of a technology solution including cloud computing services.

8.4.4. Risk Monitoring and Reporting:

- (a) Implementation of documented monitoring/surveillance and detection policies, techniques and systems that allow real-time monitoring and detection of threats (examples include, but are not limited to, firewalls, web application firewalls ("WAFs"), network behaviour analysis, anti-virus, and third-party monitoring tools);
- (b) The monitoring/surveillance system should alert the Regulated Entity to any abnormal IT system activities, transmission errors, cyber-attacks, or unusual online transactions;
- (c) Continuous monitoring of emerging Cybersecurity threats such as denial-of-service attacks, internal sabotage and malware infestations to facilitate prompt detection of intrusion attempts, unauthorised or malicious activities by internal and external parties;
- (d) Monitoring and development of Cybersecurity metrics, considering such things as risk events, regulatory requirements and audit findings, to highlight systems, processes or infrastructure that have the highest risk exposure;
- (e) Ongoing reporting to the Governing Body of significant risks, associated status of containment and recovery actions and plans, including recommendations on how to mitigate similar events in the future;

- (f) Completing periodic reviews and updates of Regulated Entities' Cybersecurity risk management processes, re-evaluating past risk-control methods with improved testing, as well as assessing the adequacy and effectiveness of their Cybersecurity risk management processes; and
- (g) Ensuring timely reporting of significant Cybersecurity Incidents or breaches to the Authority, in accordance with applicable laws and rules.

9. Cybersecurity Resources

- 9.1. Regulated Entities must ensure that adequate financial, technological and human resources are allocated to support the implementation, operation, monitoring and maintenance of the Cybersecurity Framework. R

- 9.2. Regulated Entities must ensure that personnel responsible for Cybersecurity possess appropriate authority, competence, experience and resources commensurate with the size, complexity and risk profile of the Regulated Entity. R

Selection of Employees and Third-Party Service Providers

- 9.3. Regulated Entities should implement a comprehensive and effective screening process, with stringent selection criteria, to ensure careful selection of employees, vendors, and contractors who support technology functions and to minimise Cyber risks arising from system failure, internal sabotage, or fraud.

Senior Officer Appointment (Chief Information Security Officer/Chief Information Officer)

- 9.4. A senior officer, such as a CISO, CIO, or similar position, should be appointed to oversee the Regulated Entity's Cybersecurity Framework and to liaise with the Governing Body, following best practices and staying current with all related technologies and Cybersecurity trends.
- 9.5. The appointed senior officer (e.g., CIO or CISO) should be suitably qualified, experienced and have a good understanding and knowledge of IT systems and Cybersecurity.
- 9.6. The appointed senior officer (e.g., CIO or CISO) should be provided with sufficient operational authority to carry out their role.

Incident Management Response Team

- 9.7. Regulated Entities must identify, establish, and maintain an incident management and response team with clearly defined roles and responsibilities. This team must be appropriately trained and prepared to activate in the event of a Cybersecurity Incident or breach, ensuring timely detection, containment, response, communication, and recovery. R
- 9.8. The Regulated Entity must ensure that each member of the incident management and response team has clearly defined roles and responsibilities and is appropriately trained and prepared to carry out the same, commensurate R

with the size, complexity, structure, nature of business and risk profile of its operations.

10. Cybersecurity Awareness and Training

- 10.1. Regulated Entities must establish a comprehensive training and awareness programme¹ relating to Cybersecurity and Cyber Resilience that is endorsed by its Governing Body and/or senior management. The programme must be delivered on an ongoing basis, at least annually. It should be reviewed and updated periodically to ensure the programme's content remains current and relevant, taking into account the evolving nature of technology and emerging risks, including those specific to the Regulated Entity. R
- 10.2. Regulated Entities should have a formalised plan to provide ongoing technical training to their Cybersecurity personnel and IT unit/team (including those involved in developing, maintaining and operating websites and systems) on IT systems and current and emerging Cybersecurity subject areas, as well as security principles to ensure that they are knowledgeable and aptly trained for their specific IT or Cybersecurity roles and functions.
- 10.3. Regulated Entities should make every effort to ensure that they regularly disseminate Cybersecurity information to their customers or take any other action to help increase their customers' level of Cybersecurity awareness.
- 10.4. Regulated Entities should ensure that all employees are trained to understand at a minimum the Cyber risks to which the entity is exposed and the mitigating measures employed to reduce the occurrences of Cyber Incidents.
- 10.5. The CIO, CISO, or other similarly appointed senior person should ensure that there is enterprise-wide ongoing training to new and existing employees on Cybersecurity to ensure increased awareness and enterprise-wide efforts to prevent or minimise Cyber-attacks and Cyber Incidents.
- 10.6. Regulated Entities' training programmes should ensure that their governing bodies are equipped with the requisite knowledge to competently exercise the oversight function and appraise the adequacy and effectiveness of the Regulated Entities' overall Cyber Resilience programmes.
- 10.7. Regulated Entities should ensure Cybersecurity policies and procedures are communicated to senior management and employees at all levels, and training is conducted regularly.

11. Outsourcing and Third-Party Risk Management

- 11.1. Regulated Entities that outsource Cybersecurity and/or IT functions either externally to third parties or internally to affiliated entities must: R
- (a) remain ultimately responsible for outsourced IT functions and their Cybersecurity; and
 - (b) ensure that they assess, and document/can evidence the service

¹ Training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus an individual's attention on an issue or set of issues. (Source: NIST Special Publication 800-16)

provider(s)' compliance with this RSOG and the *SOG for Outsourcing for Regulated Entities*; and

- (c) also consider outsourcing arrangements beyond IT-related functions, which may also present a Cybersecurity risk.

11.2. The Authority expects that the ultimate responsibility and accountability for outsourcing arrangements and other third-party dependencies (either an affiliated entity within a group or an entity that is external to the Regulated Entity), supporting or potentially negatively impacting Internet activities and IT systems, remain with Regulated Entities; and material outsourcing arrangements, including critical IT service providers, should be approved by their Governing Body.

11.3. Regulated Entities must notify the Authority, within a reasonable timeframe, of any changes to material outsourcing arrangements relating to Cybersecurity functions, critical IT services, or other technology services that are material to the operations of the Regulated Entity. This may include the establishment of new arrangements and the termination of existing arrangements.

R

11.4. Where Regulated Entities outsource to a professional security service provider, for example, provide 'Security as a Service' ("SaaS"), mechanisms should be in place to allow the Governing Body and senior management to ensure that Cybersecurity is being properly monitored and secured at a secure site and deficiencies addressed in a timely manner. The obligations and expectations regarding outsourcing requirements set out in the RSOG and other relevant measures should be complied with. Regular reports from the third-party service provider should be circulated to the Governing Body and senior management.

11.5. Given that outsourcing arrangements could change the Cybersecurity risk profile of Regulated Entities, including critical IT service providers, Regulated Entities should assess and document whether an outsourcing arrangement is material, taking into account its potential impact on the Regulated Entity's operations, Cybersecurity risk profile and operational resilience. The following steps should then be considered:

- (a) Prior to the appointment of a service provider, carry out due diligence to determine the viability, capability, reliability, track record and financial position of these service providers. The due diligence process should include any related subcontracting arrangements. Due Diligence Assessments should also be performed on a regular basis thereafter (at least annually or in keeping with the level of the perceived risk) in order to ensure that the Service Provider is fit and proper and can effectively perform the outsourced material function or activity, and to ensure high ethical and professional standards;
- (b) Contractual terms and conditions governing the roles, relationships, obligations and responsibilities of all service providers should be set out fully in written agreements. The requirements and conditions covered in the agreements generally include performance targets, service levels, availability, reliability, scalability, compliance, audit, security (including Cybersecurity), data protection, reporting requirements (e.g. incidents), contingency planning, disaster recovery capability and backup processing facility;

- (c) The contractual agreements with the service providers should confirm that the Authority or its authorised agent can perform an assessment of the service provider's IT systems and Cybersecurity control environment associated with the outsourced service(s) being carried out on behalf of the Regulated Entity;
- (d) Regulated Entities should require the service provider to have or implement Cybersecurity policies, procedures and controls that are at least as stringent as it would expect for its own operations;
- (e) Regulated Entities should monitor and review the security policies, procedures and controls of the service provider regularly to ensure they have robust controls in place to maintain security and compliance in the cloud as per set international standards², including commissioning or obtaining periodic independent audits on Cybersecurity adequacy and compliance in respect of the operations and services provided;
- (f) The outsourcing agreement should require the service provider to have or develop and establish a Cybersecurity Incident Recovery Contingency Framework, which defines its roles and responsibilities for documenting, maintaining and testing its contingency plans and recovery procedures;
- (g) The service provider's disaster recovery plan for Regulated Entities should be reviewed, updated and tested to reflect changes in technology, Cybersecurity, and operational requirements. The plan should consider worst-case disruption scenarios, including the unavailability of existing service providers, and identify viable alternatives for restoring IT services. Regulated Entities should ensure the plan is shared with relevant stakeholders and that they are appropriately trained to execute it;
- (h) Regulated Entities should ensure that there is an exit strategy in place in the event of termination of the relationship;
- (i) Regulated Entities should be able to apply this RSOG to any of their material outsourcing arrangements, including their critical IT service providers, as if it were not an outsourced function or service;
- (j) Regulated Entities should implement processes to monitor the levels of Cyber risk preparedness for material outsourcing arrangements and critical IT service providers;
- (k) Regulated Entities should have processes in place to ensure the timely notification of Cyber Incidents from their service providers with which they have one or more material outsourcing arrangements and their critical IT service providers;
- (l) Regulated Entities should conduct a risk assessment with respect to the jurisdiction(s) in which potential material outsourcing arrangements and critical IT service providers are, if outside the Cayman Islands, and appropriately mitigate any identified Cybersecurity risks, as necessary;

² International certifications include ISO 9001:2015 Compliance, Cloud security alliance, Cyber GRX, Cybervadis, Security standards council etc.

- (m) Regulated Entities should regularly assess their aggregate exposures relating to material outsourcing arrangements and critical IT service providers and effectively mitigate and manage any vulnerabilities, threats and Cyber risks that may result from the outsourcing arrangement or critical IT service provider(s);
- (n) Regulated Entities should maintain a centralised log of all their material outsourcing arrangements and critical IT service providers, which should be updated on an ongoing basis. The Authority should have access to the log at any time upon request;
- (o) Some Regulated Entities may choose to rely on Cloud computing in their IT system architecture. The Authority considers the use of Cloud computing to be a form of outsourcing. As such, in performing their due diligence for all forms of outsourcing arrangements, Regulated Entities should be aware of Cloud computing's unique attributes and risks, especially in areas such as data integrity, sovereignty, commingling, platform multi-tenancy, recoverability, confidentiality, regulatory compliance, auditing, and data offshoring;
- (p) Where a Cloud computing service provider adopts multi-tenancy and data commingling architectures to process data for multiple customers, Regulated Entities should consider Cloud computing service providers' abilities to isolate and clearly identify their customer data and other Information system assets for protection;
- (q) In the event of contract termination with a Cloud computing service provider, either on expiry or prematurely, Regulated Entities should have the contractual power and means to promptly remove or destroy data stored at the service provider's systems and backups;
- (r) Regulated Entities should verify the Cloud computing service provider's ability to recover the outsourced systems and IT services within the stipulated Recovery Time Objective before contracting with the service provider; and
- (s) In all cases of outsourcing, a Regulated Entity should satisfy itself that the service provider is carrying out its functions in compliance with applicable Acts, regulations, and relevant regulatory measures, where applicable.

11.6. For the avoidance of doubt, outsourcing includes arrangements entered into with third-party service providers, parent entities, subsidiaries, affiliates, shared service centres and other entities within the same corporate group.

12. Managed Entities

12.1. The Authority recognises that certain Regulated Entities are fully managed by a licensed service provider and may rely on the Cybersecurity Framework implemented and maintained by that service provider, rather than establishing a separate, standalone Cybersecurity Framework of their own. In such circumstances, Regulated Entities managed by entities licensed by the Authority must, through their Governing Body, make appropriate enquiries and satisfy themselves that the Cybersecurity Framework applied by the service provider is

R

appropriate, effective, and commensurate with the Cybersecurity risks to which the Regulated Entity is exposed.

12.2. Regulated Entities, as referred to in 12.1:

R

- (a) must ultimately be responsible for their Cybersecurity and for assessing the service provider(s)' compliance with this RSOG; and
- (b) must satisfy themselves that the Cybersecurity Framework to be applied to the services provided to them is appropriate to the Cybersecurity risks posed to them as a result of the use of technology and emerging Cybersecurity threats.

12.3. The Governing Body of a Regulated Entity referred to in section 12.1 must require the service provider to report any Cybersecurity-related breaches that pertain to the Regulated Entity. A mechanism must be in place to ensure that the Regulated Entities are aware, through the Governing Body, of the services provided by their insurance managers.

R

13. Data Protection

13.1 Regulated Entities must demonstrate that data protection is part of their Cybersecurity Framework, taking into consideration the provisions of the Data Protection Act and the guidance issued by the Cayman Islands Ombudsman on data protection.

R

13.2 Regulated Entities should implement policies, procedures, internal control mechanisms and training that:

- (a) support the protection of the privacy of customers' personal information and sensitive personal information, including preventing or minimising the misuse or inappropriate communication of personal information to third parties; and
- (b) assess the Cyber risks that may compromise the privacy of personal information, including any exposures related to the use of third-party providers.

13.3 Regulated Entities should establish suitable response measures, where a failure to protect the privacy of personal information occurs, including matters such as timely notification to affected customers and relevant competent authorities.

13.4 Regulated Entities should comply with applicable local and international data protection laws and regulatory requirements to ensure protection of sensitive and confidential information at all points along the flow of data. This includes data at endpoint (such as end user devices – mobile, notebooks, personal computers, and removable media), data in transit (data flowing in networks or between sites) and data at rest (data stored in databases, servers, on backup media and in storage platforms).

13.5 Regulated Entities should ensure that endpoint devices protect confidential information stored on the devices with strong encryption. There should be appropriate controls to address the risks of data theft, data loss and data leakage from endpoint devices, customer service locations and call centres.

- 13.6 Regulated Entities should, as much as possible, avoid the use of unsafe internet services such as social media sites, cloud-based internet storage sites, and web-based emails to communicate or store confidential information. Appropriate control measures should be in place to prevent and detect the use of such services within Regulated Entities, or to report issues with such services should they be employed.
- 13.7 Whenever confidential data is exchanged internally or externally, Regulated Entities should take appropriate measures to send information via encrypted channels (e.g. via encrypted mail protocol) or encrypt the email and its contents using strong encryption with adequate key length. The encryption key should be sent via a separate transmission channel to the intended recipients. Alternatively, Regulated Entities may choose other secure means to exchange confidential information with their intended recipients.
- 13.8 Confidential information stored on Regulated Entities' IT systems, servers and databases should be encrypted and protected through strong access controls and restricted access on a least privilege basis³.
- 13.9 Regulated Entities should assess various methods by which data could be securely removed from storage media and implement measures to prevent the loss of confidential information through the disposal of IT systems.
- 13.10 Regulated Entities should ensure that sensitive or confidential information stored on and accessed by mobile devices is encrypted to ensure the confidentiality and integrity of this information in storage and transmission.
- 13.11 Regulated Entities should ensure that the processing of sensitive or confidential transaction and customer information occurs in a secure environment.
- 13.12 Regulated Entities should take steps to educate customers on security measures to protect their own mobile devices from viruses and other errant software, which could lead to malicious damage and have harmful consequences.

14. Incident Response, Recovery, and Reporting

- 14.1 Regulated Entities must, without undue delay, notify the Authority in writing of an incident when it is deemed to have a material impact or has the potential to become a material incident, and no later than seventy-two (72) hours upon becoming aware of the said incident. R
- 14.2 Regulated Entities must ensure that their internal procedures clearly specify the required timing and immediacy for incident reporting, and must enforce those procedures in practice, particularly where reputational risk or imminent public disclosure is involved. R
- 14.3 Regulated Entities must ensure incidents are reported to the Authority using the prescribed format and through the applicable channels. R
- 14.4 The prescribed channel is a digital incident reporting form provided by the Authority, which must be completed in full and submitted via the Authority's secure submission portal for assessment. The Authority expects Regulated

³ Least privilege is defined as assigned privileges on a "need-to-have" basis.

Entities to ensure that all required fields in the form are completed accurately and that supporting documentation is attached where applicable. Submission through any other means will not be considered compliant unless expressly authorised by the Authority.

- 14.5 Regulated Entities must establish and maintain documented criteria within their Incident Management Framework for assessing the materiality and criticality of Cybersecurity Incidents, taking into account the nature, scale, scope, duration, and potential impact of the incident. R
- 14.6 Regulated Entities should establish, implement and maintain documented Cybersecurity Incident response procedures that support the effective identification, escalation, containment, eradication, recovery and post-incident review of Cybersecurity Incidents.
- 14.7 In determining whether an incident is material and reportable to the Authority, Regulated Entities must consider whether the incident falls within one or more of the following criteria, or any other circumstance that may reasonably be expected to result in a material impact on the Regulated Entity, its customers: R
- (a) Material impact on the Regulated Entity's internal operations;
 - (b) The event results in the unauthorised dissemination of any personal data either internally or externally;
 - (c) Significant operational impact on internal users that is material to customers or business operations;
 - (d) Extended disruptions to critical business systems or internal operations;
 - (e) Number of external customers impacted is significant or growing;
 - (f) If it is determined that there is potential reputational impact, either to the Regulated Entity or the Cayman Islands as a whole, notification to the Authority must occur immediately if there is any risk of premature public disclosure;
 - (g) Any loss of any card payment information, beneficial owner details, or any personally identifiable information;
 - (h) Loss or exposure of any data in violation of any applicable data protection Acts and other regulatory requirements, both foreign and domestic;
 - (i) Financial loss or theft, including misappropriation of client assets;
 - (j) Compromise of Private Keys or Wallets;
 - (k) Third party or outsourced vendor breaches; and
 - (l) Extended service outages affecting customers.
- 14.8 Cyber Incident response procedures should include predefined escalation criteria that are commensurate with the severity and criticality of the Cybersecurity Incident and aligned with the Regulated Entity's Cybersecurity Criticality classification.

- 14.9 Regulated Entities must include risk ratings that correspond to the materiality of the Cybersecurity Incidents in their notifications to the Authority. R
- 14.10 Regulated Entities must notify affected persons if a Cyber-attack results in the breach of non-public information or disrupts a service that is utilised, including information on the action taken to contain (as necessary), remedy and recover from the breach. R
- 14.11 Regulated Entities must also track and document all notifications made to affected persons as part of their incident response and reporting process. They must provide timely follow-up communications to keep affected Persons informed of progress, additional actions, and final resolution. R
- 14.12 In the case of loss of financial assets, personally identifiable data, or any other information covered under an applicable data protection Act, Regulated Entities should communicate to affected individuals, the Authority and the Ombudsman, where applicable, as quickly as possible or within appropriate time standards established by the Regulated Entities or the Data Protection Act (DPA).
- 14.13 The Authority expects that Regulated Entities provide regular updates to the Authority as new information becomes available, and until all material details about the incident have been provided.
- 14.14 Until the incident is contained or resolved, the Authority expects Regulated Entities to provide situation updates to the Authority, including any short-term and long-term remediation actions and plans.
- 14.15 Prior to formally closing a Cybersecurity Incident, Regulated Entities should ensure that:
- (a) affected services have been restored;
 - (b) appropriate processing and transmission controls to protect the integrity of their systems and data;
 - (c) Lost or corrupted data has been restored, where applicable; and
 - (d) appropriate remediation actions have been implemented to reduce the likelihood of recurrence.
- 14.16 Depending on the severity, impact and velocity of the incident, the Authority may require that Regulated Entities report using a specific method and at a specific frequency.
- 14.17 Regulated Entities should periodically test their incident response, containment and recovery arrangements through exercises appropriate to the size, complexity, structure, nature of business and risk profile of their operations. Such testing may include tabletop exercises, simulations or other appropriate testing methodologies.
- 14.18 Once a Regulated Entity has contained and recovered from a Cybersecurity Incident, it should complete a post-incident review documenting lessons learned and a plan of action to address identified deficiencies and strengthen IT controls.

Where appropriate, the review should include:

- (a) cyber forensic investigations;
- (b) a chronology of significant events;
- (c) identification of the root cause and any control deficiencies;
- (d) an assessment of the effectiveness of the incident response and recovery process; and
- (e) remediation actions designed to reduce the likelihood and impact of similar incidents.

15. Technology and Information Systems Controls

- 15.1 The Cybersecurity Framework of a Regulated Entity should include documented policies and baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within the IT environment.
- 15.2 Regulated Entities should implement:
 - (a) physical and logical access security to allow only authorised employees to access their internet operations and IT systems; and
 - (b) appropriate processing and transmission controls to protect the integrity of their systems and data.
- 15.3 Regulated Entities should ensure that their personnel, responsible for supporting internet operations, IT systems and Cybersecurity, have their duties and access to IT systems, databases and application resources scrutinised with clear segregation of duties in place.
- 15.4 Regulated Entities should establish a Control Framework around the management of their IT system that should comprise the governance structure, processes and procedures for change management, software release management, incident and problem management, as well as capacity management.
- 15.5 Where a Regulated Entity develops, acquires, or materially customises software, applications, or technology solutions, it must implement secure software development lifecycle controls commensurate with the size, complexity, structure, nature of business and risk profile of its operations. Such controls should include, where applicable, secure coding practices, code reviews, change management procedures, vulnerability testing, security testing prior to deployment, and the timely remediation of identified weaknesses.
- 15.6 Regulated Entities should ensure that clear audit trails exist for all internet transactions. Effective internal controls should be in place in highly automated environments, and these controls should be independently audited, particularly for all critical internet events and applications.

R

- 15.7 Regulated Entities should develop a technology refresh plan⁴ to ensure that the IT infrastructure is properly supported, up to date, and replaced in a timely manner as needed.
- 15.8 Regulated Entities should ensure that maintenance and repairs relating to IT infrastructure are performed in accordance with the entities' policies and procedures. Maintenance and repairs should be appropriately approved, logged, and performed in a manner to prevent unauthorised access.
- 15.9 Regulated Entities should carry out vulnerability assessments and realistic penetration tests that replicate sophisticated, current attacks based on current and targeted threat intelligence, commensurate with the size, complexity, structure, nature of business and risk profile of its operations, and the nature of Regulated Entities' risk exposures. Such assessments and testing should, at a minimum, be carried out annually or more frequently, depending on whether major changes to defences are made or threats perceived. The assessments and testing should also include, but not be limited to (as applicable):
- (a) Regular hardware and software vulnerability scans and testing of client servers and network infrastructure to identify security control gaps;
 - (b) Regular penetration testing of the network boundary (e.g. open network entry and exit points) to identify security control gaps;
 - (c) Regular testing with third-party Cyber-mitigating services;
 - (d) Regular Cyber-attacks (including distributed denial-of-service ("DDoS") and phishing attacks) and recovery simulation exercises; and
 - (e) Consideration of the impact of an internet outage across the Cayman Islands for an extended period of time on their assessment, testing and risk assessment generally.
- 15.10 Regulated Entities should establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within the IT environment.
- 15.11 Regulated Entities should install network security devices, such as firewalls, as well as intrusion detection and prevention systems, at critical junctures of their IT infrastructure to protect their network perimeters. Regulated Entities should deploy firewalls or similar measures within their internal networks to minimise the impact of security exposures originating from third-party or overseas systems (e.g., running code developed by an overseas firm), as well as from their trusted internal networks. Where cloud services are utilised, appropriate cloud security controls should also be implemented to safeguard data and systems hosted in cloud environments, ensuring alignment with industry best practices.

Payment Systems and Card Payment Cards

- 15.12 Regulated Entities that accept, store, process, and/or transmit cardholder data should maintain a secure environment and ensure that they are Payment Card Industry Data Security Standard compliant.

⁴ Technology refresh is the cycle of regularly updating key elements of an IT infrastructure to maximise system performance.

- 15.13 Regulated Entities should implement IT security measures that apply to their participation in payment systems, including but not limited to, point of sale terminals; online services and payments (inclusive of mobile platforms); and other emerging technologies, as applicable.
- 15.14 Regulated Entities should conduct a risk assessment to identify possible fraud scenarios with respect to the issuance of payment cards and put in place appropriate measures to counteract payment card fraud via mobile devices.

Use of the Internet

- 15.15 Regulated Entities should establish suitable policies and controls to:
- (a) Guard against potential Cyber-attacks or minimise the impact of such attacks and Cybersecurity Incidents on their internet systems where they provide financial services online, and customers transact online; and
 - (b) Ensure that transactions performed over the internet, as well as online login credentials, passwords, personal identification numbers and other sensitive personal or account information, are adequately protected, authenticated and secured against exploits, including but not limited to account takeovers, automated teller machine skimming, card cloning, hacking, phishing, multi-factor authentication ("MFA") hijacking, ransomware and malware.
- 15.16 Educate users on safe internet practices, including recognising phishing attempts, using strong passwords, enabling multi-factor authentication, and avoiding insecure networks when conducting online financial transactions. Regulated Entities should properly evaluate the security requirements of their Internet systems and adopt encryption algorithms that conform to well-established international standards and are rigorously scrutinised.
- 15.17 Regulated Entities should consider the deployment of MFA at login for all types of online financial systems and transaction-signing for authorising transactions.
- 15.18 Regulated Entities should maintain high resiliency and availability of online systems and supporting systems. They should put in place measures to plan and track capacity utilisation, as well as to guard against online attacks such as denial-of-service (DoS) and distributed denial-of-service (DDoS). Where cloud services are utilised, Regulated Entities should implement cloud-specific resilience measures, such as multi-region redundancy, automated failover, secure backup strategies, and capacity scaling, to ensure continuity and minimise downtime during Cyber incidents or service disruptions.
- 15.19 Regulated Entities should take appropriate measures to minimise exposure to other forms of Cyber-attacks, such as Business E-mail Compromise schemes, also known as middleman attacks, man-in-the-middle attack ("MITMA"), man-in-the-browser attack or man-in-the-application attack.
- 15.20 Regulated Entities should ensure sufficient information is available on their websites for potential customers to make an informed assessment of the institution's identity, including the physical address of the Regulated Entity and its head office. As a matter of best practice, websites should also state that the entity is regulated by the Authority and, where applicable, its home supervisor,

with prominent notification provided before entering any internet transaction.

- 15.21 Regulated Entities should maintain clear and accessible privacy notices outlining how customer data is collected, stored, processed, and used in accordance with applicable data protection and privacy requirements.

16. Independent Review, Audit and Testing

- 16.1 To support compliance with Rule 6.3, reviews of a Regulated Entity's Cybersecurity Framework should incorporate periodic assessments of Cyber and IT risks to confirm that the controls, governance structures, and operational processes remain appropriate and effective. These reviews should consider evolving threats and emerging technologies to ensure that the overall Framework stays robust, adaptable, and aligned with the Regulated Entity's IT system management requirements.
- 16.2 The Cybersecurity Framework should include a "feedback loop" which ensures transparency and allows the Governing Body and senior management to take necessary action in response to changes in the IT and Cybersecurity risk profile of Regulated Entities, particularly between the Governing Body and the designated CIO or CISO where such positions exist in Regulated Entities or some other similar position that would be responsible for liaising with the Governing Body. The feedback loop will also ensure that decisions made by the Governing Body and Senior Management are implemented and their effects monitored to determine whether they are, in fact, appropriate.
- 16.3 The Cybersecurity framework should be tested on a periodic basis for effectiveness. Accordingly, if, following the review of the Cybersecurity Framework, a Regulated Entity finds it deficient or ineffective, it should update or amend it as needed.
- 16.4 Regulated Entities are expected to retain a copy of the submitted report and all supporting documentation, correspondence, and evidence for a minimum of five (5) years. These records must be maintained to ensure traceability, auditability, and accessibility, and must be made available to the Authority upon request. This requirement aligns with FIRE Framework's emphasis on robust data governance and post-incident review capabilities.

17. Enforcement

- 17.1 Where the Authority determines a breach of these Rules has occurred, the policies and procedures of the Authority, as contained in its Enforcement Manual, will apply, in addition to any other powers provided in the MAA and the relevant regulatory acts.

18. Effective Date

- 18.1 This RSOG will come into effect within three (3) months of the date that it is published in the Gazette.



Pavilion East, Cricket Square
PO Box 10052
Grand Cayman KY1-1001
Cayman Islands

Tel: +1 (345) 949-7089
www.cima.ky