



PRIVATE SECTOR CONSULTATION

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

October 2026

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

A. Introduction

1. The Cayman Islands Monetary Authority ("CIMA" or "the Authority") seeks consultation and comment from private sector associations concerning the proposed *Rule and Statement of Guidance on Cybersecurity and Incident Reporting for Regulated Entities (the "RSOG" or "proposed measure")* (attached as **Appendix I**).
2. Requirements specific to the private sector consultation are outlined in section 4(1) of the Monetary Authority Act (2020 Revision) ("MAA"), which states:

"(b) before proceeding with the proposed measure, the Authority shall have regard to any representations made by the private sector associations, and shall give a written response, which shall be copied to all the private sector associations."

3. Section 34(1)(a) of the MAA states 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 licensees and their officers and employees, and any other persons to whom and to the extent that the regulatory laws may apply;"

B. Background and Rationale

4. Recognising the increasing importance of cybersecurity and technology risk within the financial services sector, in 2020, the Authority issued a *Rule and Statement of Guidance on Cybersecurity for Regulated Entities* to establish baseline requirements for cyber risk management and incident reporting. Since their issuance, significant technological advancements, rising cyber threats, and evolving international standards have underscored the need to enhance the existing framework, particularly regarding Cyber Incident Reporting ("CIR").
5. Since the issuance of the existing cybersecurity framework, international standard-setting bodies have continued to develop their expectations for cyber resilience and incident reporting. In 2023, the Financial Stability Board ("FSB") introduced the Format for Incident Reporting Exchange ("FIRE"), which promotes a harmonised and standardised approach to incident reporting and establishes structured reporting data points relating to matters such as incident type, root cause, operational impact, recovery timelines, and remediation measures. These developments, together with evolving international standards advanced by organisations such as the Basel Committee on Banking Supervision ("BCBS") and the Group of International Finance Centre Supervisors ("GIFCS"), underscore the need for a more structured and globally aligned cybersecurity and incident reporting framework.
6. In response to these developments, the Authority conducted a gap assessment comparing its existing CIR requirements against the FIRE framework and identified several areas where the current framework is only partially aligned. Key gaps include limited reporting on operational impact, customer and staff notifications, incident discovery methods, and remediation activities. In addition, a thematic cybersecurity review conducted by the Authority in June 2023 identified weaknesses in incident

notification practices, including inadequate procedures to meet the Authority's seventy-two (72)-hour reporting requirement and insufficient integration of local regulatory obligations into group-wide cybersecurity policies.

7. To address these identified gaps and reflect evolving international standards and supervisory expectations, the Authority is proposing to consolidate and revise the existing Rule and Statement of Guidance into a single *Rule and Statement of Guidance on Cybersecurity and Incident Reporting for Regulated Entities* ("RSOG") (**Appendix 1**). The revised RSOG seeks to provide a clearer, more coherent regulatory framework, strengthen incident notification requirements, and more explicitly link mandatory obligations to supporting guidance. The proposed revisions are intended to improve consistency, interpretation, data collection, analysis, and compliance outcomes across the financial services industry.

C. International Standards

8. International standard-setting bodies recognise the increasing importance of cybersecurity, Technology Risk Management ("TRM"), operational resilience and effective Cyber Incident Reporting ("CIR") within the financial services sector. International standards and recommendations increasingly emphasise robust governance, cyber risk management, business continuity, incident response and recovery, and consistent and timely reporting of material cyber incidents. Some of the relevant international standards and recommendations are summarised below:

Basel Committee on Banking Supervision ("BCBS")

9. The BCBS's supervisory focus has evolved from traditional operational risk management towards strengthening operational resilience against increasing technological and cyber threats. The 2025 updates to the Basel Core Principles for Effective Banking Supervision ("BCPs") emphasise cybersecurity risk mitigation as a core component of operational resilience and business continuity planning. The BCPs also support supervisory frameworks that assess the ability of financial institutions to prevent, withstand and recover from cyber incidents, thereby supporting the stability and integrity of the financial system.

International Organisation of Securities Commissions ("IOSCO")

10. IOSCO's *Objectives and Principles of Securities Regulation* address operational risk and resilience, business continuity and internal controls through Principles 29 and 30. More recently, IOSCO has strengthened its guidance on cybersecurity and operational resilience through publications including its 2021 *Principles on Outsourcing* and its 2023 *Final Report on Operational Resilience of Trading Venues and Market Intermediaries*. These publications emphasise cyber risk management, third-party and outsourcing risk oversight, business continuity and operational resilience, including effective incident response and reporting arrangements to protect investors, support market integrity and strengthen resilience against increasingly sophisticated cyber threats.

International Association of Insurance Supervisors ("IAIS")

11. Between 2020 and 2023, the IAIS strengthened its expectations regarding cyber risk management and operational resilience through its Insurance Core Principles ("ICPs"), including those relating to Corporate Governance (ICP 7), Risk Management and Internal Controls (ICP 8), and Enterprise Risk Management (ICP 16), together with its work concerning operational resilience within the insurance sector. These standards emphasise robust governance, operational risk management, business

continuity, third-party risk oversight and recovery capabilities to enable insurers to prepare for, withstand, respond to and recover from cyber and other operational disruptions, thereby supporting policyholder protection and financial stability.

Group of International Finance Centre Supervisors ("GIFCS")

12. The GIFCS' *Standards on the Regulation of Trust and Corporate Service Providers* have strengthened the focus on cybersecurity and operational resilience through expectations relating to governance, risk management, business continuity and incident reporting. The 2025 consultation to update the Standards also included recommendations to formally codify cybersecurity requirements, reinforcing supervisory expectations and supporting the stability and integrity of international financial centres.

Financial Stability Board ("FSB")

13. In 2023, the FSB published its *Recommendations to Achieve Greater Convergence in Cyber Incident Reporting*, which seeks to promote greater harmonisation of CIR practices across jurisdictions through common data requirements, standardised reporting formats and interoperable reporting frameworks. The FSB identified fragmented reporting requirements as creating inefficiencies, increasing reporting burdens and potentially hindering timely responses to cross-border cyber incidents. Its recommendations therefore promote more consistent incident definitions, common data requirements, phased reporting, appropriate reporting triggers and calibrated reporting windows.
14. To further support greater convergence in CIR, the FSB developed the *Format for Incident Reporting Exchange ("FIRE")*, a standardised, non-binding data format designed to improve the reporting of cyber incidents across jurisdictions and financial institutions. FIRE seeks to promote cross-border interoperability, enable timely and consistent communication, and support coordinated responses to cyber threats that may pose systemic risks.
15. Importantly, FIRE does not prescribe whether an incident must be reported, the applicable reporting trigger, the reporting timeframe, or the authority to which an incident must be reported. Rather, it complements existing national regulatory requirements by providing a standardised format for the information required when an incident is reportable. Accordingly, CIMA remains responsible for establishing the applicable reporting triggers and timelines, while FIRE informs how incident information is structured, captured and transmitted to promote compatibility with international standards.
16. FIRE also promotes structured, machine-readable reporting formats and a common set of reporting fields covering matters such as incident identification, the nature of the incident and affected systems, operational and financial impact, response and remediation actions, and reporting metadata. The use of structured reporting supports more consistent data collection and facilitates automated analysis and information exchange across regulated entities and jurisdictions.

D. Purpose of Proposed Measure and Consistency with the Authority's Functions

17. The purpose of the proposed RSOG is to establish a clear, consistent and comprehensive framework for the management of cybersecurity risk and Cyber Incident Reporting ("CIR") by Regulated Entities. In particular, the proposed RSOG seeks to strengthen the Authority's existing cybersecurity framework by clarifying mandatory obligations and supporting guidance, enhancing incident notification and

reporting requirements, and promoting more consistent and structured machine-readable collection of cyber incident information. These enhancements are intended to strengthen the Authority's supervisory oversight, improve its ability to identify and assess emerging cyber risks and vulnerabilities, and promote greater operational resilience across the financial services industry.

18. The proposed RSOG is consistent with the Authority's regulatory functions, as outlined in Section 6(1)(b) of the MAA, which provides that:

"(1) The principal functions of the Authority are –

(b) regulatory functions, namely –

(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;"

19. Furthermore, Section 6(3) of the MAA provides that in performing its regulatory functions and its co-operative functions, the Authority shall, inter alia:

"(a) endeavour to promote and enhance market confidence, consumer protection and the reputation of the Islands as a financial centre;

(b) endeavour to reduce the possibility of financial services business or relevant financial business being used for the purpose of money laundering or other crime;

(c) recognise the international character of financial services and markets and the necessity of maintaining the competitive position of the Islands, from the point of view of both consumers and suppliers of financial services, while conforming to internationally applied standards insofar as they are relevant and appropriate to the circumstances of the Islands"

E. Jurisdictional Comparison

20. To provide context for the proposed revisions to the RSOG, the Authority conducted a comparative review of the cyber incident reporting frameworks in Guernsey, Jersey, the United Kingdom, Singapore and Bermuda. These jurisdictions were selected to assess how comparable financial services regulators have implemented key components of the FSB's recommendations on Cyber Incident Reporting ("CIR"), including reporting triggers, prescribed reporting timelines, reporting structures, data granularity, follow-up reporting, and the regulatory use of incident data. The review also considered the extent to which the respective frameworks incorporate standardised or machine-readable reporting arrangements comparable to the FIRE framework.

Table 1: Overview of Cyber Incident Reporting Frameworks across Comparable Jurisdictions.

Reporting Features	Guernsey (GFSC)	Jersey (JCSC)	UK (FCA)	Singapore (MAS)	Bermuda (BMA)	Cayman Islands (CIMA)
Formal Adoption of FIRE Framework	X	X	X	X	X	X
Defined Reporting Triggers	✓	✓	✓	✓	✓	✓

Prescribed Initial Reporting Timeline	✓	X	✓	✓	✓	✓
Follow-up / final reporting mechanism	✓	X	✓	✓	✓	✓
Standardised reporting form or template	✓	X	✓	✓	✓	✓
Structured/machine-readable reporting	X	X	X	X	X	X
Data Granularity	Moderate	Limited	High	High	Moderate to High	Moderate
Regulatory use for systemic / cross-sector analysis	Limited	Limited	✓	✓	✓	Limited

F. Cost and Benefit Analysis

21. **Table 2** provides a cost-benefit analysis of the estimated costs and benefits of the proposed RSOG

Table 2: Estimated Costs and Benefits of the Proposed RSOG.

Stakeholder	Costs	Benefits
CIMA	- Administrative costs associated with Staff training on the new standardised incident reporting format (e.g., XBRL/DPM). - Internal resource costs associated with the analysis, configuration, integration, testing and deployment of the proposed incident reporting form within REEFS.	- Enhanced supervisory capability through automated data ingestion and analysis. - Strengthened data gathering capabilities to assess emerging risks and threats and the ability to create a regulatory response for the benefit of the financial system. - Faster and more consistent incident assessments across divisions. - Improved alignment with FSB's FIRE framework, principles of interoperability and real-time data exchange.
Cayman Islands	- Public sector expenditure on any national cyber infrastructure or information-sharing arrangements needed to support coordination of incident information across relevant agencies. - Staff time and administrative resources required for agencies to establish information-sharing protocols, coordinate responses, and analyse incident trends at the national level.	- Greater alignment with international standards and best practices. - Strengthened resilience of the jurisdiction's financial system against cross-border cyber threats. - Increased international credibility as a well-regulated financial centre.

Regulated Entities	▪ Potential costs associated with adapting internal systems to comply with new reporting requirements and formats. ▪ Staff training for incident reporting and coordination protocols.	▪ Reduced administrative burden through streamlined reporting processes. ▪ Improved clarity and consistency in regulatory expectations. ▪ Enhanced confidence in the jurisdiction's robust cybersecurity framework and global interoperability.
---------------------------	---	---

G. Consultation Feedback and Comments

22. Before proceeding with the proposed measure, the Authority shall have regard to any representations made by the private sector associations only. Feedback submitted by individuals, entities, or other bodies, unless acting on behalf of private sector associations, will not be accepted by the Authority. Representations from private sector associations must be submitted as a consolidated document, and a listing of the entities that provided feedback should be included. Private sector associations should ensure that conflicting positions are resolved prior to submission to the Authority. Where positions conflict within or across associations, the Authority will consider all available information in taking a decision, which will be at its sole discretion.
23. To ensure that all responses are given due consideration, it is important that private sector associations make clear reference to the sections of the measure being commented on, and that responses are unambiguous, clearly articulated and based on fact. The consultation process is not designed to address complaints or grievances. Feedback of this nature should be submitted through the established complaints process.
24. In cases where the feedback proposes to change a policy position of the Authority or substantially amend any requirement of the proposed measure, information to support the position of the association must be provided. The table below provides an example of the Authority's expectation with regard to feedback for the proposed measure.

Reference	Example of a Helpful Comment	Examples of Comments needing more Support
Rule 4.2 ¹	In Rule 4.2 the current text omits the fair value measurement of liabilities. Also, as defined it is not asymmetrical with the Market Price definition and thus scenarios exists that fall into neither category. <u>Suggested wording:</u> <i>Hard-to-Value Securities means an asset or liability for</i>	× This is not what is done in other jurisdictions. × I don't think we should do this. × CIMA is not considering the position of the experts.

¹ This example is not reflective of the content of the proposed measure.

	<u>which there is no Market Price which is required to be measured at fair value pursuant to 5.2</u>	
--	--	--

25. All feedback submitted by private sector associations will be given due consideration; nevertheless, the decision to adopt any feedback provided into a proposed measure will be at the sole discretion of the Authority.

H. Notice of Representations

26. The Authority seeks consultation through written comments and representations from the private sector associations concerning the proposed:

*Rule and Statement of Guidance on Cybersecurity and Incident Reporting for Regulated Entities (**Appendix 1**).*

27. The Authority must receive representations by **Tuesday, 10 November 2026**. Representations received after this deadline may not be considered and will not form part of the collated written response provided to private sector associations.

28. Comments and representations must be addressed to²:

The Chief Executive Officer
Cayman Islands Monetary Authority
P.O. Box 10052
Pavilion East, Cricket Square
Grand Cayman KY1-1001
Cayman Islands
Tel: 345-949-7089
Fax: 345-946-5611
Email: contactpolicy@cima.ky
and copied to Jabariheywood@cima.ky

29. The Authority shall have due regard to any representation made by the private sector associations and industry stakeholders. The Authority shall provide a written response collating the feedback received and the Authority's position on this feedback. This response shall be copied to all relevant private sector associations only.

² Where the private sector association or industry stakeholder has no comments or representations on the proposed measure, it is recommended that the Authority be informed of this fact.



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

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