



RULE and STATEMENT OF GUIDANCE

Cybersecurity for Virtual Asset Service Providers

XXX 2026

Table of Contents

List of Acronyms	3
1. Introduction.....	4
2. Statement of Objectives.....	5
3. Statutory Authority	5
4. Scope of Application.....	6
5. Definitions	6
6. Establishing of a VASP-specific Cybersecurity Framework	8
7. Cybersecurity Risk Management	9
8. Governance and Accountability for the Cybersecurity Framework	9
9. Technology, Infrastructure, and Security Controls.....	11
10. Cyber Incident Response, Recovery and Reporting	16
11. Outsourcing and Third-Party Risk Management	17
12. Data Protection and Privacy	18
13. Cybersecurity Audit and Testing Program	18
14. Integration with Enterprise Risk	19
15. Enforcement.....	20
16. Effective Date.....	20

List of Acronyms

AML	Anti-Money Laundering
CIMA	Cayman Islands Monetary Authority
DPA	Data Protection Act
FSB	Financial Stability Board
IMF	International Monetary Fund
MAA	Monetary Authority Act
MFSC	Ministry of Financial Services and Commerce
NIST	National Institute of Standards and Technology
PSAs	Private Sector Associations
REs	Regulated Entities
RSOG	Rule and Statement of Guidance
VA	Virtual Assets
VASP	Virtual Asset Service Provider
VASPA	Virtual Asset Service Provider Act

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

1. Introduction

- 1.1. This document establishes the Cayman Islands Monetary Authority's (the "Authority" or "CIMA") *Rule and Statement of Guidance on Cybersecurity for Virtual Asset Service Providers* ("VASPs").
- 1.2. The Authority acknowledges that technology provides important innovation, competitive advantages, as well as greater efficiency, effectiveness and productivity for VASPs and their customers.
- 1.3. VASPs operate technology-enabled business models that give rise to inherent and elevated Cybersecurity risks relative to those typically associated with traditional financial services activities. These risks arise from the digital nature of the customer assets, custody and transfer of virtual assets, smart contracts, and dependence on third-party service providers.
- 1.4. It is important for VASPs to be able to appropriately identify, protect, detect, respond to and recover from such Cybersecurity-related threats, incidents and breaches. Cybersecurity Threats can result in the loss of customer assets, unauthorised access to sensitive information, or disruption to critical services.
- 1.5. The Authority therefore expects Cybersecurity to be addressed by VASPs as a material operational and prudential risk, supported by formal risk management frameworks and ongoing oversight that is proportionate to the nature, scale, risk profile and complexity of activities being undertaken by the VASP.
- 1.6. This Rule and Statement of Guidance ("RSOG") should be read in conjunction with the following:
 - a) the Virtual Asset (Service Providers) Act (the "VASPA");
 - b) the Data Protection Act (the "DPA");
 - c) the Rule and Statement of Guidance on Cybersecurity for Regulated Entities¹;
 - d) Statement of Guidance on Business Continuity Management;
 - e) the Rule and Statement of Guidance Market Conduct for VASPs;
 - f) Statement of Guidance on Outsourcing for Regulated Entities;
 - g) the Rule and Statement of Guidance on Internal Controls for Regulated Entities;
 - h) Statement of Guidance on Nature, Accessibility and Retention of Records;
 - i) Statement of Principles on Conduct of Virtual Asset Services; and

¹ This RSOG establishes cybersecurity requirements specific to Virtual Asset Service Providers and should be read in conjunction with the Rule and Statement of Guidance – Cybersecurity for Regulated Entities. Where a requirement in this RSOG is more specific, it prevails in relation to VASPs.

- j) any other relevant legislation issued by the Cayman Islands Government and regulatory instruments issued by the Authority from time to time.
- 1.7. 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.
- 1.8. 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 This RSOG establishes minimum requirements and guidelines for the establishment and implementation of an effective Cybersecurity risk management for VASPs.

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 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 The RSOG is also consistent with section 34(1) 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;*
- (c) issue or amend rules or statements of principle or guidance to reduce the risk of financial services business being used for money laundering or other criminal purposes."*

- 3.3 Additionally, section 8(4)(b)(iii) of the VASPA stipulates that:

"The Authority in determining whether to approve the application from a person in subsection (1), shall consider whether –

(b) the applicant has –

(iii) adequate capital and Cybersecurity measures, as the Authority

considers appropriate having regard to the size, scope and complexity of the business...”

4. Scope of Application

- 4.1 This RSOG applies to all Regulated Entities that conduct virtual asset services pursuant to the VASPA.
- 4.2 The provisions of the RSOG supplement the existing requirements and guidelines set out in the *Rule and Statement of Guidance on Cybersecurity and Incident Reporting for Regulated Entities*.
- 4.3 Where a VASP is part of a group, it may rely on the group Cybersecurity Framework, provided that the Governing Body of the VASP is satisfied that the framework is commensurate with the size, complexity, structure, nature of business and risk profile of the operations of the VASP and legal requirements in the Cayman Islands, including those outlined in this RSOG. Where gaps are identified, a tailored Cybersecurity framework that complies with this RSOG and legal requirements in the Cayman Islands should be implemented.
- 4.4 Where VASPs conduct virtual asset activities across multiple jurisdictions, the VASP must ensure that its Cybersecurity Framework meets the higher applicable regulatory standard without neglecting local compliance obligations where gaps arise.
- 4.5 To the extent that this RSOG establishes more specific requirements applicable to VASPs, VASPs must comply with those requirements in conjunction with the *Rule – Cybersecurity for Regulated Entities*.
- 4.6 The Authority will assess the compliance of each VASP with this RSOG in a manner commensurate with the size, complexity, structure, nature of business and risk profile of its operations.

5. Definitions

5.1 The following definitions are provided for the purpose of this Rule:

- 5.1.1 “**Chief Information Security Officer**” or “**CISO**” is the senior officer designated by the Regulated Entity who is responsible for overseeing the implementation and effective operation of the Cybersecurity Framework, including the enforcement of the policies and procedures, and for reporting to Senior Management or the Governing Body on Cybersecurity risks, incidents, and the overall effectiveness of the Cybersecurity Framework. This individual is a senior officer of the Regulated Entity performing a control function.
- 5.1.2 “**Cold Wallet**” means a digital wallet that stores private cryptographic keys in an offline environment that is isolated from internet connectivity, providing enhanced security for the storage and protection of virtual assets.
- 5.1.3 “**Cyber Attack**” means actions taken using computer networks to breach, disrupt, steal from, or damage computer systems, networks, digital devices, or data. Such actions are carried out for malicious purposes such as unauthorised access, data theft, service disruption, system manipulation, or the compromise of confidential, sensitive or controlled information.

- 5.1.4 **"Cybersecurity Breach"** means any unauthorised access to, or compromise of, an organisation's information systems, networks, digital technologies, or data resulting from the failure, circumvention, or breakdown of the security controls designed to protect against Cyber risk.
- 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 **"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.
- 5.1.7 **"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.
- 5.1.8 **"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.
- 5.1.9 **"Data Protection Officer" or "DPO"** means the person responsible for ensuring compliance with the applicable data protection legislation. The DPO oversees privacy governance, data-minimisation practices, breach reporting and cross-border data obligations. This role may be combined with the CISO role. This individual is a senior officer of the Regulated Entity performing a control function.
- 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 **"Hot Wallet"** means a that stores or manages the private cryptographic keys associated with virtual assets in an internet-connected environment, enabling the execution of frequent, timely, or automated transactions.
- 5.1.12 **"Regulated Entity"** means any legal person or arrangement that has been granted a licence or registration or waiver in accordance with the VASP waiver.

- 5.1.13 **"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.
- 5.1.14 **"Smart Contract"** means a computer program deployed on a blockchain or distributed ledger that automatically records, verifies, or enforces predefined actions, transactions, or contractual obligations, including the transfer, management, or other operation of Virtual Assets, when predefined conditions encoded in the program are satisfied.
- 5.1.15 **"Virtual Asset"** has the same meaning as defined in the VASP Act.
- 5.1.16 **"Virtual Asset Custodian"** has the same meaning as defined in the VASP Act.
- 5.1.17 **"Virtual Asset Custody Service"** has the same meaning as defined in the VASP Act.
- 5.1.18 **"Virtual Asset Service"** has the same meaning as defined in the VASP Act.
- 5.1.19 **"Virtual Asset Service Provider"** or **"VASP"** has the same meaning as defined in the VASP Act.
- 5.1.20 **"Wallet"** means a software application, device, or service that enables a user to generate, store, manage, access, or use cryptographic keys, payment credentials, or other authentication mechanisms to access, control, transfer, receive, or otherwise manage Virtual Assets, electronic money, or other digital representations of value, and to initiate and receive transactions over electronic networks.
- 5.1.21 **"Warm Wallet"** means a digital wallet in which cryptographic keys are stored or managed in an environment where internet connectivity is limited, controlled, or enabled only as necessary to facilitate transactions while reducing exposure to cyber risk relative to a hot wallet.

6. Establishing of a VASP-specific Cybersecurity Framework

- 6.1 A VASP must establish, document, and implement an effective Cybersecurity Framework appropriate to the nature, size, complexity, and risk profile of its operations, and the Governing Body of the VASP must approve the framework. R
- 6.2 The Cybersecurity Framework must incorporate the following core components, at a minimum: R
- (1) Cybersecurity Risk Identification and Assessment;
 - (2) Governance and Accountability for the Cybersecurity Framework;
 - (3) Technology, Infrastructure and Security Controls;
 - (4) Data Protection and Privacy;

- (5) Cyber Incident Response, Recovery and Reporting;
- (6) Outsourcing and Third-Party Risk Management;
- (7) Cybersecurity Audit and Testing Program; and
- (8) Integration with Enterprise Risk Management.

7. Cybersecurity Risk Management

- | | | |
|-----|--|---|
| 7.1 | A VASP must conduct risk assessments that must be reviewed at least annually and upon any material change in the technology, operations or risk profile of the VASP, whether planned or unplanned. | R |
| 7.2 | A comprehensive risk assessment of the VASP must be conducted prior to the adoption or material use of cloud computing services. | R |
| 7.3 | A risk assessment of a VASP must cover an evaluation of the security architecture, legal and regulatory risks, data protection considerations, and the allocation of roles and responsibilities between the VASP and third-party providers such as cloud service providers. | R |
| 7.4 | VASPs must implement a formal vulnerability management programme covering the identification, assessment, prioritisation, remediation and verification of vulnerabilities across systems and applications. | R |
| 7.5 | Where material, VASPs must identify, assess and manage risks arising from end-user developed applications or tools that support the Virtual Asset activities of the organisation. | R |
| 7.6 | The Governing Body of a VASP must ensure that Cybersecurity and technology risk assessments are formally documented, maintained in a central risk register, and retained for a minimum period of five (5) years. | R |
| 7.7 | A VASP must establish ongoing processes to monitor its cybersecurity risk profile and report material cybersecurity risks, significant control weaknesses, and changes to its cybersecurity risk environment to Senior Management and the Governing Body in a timely manner. | R |

8. Governance and Accountability for the Cybersecurity Framework

Cybersecurity Governance

- | | | |
|-----|--|---|
| 8.1 | A VASP must establish, implement, and maintain an appropriate Cybersecurity governance approach to ensure effective oversight, accountability, and management of Cybersecurity risks. | R |
| 8.2 | The Cybersecurity governance approach of a VASP must form part of its broader corporate governance and risk management arrangements. It should incorporate, at a minimum, appropriate oversight, accountability, documented policies and procedures, defined roles and responsibilities, and periodic review mechanisms. The governance approach should, where appropriate, be aligned with internationally recognised Cybersecurity standards and best practices: | R |

- (a) The IT and cybersecurity strategies of a VASP must be reviewed and approved by the entity's Governing Body annually.
- (b) A VASP must, at least annually, review the Cybersecurity and IT risks it faces and assess whether its Cybersecurity Framework remains appropriate to manage the adverse impacts of Cybersecurity and IT risks.
- (c) A VASP must maintain adequate and documented policies and procedures governing:
 - i. Cybersecurity;
 - ii. incident response and recovery; and
 - iii. business continuity and disaster recovery, including backups.
- (d) A VASP must ensure that roles and responsibilities relating to general IT controls, information security, Cybersecurity, and private key management are clearly defined, documented, and communicated within the organisation.

R

Appointment of the Chief Information Security Officer ("CISO")

- 8.3 A VASP Governing Body must formally appoint a suitably qualified and experienced person at a senior management level to serve as the CISO, who has a good understanding and knowledge of the VASP's IT systems and Cybersecurity, and the Authority must approve such appointment for a CISO to be considered suitably qualified and experienced for the appointment by the Governing Body, they must, at a minimum:
- (a) have relevant qualifications appropriate for the nature, size, complexity, and risk profile of the VASP;
 - (b) demonstrate experience designing, implementing, or overseeing Cybersecurity frameworks that are aligned with best practices appropriate to the VASP;
 - (c) have sufficient authority, independence, and resources to perform their duties and must not have conflicting operational responsibilities that could compromise the execution of CISO roles and responsibilities; and
 - (d) have experience managing cyber risk in regulated or technology-led or technology intensive organizations or high-risk technology-centric environments.

R

Responsibilities of the CISO

- 8.4 The responsibilities of the CISO of a VASP must include, but are not limited to:
- 8.4.1. effective design, implementation, operation, and ongoing maintenance of the Cybersecurity Framework of the VASP, including governance arrangements, monitoring and reporting procedures, key management controls, smart-contract security, wallet security controls, and cyber resilience testing.

R

- | | | |
|--------|--|---|
| 8.4.2. | ensuring that appropriate measures are implemented to comply with this RSOG and any other Cybersecurity-related obligations under the VASP Act or any regulatory measures issued by the Authority from time to time. | R |
| 8.4.3. | ensuring that the Cybersecurity Framework is periodically reviewed, updated, and enhanced to remain relevant and effective, including to reflect changes in the technology environment, threat landscape, operational risks, and regulatory expectations of the VASP. | R |
| 8.4.4. | monitoring and assessing current and emerging Cybersecurity Threats by reviewing global threat intelligence, security data, findings from vulnerability assessments and penetration testing (including Threat-Led Penetration Testing ("TLPT"), where applicable), internal incident trends, and any newly identified attack vectors relevant to Virtual Asset technologies and distributed ledger environments. | R |
| 8.4.5. | ensuring that appropriate processes are established for timely detecting, responding to, and recovering from Cybersecurity incidents, as well as meeting regulatory reporting obligations. | R |
| 8.4.6. | reporting periodically to senior management and the Governing Body, or an appropriate committee/subcommittee of the Governing Body, on the effectiveness of the Cybersecurity Framework, material Cybersecurity risks, significant Cybersecurity incidents, and remediation actions. | R |
| 8.4.7. | ensuring that Cybersecurity Risks associated with third-party service providers, technology vendors, and external infrastructure supporting the operations of the VASP are appropriately identified, assessed, and managed. | R |

9. Technology, Infrastructure, and Security Controls

Custody, Wallet, and Key Management Controls

PART A: Applicable to all VASPs

- | | | |
|-----|--|---|
| 9.1 | VASPs that transfer, authorise, have access to, facilitate the movement of or otherwise have the ability to affect customers' Virtual Assets must design, implement and maintain systems and controls specific to the safeguarding of keys and virtual asset wallets. | R |
| 9.2 | VASPs must establish and maintain governance, operational, and security controls to identify, manage and prevent any single individual, credential, cryptographic key, privileged system access, device, or location from creating a concentration of risk or single point of failure in respect of customers' Virtual Assets or fiat funds. | R |
| 9.3 | VASPs must identify, assess and manage risks arising from dependency on individuals who possess signing authority, privileged system access, recovery credentials, administrative authority or other forms of control over customers' Virtual Assets or fiat funds. | R |

- | | | |
|------|--|---|
| 9.4 | VASPs must establish and maintain effective segregation of duties for activities involving the initiation, approval, execution, reconciliation, administration or oversight of transactions involving customers' Virtual Assets or fiat funds. | R |
| 9.5 | VASPs must implement controls designed to mitigate the risks of theft, fraud, error, misuse, unauthorised activity, operational disruption and conflicts of interest arising from customer virtual assets and fiat funds processing and/ handling activities. | R |
| 9.6 | VASPs must implement transaction monitoring and emergency control mechanisms, including, where appropriate, velocity limits, transaction freezes or circuit breakers, to protect customers' Virtual Assets in the event of suspected compromise or irregular activity. | R |
| 9.7 | VASPs should ensure that transaction controls are consistent with their customer protection obligations and risk tolerance. | |
| 9.8 | VASPs should consider formal procedures for onboarding and offboarding individuals with private key or signing authority, including immediate revocation of access and assessment of whether key rotation is required. | |
| | PART B: Applicable to Virtual Asset Custodians ("Custodians") and Virtual Asset Trading Platforms that provide virtual asset custody services must ("Trading Platforms") | |
| 9.9 | Custodians or Trading Platforms must establish, implement and maintain risk-based effective systems and controls specific to the safeguarding of customer assets throughout their lifecycle, including appropriate controls over virtual assets custody infrastructure and fiat funds. | R |
| 9.10 | Custodians or Trading Platforms must maintain documented policies and procedures governing the lifecycle of cryptographic keys and credentials, including roles, responsibilities, approvals, access management and security requirements. | R |
| 9.11 | <p>Custodians or Trading Platforms must implement the policies, procedures and controls / a key management framework referenced in 9.10 to securely manage cryptographic keys and credentials throughout their lifecycle across virtual asset custody, wallet management, encryption, transaction authorisation authentication and other security-critical functions. The Custodian or Trading platform must:</p> <ul style="list-style-type: none"> (a) implement industry best practices for the generation, storage, usage distribution, backup, recovery, rotation, suspension, replacement, destruction and retirement of all cryptographic keys and credentials used; (b) implement backup procedures for all private keys which are in line with industry best practices; (c) implement a Key Compromise Protocol which is tested and reviewed at least annually; (d) have controls in place to meet liquidity and other demands; and | R |

- (e) arrange for security audits to be performed on a regular basis by an independent third party.
- 9.12 Hot, warm, and cold wallets must be segregated and protected through layered operational controls. Wallet backups must be encrypted, geographically distributed, and subjected to periodic restoration testing. R
- 9.13 Cold-storage vaults, omnibus wallets, and operational floats must follow diversification and segregation standards that prevent systemic exposure to single points of failure. R
- 9.14 The Authority recognises that the compromise of private keys presents a materially² different risk profile from traditional information security incidents. Custodians/Trading Platforms should consider the implementation of layered key management arrangements, including multi-signature or multi-party authorisation models, hardware security models, secure key storage environments, and robust access logging.
- 9.15 Custodian/Trading Platforms must ensure that customer funds and/or assets are clearly segregated in compliance with the relevant requirements under the VASPA and relevant regulatory measures. R
- 9.16 Segregation should be capable of being demonstrated both technically and through internal records. VASPs are expected to be able to demonstrate segregation promptly upon request, including during periods of stress or disruption. Transaction controls should be consistent with customer protection obligations and risk tolerance.
- 9.17 A Custodian or Trading Platform must implement wallet architecture and custody arrangement appropriate to the nature, scale, complexity and risk profile of its activities. Wallets used for operational, liquidity, customer withdrawals and long-term storage/holdings must be subject to differentiated security controls and access restrictions. Transaction approval processes should support timely intervention in the event of suspected compromise or anomalous behaviour. R
- 9.18 Wallet backups should be encrypted, protected from unauthorised access, maintained in geographically resilient locations where appropriate, and subjected to periodic recovery and restoration testing.
- 9.19 A Custodian or Trading Platform must employ technical controls such as cryptographic, multi-signature or multi-party computation ("MPC") mechanisms that have been reviewed and approved by the CISO or senior management representatives or Board to ensure that no individual or system can unilaterally authorise transactions. R

Infrastructure and Access Controls

- 9.20 A VASP must implement and maintain effective application, network and infrastructure security controls to protect its systems, data, and virtual assets from Cyber threats. R

² means a contravention of a Regulatory Act, or a Regulatory Measure, which includes an act or omission, as per Volume 2 of the Regulatory Handbook.

- | | | |
|--|---|---|
| 9.21 | VASPs should implement appropriate physical security and logical controls to protect facilities, hardware, security modules, key storage environments and other physical locations that support critical systems or the safeguarding of customer virtual assets. | R |
| 9.22 | Technology infrastructure controls must include processes to regularly review, update, and patch network components, systems, applications, and configurations, having regard to the size, complexity, structure, nature of business and risk profile of the VASP, and the evolving Cybersecurity Threats. | R |
| 9.23 | VASPs should maintain a current and sufficiently detailed inventory or register of the technology infrastructure and information assets that support their cyber resilience framework. The inventory or register should identify, where relevant, the systems, networks, platforms, applications, data repositories and supporting services that are critical to the provision of virtual asset activities or the safeguarding of customer assets. It should be reviewed and updated periodically, and following any material change to the technology environment of the VASP, operations or service arrangements. | R |
| 9.24 | VASPs must implement multi-factor authentication for privileged access, remote access and any access to systems or environments supporting the safeguarding of customer virtual assets or sensitive data. | R |
| 9.25 | VASPs should adopt authentication methods and controls that are appropriate to the level of risk, including the use of strong, phishing-resistant factors where feasible, and the application of additional safeguards for highly privileged or high-risk activities. | R |
| 9.26 | VASPs should ensure that authentication mechanisms are consistently enforced, regularly reviewed, and supported by appropriate monitoring, exception management, and user access governance arrangements. | R |
| Security and Application Controls | | |
| 9.27 | VASPs must implement data loss prevention or equivalent controls designed to detect and prevent the unauthorised exfiltration, transmission or disclosure of sensitive or confidential data. | R |
| 9.28 | Where a VASP develops or materially customises software or technology solutions, the VASP must implement secure software development lifecycle controls, including secure coding practices, code review, vulnerability testing and change control. | R |
| 9.29 | The IT and cybersecurity strategies of a VASP must be reviewed and approved by the Governing Body annually. | R |
| 9.30 | VASPs must implement and maintain controls designed to protect systems and environments against malicious code, including appropriate detection, prevention and response capabilities. | R |
| 9.31 | VASPs must implement centralised logging and continuous security monitoring capabilities sufficient to detect anomalous activity, Cybersecurity events and potential compromise of systems supporting virtual asset services. | R |

Smart Contracts

- 9.32 Where a VASP relies on smart contracts, protocols, or automated execution mechanisms to provide virtual asset services, the VASP must identify and assess risks arising from such technologies as part of its Cybersecurity and operational risk management. R
- 9.33 A VASP must ensure that material vulnerabilities in smart contracts or protocols that may impact customer assets or service continuity are identified, assessed, and addressed in a timely manner. R
- 9.34 Where smart contracts are material to the provision of regulated virtual asset services, VASPs should conduct or obtain independent code review and testing appropriate to the nature, scale and risk of the activity.
- 9.35 VASPs should remain alert to protocol changes, or external dependencies that could materially affect customer transactions, custody, settlement, or customer asset access. Where protocols are not directly controlled by the VASP, appropriate monitoring and contingency measures should be considered.

Virtual Asset Trading Platforms

- 9.36 Trading platforms that facilitate the execution, matching, clearing, or settlement of virtual asset transactions must be subject to Cybersecurity controls commensurate with the custody, transactional, and market integrity risks they present. R
- 9.37 Trading platforms must ensure a clear segregation between customer assets and assets used for proprietary trading, market-making or platform operational purposes, both at a legal and technical level. R
- 9.38 This segregation should be reflected in wallet structures, distributed ledger-based systems, access controls and transaction processing logic to prevent the commingling or inappropriate use of customer assets.

Human Resource Security

- 9.39 VASPs must implement and maintain risk-based employee vetting and background screening procedures for employees, service providers, and other personnel with access to sensitive systems, customer assets or confidential information. R
- 9.40 VASPs must ensure that employees, service providers and any other relevant third parties are appropriately trained and made aware of the Cybersecurity Framework, incident identification and reporting procedures. R

Operational Resilience

- 9.41 VASPs must design, implement and maintain capacity and performance management processes that ensure the continued availability, scalability and resilience of critical systems and services, considering current and projected business demand. R

- 9.42 VASPs should integrate Cyber Resilience considerations across people, processes, and technology, and embed such considerations into both new and existing business initiatives.

10. Cyber Incident Response, Recovery and Reporting

- | | | |
|-------|--|---|
| 10.1 | A VASP must maintain arrangements to support the orderly recovery and transfer of customer virtual assets in the event of operational failure, insolvency, or the failure of a material custodian or technology provider. | R |
| 10.2 | VASPs must implement and maintain disaster recovery, business continuity plans, governance structures and controls to ensure the availability and timely recovery of critical data and systems supporting the operations of virtual asset services. | R |
| 10.3 | VASPs must maintain documented procedures governing Cybersecurity incident response and notification actions, including internal escalation, containment, recovery, customer communications, regulatory notifications and emergency protective measures. | R |
| 10.4 | Response arrangements should support timely actions to limit further loss, preserve the integrity of customer assets, and maintain appropriate oversight. | |
| 10.5 | VASPs should consider dependencies on custodians, protocols, and other service providers, as well as scenarios involving loss of access or failure of critical arrangements. Response and recovery arrangements should be reviewed periodically and updated to reflect changes in technology, custody models, and threat exposure. | |
| 10.6 | VASPs should maintain documented response and recovery arrangements that address Cybersecurity incidents affecting virtual asset custody (including wallet infrastructure and private keys) and supporting distributed ledger technologies. Such arrangements should be proportionate to the nature, scale, and complexity of the VASP's activities and aligned with the extent of control exercised over customer virtual assets. | |
| 10.7 | VASPs should identify critical systems, processes and assets, establish recovery priorities and define recovery objectives that are consistent with the potential impact on customers, markets and the ongoing viability of the VASP. | |
| 10.8 | VASPs should identify as critical any systems, processes, or assets whose disruption could lead to the loss of customer virtual assets, prevent withdrawals or deposits, disrupt trading or settlement, compromise private keys, or result in material regulatory breaches. | |
| 10.9 | Systems supporting custody services (including wallet infrastructure and key management), customer authentication, and core transaction processing would typically be considered critical, where their failure could affect many customers or expose customer assets to loss. | |
| 10.10 | Recovery arrangements should address the secure restoration of operations following a Cybersecurity incident, including validation of access, reconciliation of customer holdings, and the orderly resumption of services. | |

- 10.11 VASPs must conduct a formal post-incident review following material Cybersecurity incidents to determine root cause, assess control effectiveness and implement remedial actions. R
- 10.12 A VASP must notify the Authority promptly upon becoming aware of any actual or suspected Cybersecurity incident that has resulted in, or could reasonably result in, the loss, theft, unauthorised transfer, impairment, destruction or inaccessibility of customer virtual assets or other financial assets. R
- 10.13 The notification should include, to the extent known at the time:
- (a) the nature and circumstances of the incident;
 - (b) the date and time the incident was identified;
 - (c) the type and estimated value of the assets affected or potentially affected;
 - (d) the number and categories of customers affected or potentially affected;
 - (e) the systems, wallets, private keys, custodians, protocols or service providers involved;
 - (f) the containment, safeguarding and recovery measures taken or proposed; and
 - (g) any actual or anticipated impact on customers, the operations of the VASP or its ability to meet its obligations.
- 10.14 A VASP should not delay an initial notification where the full cause, scope or financial impact of the incident has not yet been established. The VASP should provide the information reasonably available at the time and submit material updates as further information becomes known.
- 10.15 The reporting obligation applies whether or not the affected assets are subsequently recovered, restored or reimbursed and is separate from any obligation to report the loss or compromise of personal data.

11. Outsourcing and Third-Party Risk Management

- 11.1 The Authority recognises that organisations often rely on third-party service providers to support core business functions, and that these providers frequently have access to the data and internal systems of the organisation. While such third-party ecosystems can be efficient, they also present potential entry points for cybercriminals. If a VASP chooses to outsource controls, it should maintain regular oversight of these arrangements, including formal periodic assessments, to ensure that the outsourced work remains effective and to mitigate the risk of data breaches and other Cyber threats.
- 11.2 A VASP should ensure the following is performed over any material outsourcing including IT third-party service provider, including those carrying out any related outsourced functions:
- (a) due diligence reviews;
 - (b) review of contractual terms and conditions;

- (c) review of cyber security policies, procedures and controls in place at the service provider;
 - (d) review of the incident recovery strategy of the service provider;
 - (e) review of the disaster recovery plan of the service provider;
 - (f) review of the financial stability of the service provider; and
 - (g) insurance cover of the service provider.
- 11.3 Where reliance is placed on third-party trading platforms or custodians, the VASP remains responsible for understanding and overseeing the safeguarding arrangements applicable to customer virtual assets and for assessing associated Cybersecurity and operational risks.
- 11.4 Where a VASP outsources material technology, custody, operational, or cybersecurity-related functions to a third party, the VASP must ensure that such third party complies with the applicable requirements under the VASPA, this RSOG, and any other applicable regulatory measures. R
- 11.5 For Rule 11.4, material outsourced functions may include, but are not limited to, custody arrangements, wallet infrastructure, cloud services, key management solutions, smart contract infrastructure, distributed ledger infrastructure, cybersecurity services, transaction processing, or other technology services supporting the provision of virtual asset services.
- 11.6 VASPs should maintain appropriate exit and transition arrangements for material third-party technology and service providers to support the orderly continuation, transfer, or termination of critical services, including the protection and recovery of customer assets, data, and operational capabilities.
- 12. Data Protection and Privacy**
 - 12.1 VASPs must demonstrate that data protection is part of their strategy and 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
 - 12.2 VASPs must also notify the relevant data-protection authority, being the Office of the Ombudsman, and any affected individuals, where they are legally required to do so under the DPA, of any cyber incidents that may occur. R
 - 12.3 VASPs must report to the Authority all confirmed or suspected data breaches that may materially impact customer assets, customer data, operations, or market integrity, as indicated in the Rule for Cybersecurity for Regulated Entities, and such report must include, where applicable, the affected data types, number of impacted entities or individuals, a preliminary impact assessment, containment measures, and planned follow-up actions. R
- 13. Cybersecurity Audit and Testing Program**
 - 13.1 A VASP must establish and maintain a risk-based Cybersecurity audit and testing program, proportionate to its size, complexity, and risk profile, to evaluate the effectiveness of its Cybersecurity Framework, identify vulnerabilities, and ensure that security controls operate as intended. R

- 13.2 Such a program should, at a minimum, include coverage of identity and access management controls; cryptographic key and wallet management arrangements; network and infrastructure security; change management; system configuration and vulnerability management; monitoring and logging capabilities; incident detection and response arrangements; and the effectiveness of controls over critical third-party service providers.
- 13.3 The program should also include periodic testing of systems supporting the safeguarding, transfer, and reconciliation of client virtual assets, and shall ensure that identified deficiencies are documented, prioritised, and remediated in a timely manner.
- 13.4 VASPs must conduct an independent Cybersecurity audit of its Cybersecurity Framework annually, or at such times as following any material change to its systems, operations, technology environment, or risk profile, commensurate with the size, complexity, structure, nature of business, and risk profile of its operations. Such audits may be performed using internal or external resources, provided that the audit function maintains appropriate independence, objectivity, and competence. R
- 13.5 For Rule 13.4, material changes may include, but are not limited to, significant changes to custody arrangements, wallet infrastructure, smart contract deployments, cloud environments, core systems, distributed ledger infrastructure, cybersecurity architecture, outsourcing arrangements, or other material operational or technology changes that may impact the Cybersecurity Framework of the VASP.
- 13.6 VASPs should test their recovery arrangements and business continuity on a periodic basis and following material changes to systems, processes, business activities or threat environment.
- 13.7 Recovery arrangements should be realistic, tested where practicable, and aligned with the custody model of the VASP. The Authority expects VASPs to consider scenarios involving the failure of custodians, loss of signing authority, or compromise of supporting infrastructure.
- 13.8 Testing should be proportionate to the risk profile of the VASP and may include scenario-based exercises, simulation of Cyber incidents and validation of recovery capabilities.

14. Integration with Enterprise Risk

- 14.1 A VASP must ensure that cybersecurity and virtual asset-related risks are identified, assessed, and managed as part of its enterprise-wide risk management framework. R
- 14.2 A VASP must ensure that material cyber risks, including those relating to custody, key management, and technology dependencies, are subject to appropriate governance, escalation, and reporting to the Governing Body and Senior Management. R
- 14.3 VASPs should ensure that cyber resilience considerations are embedded across enterprise risk processes, including risk assessments, risk appetite setting, and

ongoing monitoring, and that interdependencies between cyber risks and other risk categories are appropriately understood and managed.

- 14.4 Cyber resilience should not operate as a standalone function but should form part of the enterprise-wide governance, risk management, operational planning, and change management activities. This includes ensuring that staff roles and responsibilities support resilience objectives, that operational processes incorporate appropriate controls and escalation mechanisms, and that technology decisions are assessed for their potential impact on security and continuity.

15. Enforcement

- 15.1 Where the Authority determines that a VASP has failed to comply with the Rules contained in this RSOG, the policies and procedures of the Authority, as contained in its Enforcement Manual, will apply, in addition to any other powers provided in the relevant Acts and the MAA.

16. Effective Date

- 16.1 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