



PRIVATE SECTOR CONSULTATION

Cybersecurity for VASPs

October 2026

Private Sector Consultation
Rule and Statement of Guidance on Cybersecurity for VASPs

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 for Virtual Asset Service Providers (the "RSOG") (attached as Appendix I).
2. Requirements specific to the private sector consultation are outlined in section 4(1) of the Monetary Authority Acts (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 Monetary Authority Act (2024 Revision) ("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. The Authority has progressively strengthened its Cybersecurity framework in response to the increasing digitalisation of the financial services sector. This has included adopting the National Institute of Standards and Technology ("NIST") Cybersecurity Framework, issuing guidance and alerts to Regulated Entities, implementing the Information Systems Questionnaire, and embedding Cybersecurity considerations within supervisory activities.
5. In 2020, the Authority issued the *Rule on Cybersecurity for Regulated Entities and Statement of Guidance* (the "existing Measures"), establishing minimum requirements for Cybersecurity governance, risk management, incident response and operational resilience. In April 2023, the existing Measures were extended to Virtual Asset Service Providers ("VASPs").
6. Since that time, supervisory experience and legislative developments, including the licensing of virtual asset trading platforms and virtual asset custodians under the Virtual Asset (Service Providers) Act ("VASPA"), have demonstrated that VASPs are exposed to technological and operational risks which differ materially from those of other regulated sectors. These include risks associated with wallet infrastructure, private key management, smart contracts, blockchain interactions, custody arrangements and third-party technology providers.
7. Following an internal assessment, the Authority determined that while the existing cross-sector Cybersecurity Measures provide an appropriate regulatory baseline, they do not sufficiently address the specific and nuanced risks associated with conducting VASP activities.

8. Accordingly, the Authority is proposing a standalone RSOG specific to VASPs. The proposed RSOG seeks to provide greater regulatory clarity and establish requirements proportionate to the particular Cybersecurity, operational and custody risks associated with virtual asset activities, while maintaining consistency with the Authority's existing principles-based supervisory framework.

C. International Standards

9. International standard-setting bodies increasingly recognise Cybersecurity as an important component of operational resilience and financial stability. The proposed RSOG has therefore been informed by evolving international standards and supervisory practices relevant to VASPs.

10. *International Monetary Fund ("IMF")*

In January 2026, the IMF published its Departmental Paper on *Good Practices in Cyber Risk Regulation and Supervision*. The Paper emphasises systemic Cyber risk, third-party dependencies and supervisory engagement, including the need for regulated entities to identify and manage risks associated with outsourcing and critical service providers and to prepare for severe but plausible Cyber scenarios.

The IMF advocates a principles-based and risk-proportionate supervisory approach which focuses on defined supervisory outcomes rather than uniform technical controls. These outcomes include effective governance, robust risk identification, strong preventive safeguards, timely detection and effective response and recovery capabilities.

11. *Financial Stability Board ("FSB")*

The FSB's *Effective Practices for Cyber Incident Response and Recovery* similarly treats Cybersecurity as a matter extending beyond information technology and operational risk to encompass broader financial stability considerations.

The FSB emphasises strong governance and the integration of Cybersecurity into an overall risk management framework of the institution. Its approach addresses the full Cyber incident lifecycle, including preparedness, prevention, detection, response, recovery and continuous improvement.

The FSB also adopts a proportionate and risk-based approach, recognising that regulated entities should implement practices commensurate with their size, complexity, systemic relevance and risk profile.

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

12. The purpose of the proposed measure is to establish a clear and proportionate VASP-specific framework for the identification, assessment and management of Cybersecurity risk.

13. The mandate of the Authority for this proposed RSOG is found under Section 6(1)(b) of the MAA which states:

"(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;"

14. 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

15. The Authority conducted a review of Bermuda, Dubai, Guernsey and Singapore. These jurisdictions were selected based on their published regulatory Cybersecurity frameworks. Each of the jurisdictions has adopted distinct approaches to regulating VASPs, in relation to Cybersecurity which has been summarised in **Table 1** below.

Regulatory Requirements	Jurisdictional Regulatory Bodies				
	Bermuda Monetary Authority	Virtual Assets Regulatory Authority (Dubai)	Guernsey Financial Services Commission	Monetary Authority of Singapore	Cayman Islands Monetary Authority
Legislative Framework - Is there any VASP-specific Cybersecurity Legislation?	Yes – under the Digital Asset Business Act 2018 - <u>Digital Asset Business Operational Cyber Risk Management Code of Practice</u>	Yes – under <u>Law No. [4] of 2022</u> – <u>Technology and Information Rulebook</u>	<u>Cyber Security Rules and Guidance</u>	Yes – Financial Services and Markets Act 2022 - <u>MAS Notice No.: FSM-N06</u>	Yes – <u>VASP Act</u> and <u>Cybersecurity Rule</u>
Governance – Must the VASP designate a qualified individual (e.g., CISO) with responsibility for Cybersecurity?	Expected via guidance or principles-based supervision	Yes	Expected via guidance or principles-based supervision	Expected via guidance or principles-based supervision	Expected via guidance or principles-based supervision
Applied International Standards – Is the regulatory framework aligned with any global best practices, like NIST or DORA?	Yes	No	Yes	No	Yes
Frequency of Audit or Review of Cybersecurity Framework – Must the Cybersecurity framework of the VASP be reviewed at least annually?	Yes	Yes	No	No	No – periodic/regular review
Independence of Audit or Reviews - Are independent Cyber audits required?	Principles-based	Yes	Principles-based	Principles-based	Yes
Cybersecurity Testing - Are there any Testing Requirements?	Principles-based (Section 5.17)	Yes (Section E.1)	No – not mandated	Principles-based	Yes
Wallet or Key Management, Security & Controls - Are there explicit obligations for wallet/key operations (e.g., approvals, access logging, governance of key/wallet management)?	Principles-based	Yes	Principles-based	Principles-based	Principles-based

F. Cost and Benefit Analysis of Implementing the Proposed Measures

16. Identified costs and benefits of implementing the Proposed RSOG are set out in **Table 2** below.

	Costs	Benefits
CIMA	1. CIMA will incur the usual administrative costs associated with publishing the new requirement measure and amending internal supervisory manuals. 2. Costs related to processing new measures, conducting consultation, and reviewing feedback. 3. Costs related to aligning Off-site and on-site procedures with the RSOG and investigating and taking action in response to any breaches of rules.	The Authority stands to benefit from: 1. improved compliance by supervised entities with the measure. 2. Providing clarity and certainty on the obligations of VASPs regarding Cybersecurity policies and frameworks. 3. Strengthened regulatory/supervisory framework for the VASP sector that supports CIMA's mandate.
Cayman Islands	1. Some entities may determine that compliance costs outweigh the commercial benefits of remaining in the jurisdiction; however, the Authority expects this risk to be limited.	The jurisdiction stands to benefit from: 1. an enhanced jurisdictional profile as an international financial centre as a result of improved compliance with international best practices on Cybersecurity for VASPs. Moreover, adopting globally uniform standards promotes consistency across jurisdictions, facilitating seamless international operations and reinforcing trust among clients and regulators. 2. minimising risks associated with weak Cybersecurity regulations for VASPs. Such risks include, but are not limited to: 1) custody models; 2) private key management; 3) wallet infrastructure; 4) smart contracts; and 5) third-party technology arrangements. 3. the mandatory disclosures within the RSOG that will empower VASP clients with the necessary information to make informed financial decisions, while simultaneously strengthening industry discipline through greater accountability and clear redress mechanisms. 4. improved results in international assessments and evaluations with greater clarity surrounding the enforceability of the requirements established in the proposed measure.
VASPs	1. VASPs may incur compliance costs relating to implementing proposed rules.	1. VASPs benefit from enhanced clarity regarding their Cybersecurity obligations, while also gaining increased certainty about audits, testing and expectations from the Authority. 2. By mitigating the risk of regulatory breaches linked to cyber incidents, operational failures, cybersecurity breaches and associated regulatory breaches, the rules offer tangible benefits to VASPs. They reduce exposure to fines, penalties, and reputational damage while enhancing compliance and credibility. 3. VASPs will benefit from the positive spillovers associated with increased client confidence emanating from good Cybersecurity/notification practices. This will result in positive knock-on effects on profitability, customer growth and overall VASP performance.
Summary	Consequent to the above, it is determined that the benefits outweigh the costs, and that the issuance of the RSOG should therefore be pursued by the Authority.	

G. Consultation Feedback and Comments

17. Before proceeding with the proposed measure, the Authority shall have regard to any representations made by the private sector associations and industry stakeholders

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 which 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.

18. 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.
19. In cases where the feedback proposes to change a policy position of the Authority or substantially amend any requirement of the draft measure, information to support the position of the association must be provided. The table below provides an example of the Authority's expectations regarding feedback on 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 exist that fall into neither category. <u>Suggested wording:</u> <i>Hard-to-Value Securities means an asset or liability for which there is no Market Price which is required to be measured at fair value pursuant to 5.2</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.

20. 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**

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

Rule and Statement of Guidance on Cybersecurity for Virtual Asset Service Providers.

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

22. 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.
23. 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: consultation@cima.ky
and copied to KathyGonzalez@cima.ky

24. 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