Cayman Monetary Regulatory Authority International

At the forefront of financial regulation, the Cayman Monetary Regulatory Authority International (CMRAI) is dedicated to upholding the highest standards of financial oversight and compliance. Our mission is to safeguard the stability and integrity of the global financial system by ensuring that financial services operate within a framework of transparency, accountability, and excellence.

As a trusted partner to financial institutions worldwide, CMRAI provides rigorous supervision, innovative solutions, and strategic guidance to foster a secure and thriving financial environment. With decades of experience and a commitment to global standards, we stand as a pillar of trust and security in an ever-evolving financial landscape.

With a legacy of excellence in financial oversight, the Cayman Monetary Regulatory Authority International (CMRAI) is a beacon of trust in the international financial community. Our role extends beyond regulation; we are innovators, collaborators, and protectors of the global financial ecosystem. By fostering compliance, promoting best practices, and embracing technological advancements, CMRAI ensures that financial services remain resilient and adaptable in a dynamic global market.

Our comprehensive approach to regulation encompasses a deep understanding of financial risks and a proactive stance on emerging challenges. We are committed to empowering financial institutions with the tools and guidance necessary to navigate complex regulatory landscapes, thereby contributing to global economic stability and growth.

1 SUMMARY OF PRIVATE SECTOR CONSULTATION AND FEEDBACK STATEMENT Amendment to certain Regulatory Measures for applicability to Virtual Asset Service Providers and other regulated entities No. Section Comments Authority s Response Consequent Amendments to the Proposed Measure Statement of Guidance - Outsourcing Regulated Entities SECTION-SPECIFIC COMMENTS 1. GENERAL N/A Language around size, nature and complexity have been refined for further clarity throughout the measure. Language refined to commensurate with the size, complexity, structure, nature of business and risk profile of its operations as follows: SOG Outsourcing Section 5.2 Rule Cybersecurity Sections 3.4 and 6.4.2 SOG Cybersecurity Sections 5.2, 6.3, 9.1 h) and 10.1 f) SOG Nature, Accessibility and Retention of Records Section 1.2 2. SOG 2.1 Exceptions: 1. regulated mutual funds as defined in the Mutual Funds Law; 2. excluded persons under the Securities Investment Business Law; and The current Scope of Application at Section 2.1 contains a footnoted exemption for "regulated mutual funds" as defined under the Mutual Funds Act and for "private trust companies" as defined in the Private Trust Companies Regulations. It is not clear why the reference to "excluded The Authority has amended the footnote. The footnote on Excluded Persons has been removed as originally intended in the May 2022 consultation. The SOG will not apply to regulated mutual funds and private trust companies. However, The footnote on excluded persons has been removed as originally intended in the May 2022 consultation. Footnote 1, Page 1 has been revised to read as follows: Exceptions are a) Regulated mutual funds as defined in the 2 3. private trust companies as defined in the Private Trust Companies Regulations. persons" under the Securities Investment Business Act has been retained: To ensure that the exemption to the SOG is applied logically and consistently with respect to certain types of regulated entities across all Regulatory Measures, Rules and SOGs, we would suggest that the following types of "regulated entities" should also be included within the list of exempted entities/persons under Section 2.1 of the SOG (e.g., for inclusion in the footnote to that provision or listed elsewhere within the SOG): a. regulated EU connected Fund as defined in the Mutual Funds Act. b. private fund as defined in the Private Funds Act. c. restricted scope private fund as defined in the Private Funds Act; and d. controlled subsidiaries as defined under the Banks and Trust Companies Act the SOG will apply to controlled subsidiaries. Oversight of service providers relating to regulated mutual funds is provided for within the SOG for Regulated Mutual Funds Corporate Governance Mutual Funds Act (as amended); b) Private Trust Companies as defined in the Private Trust Companies Regulations (as amended); and c) Private Funds as defined in the Private Funds Act (as amended). 3. SOG 2.1 This Statement of Guidance applies to all entities regulated by the Authority including controlled subsidiaries as defined in the Banks and Trust Companies Law. For the purpose of this Guidance, a regulated MAA defines regulatory laws and not acts. The other appendix all use laws. Recommend consistency between the R&G The Authority agrees to the proposed suggestion and notes that, pursuant to Law 56 of 2020, all laws should now be referred to as Acts. Therefore, all references in the Rule and Statement of Guidance will be adjusted to give effect to this change. SOG 2.1 revised to read as follows: This Statement of Guidance applies to all entities regulated by the Authority including controlled as defined in the Banks and Trust Companies Law Act (as amended). For the purpose of 3 entity is

an entity that is regulated by the Authority in accordance with the regulatory laws, as defined in the Monetary Authority Act (as amended). this Guidance, a regulated entity is an entity that is regulated by the Authority in accordance with the regulatory laws Acts, as defined in the Monetary Authority Law Act (as amended). 4. SOG 2.2 This Guidance applies regardless of whether the outsourcing arrangement established by a regulated entity is with a related or unrelated entity. Insertion of a new paragraph has been removed. The Authority agrees to the proposed amendment. The noted paragraph was inadvertently deleted and has now been reinserted. SOG 2.3, reinserted and read as follows: This Guidance should not preclude the need for all functions and activities (whether material or not) to be subject to adequate risk management and sound internal controls. 5. SOG 3.1.6 Governing Body: in the case of a company, the Board of Directors and in the case of partnerships, the general partners. In the case of a branch or of an entity incorporated or established outside of the Cayman Islands, a management committee or body (beyond local management) empowered with oversight and supervision responsibilities for the entity in the Cayman Islands. 3.1. has reverted to its pre-May 2022 (pre-con) version. The Authority has reviewed and amended the definition of governing body. Governing body definition, SOG 3.1.6 revised to reads as follows: Governing Body: the Board of Directors where the entity is a corporation, the General Partner where the entity is a partnership, the manager (or equivalent) where the entity is a Limited Liability Company, and the Board of Trustees where the entity is a trust business. In the case of a company, the Board of Directors and in the case of partnership, the general partners. In the case of a branch of an entity incorporated or established outside of the Cayman Islands, a management committee or body (beyond local management) empowered with oversight and supervision 4 responsibilities for the entity in the Cayman Islands. 6. SOG 5.9 A regulated entity should ensure that all books and records pertaining to its outsourced material functions or activities, including any record of transaction activities for clients, are readily accessible to the Authority. readily accessible : What does this mean (within an hour, a day, a week)? The Authority recommends regulated entities be guided by SOG 4.2, Statement of Guidance on Nature, Accessibility and Retention of Records, which states: Accessible records are records that can be provided by the regulated entity to the Authority within a reasonably short timeframe. The Authority expects that most records should be provided within 1-3 business days from the time they are requested by the Authority, or within the timeframe as determined from time to time by the Authority, whether stored within the Cayman Islands or in another jurisdiction. No amendments are required. 7. SOG 5.11 Regulated entities should assess their outsourcing risk management framework and address any deficiencies within a year of the issue of this Guidance. Should this be re-worded? What happens if a newly regulated entity is found to not comply with this SOG? The Authority has reviewed and amended SOG 5.11. SOG 5.11 revised to read as follows: Regulated entities should assess their outsourcing risk management framework and address any deficiencies as appropriate. within a year of the issue of this Guidance.. 5 8. SOG 9.7 Outsourcing agreements should allow the regulated entity to conduct audits on the Service Provider and its sub-contractors with respect to the material outsourced material function or activity, whether by its internal and external auditors or by agents appointed by it. Duplication of the word material . The Authority has reviewed and amended SOG 9.7. SOG 9.7 revised to read as

follows: Outsourcing agreements should allow the regulated entity to conduct audits on the Service Provider and its sub-contractors with respect to the material outsourced material function or activity, whether by its internal and external auditors or by agents appointed by it. 9. Footnote 1, page 1 References to "Law" should be amended to "Act" in accordance with the Citation of Acts of Parliament Act,2020. The Authority agrees to the proposed amendment and has updated the measure to ensure consistency throughout. References to Law have been amended to Act throughout the measure. We would propose extending this exception to private funds (In addition to mutual funds). We assume reference to "excluded persons" should be deleted as this concept has now been superseded by amendments to the Securities Investment Business Act. The Authority agrees to the proposed amendment. Footnote 1, Page 1 has been revised to read as follows: Exceptions are a) Regulated mutual funds as defined in the Mutual Funds Act (as amended); b) Private Trust Companies as defined in the Private Trust Companies Regulations (as amended); and c) Private Funds as defined in the Private Funds Act (as amended). RULE - Cybersecurity for Regulated Entities 10. Rule 1.1 To set out the Cayman Islands Monetary Authority s (the Authority) Rule on cybersecurity applicable to regulated entities, pursuant to Same comment as 3.1 applies throughout the document (e.g., 1.1, 2.1 etc.) The Authority agrees to the proposed amendment. Rule 1.1 amended as follows: To set out the Cayman Islands Monetary Authority s (the Authority) Rule on cybersecurity Rule 1.1 has been amended and now reads as follows: To set out the Cayman Islands Monetary Authority s (the Authority) Rule on cybersecurity applicable to regulated entities, 6 the Monetary Authority Law (MAL). applicable to regulated entities, pursuant to the Monetary Authority Act Law (MAL) (MAA) pursuant to the Monetary Authority Act (MAA). 11. Rule 3.1 This Rule applies to entities regulated by the Authority including controlled subsidiaries as defined in the Banks and Trust Companies Law. For the purpose of this Rule, a regulated entity is an entity that is regulated by the Authority in accordance with the regulatory laws, as defined in the Monetary Authority Act (as amended). No need to use the long form of Monetary Authority Act, the acronym MAA is defined in 1.1. Change to MAA The Authority has reviewed and amended Rule 3.1 as follows: This Rule applies to entities regulated by the Authority including controlled subsidiaries as defined in the Banks and Trust Companies Law Act (as amended) For the purpose of this Rule, a regulated entity is an entity that is regulated by the Authority in accordance with the regulatory laws Acts, as defined in the Monetary Authority Act MAA (as amended). Rule 3.1 revised to read as follows: This Rule applies to entities regulated by the Authority including controlled subsidiaries as defined in the Banks and Trust Companies Act (as amended). For the purpose of this Rule, a regulated entity is an entity that is regulated by the Authority in accordance with the regulatory Acts, as defined in the MAA (as amended). 12. 3.1 Footnote 1, page 3 Exceptions: Regulated mutual funds The current Scope of Application at Section 3.1 contains a footnoted exemption for "regulated mutual funds" [as defined under the Mutual Funds Accordingly, to ensure that the exemption to the Rule is applied logically and consistently with respect to certain types of regulated entities across all Regulatory Measures, Rules and SOGs, we would suggest that the following types of "regulated entities" should also be included within the list of Please see the response provided above for SOG 2.1 by the Authority. Footnote 1, page 3 has been revised to read as follows:

Exceptions are a) Regulated mutual funds as defined in the Mutual Funds Act (as amended); and b) Private Funds as defined in the Private Funds Act (as amended). 7 exempted entities/persons under 3.1 (e.g., for inclusion in the footnote to that provision or listed elsewhere within the SOG): a. regulated EU connected Fund as defined in the Mutual Funds Act; b. private fund as defined in the Private Funds Act; c. restricted scope private fund as defined in the Private Funds Act; and d. controlled subsidiaries as defined under the Banks and Trust Companies Act 13. Rule 2.1 2.1. Section 34(1)(a) of the MAL provides that: After private sector consultation and consultation with the Minister charged with responsibility for Financial Services, the Authority may - Same comment as 3.1 applies throughout the document (e.g., 1.1, 2.1 etc.) The Authority has reviewed and amended Rule 2.1 as follows: Section 34(1)(a) of the MAL MAA provides that: After private sector consultation and consultation with the Minister charged with responsibility for Financial Services, the Authority may - ... Rule 2.1 revised to read as follows: 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 ... 14. Rule 2.2 Rule 2.2 - Reference to other measures currently includes some which will be repealed. Revise list and/or consider more general capture of the necessary reference to other relevant measures. After consultations, listed regulatory instruments deleted and a general capture of regulatory instruments issued by Authority adopted. Rule 2.3 merged with Rule 2.2 to avert repetition. Consequently, Rule 2.2 amended to better capture reference to regulatory instruments issued by the Authority, and reads as follows: This document establishes the Rule on cybersecurity for regulated entities and should be read in conjunction, with other regulatory instruments issued by the 8 Authority from time to time, where applicable. 15. Rule 3.1 Rule 3.1 - (Footnote 1) Move reference to after Authority . Reference placement of similar footnote in SOG. For consistency, footnote moved after Authority Rule 3.1 footnote 1 location moved accordingly. 16. Rule 3.2 Removal of an addition: paragraph 3.2 The Authority agrees to the proposed amendment and reinserted the paragraph that had been inadvertently deleted. Rule 3.2, reinserted and read as follows: References to any act or regulation shall be construed as references to those provisions as amended, modified, re-enacted, or replaced from time to time. 17. Rule 4.1.10 Governing body: In the case of a company, the term refers to the Board of Directors. In the case of partnerships, the term refers to the general partners. In the case of a branch or of an entity incorporated or established outside of the Cayman Islands, the term refers to a management committee or body (beyond local management) empowered with oversight and supervision responsibilities for the entity in the Cayman Islands. Rule 4.1.10 has reverted to its pre-May 2022 (pre-con) version. The Authority has reviewed and amended definition of governing body; RULE 4.1.10 as follows: Governing Body: the Board of Directors where the entity is a corporation, the General Partner where the entity is a partnership, the manager (or equivalent) where the entity is a Limited Liability Company, and the Board of Trustees where the entity is a trust business. In the case of a company, the Board of Directors and in the case of partnership, the general partners. In the case of a branch Governing body definition, RULE 4.1.10 revised to read as follows: Governing Body: the Board of Directors where the entity is a corporation, the General Partner where the entity is a partnership, the manager (or equivalent) where the entity is a Limited Liability Company, and the Board of Trustees

where the entity is a trust business. 9 of an entity incorporated or established outside of the Cayman Islands, a management committee or body (beyond local management) empowered with oversight and supervision responsibilities for the entity in the Cayman Islands. 18. Rule 3.3 Regulated entities that are natural persons must ensure that services offered to clients are not carried out in such a way that compromises the confidentiality, integrity and availability of clients data or the regulated entities systems, where applicable. Regulated entities should apply this Rule and consider the corresponding Statement of Guidance (SOG) Cybersecurity for Regulated Entities, where applicable, to ensure that there is a suitable and robust cybersecurity framework in place. The Scope of Application at Section 3.3 is confusing as currently drafted. The provision refers to "Regulated entities that are natural persons" We would suggest that this paragraph is reworded as follows: "Although natural persons which are subject to regulation under the regulatory laws are not subject to this Rule, they should nevertheless ensure that services offered to clients are not carried out in such a way that compromises the confidentiality, integrity and availability of clients data or the regulated entities systems, where applicable. Regulated entities should apply this Rule and consider the corresponding Statement of Guidance (SOG) Cybersecurity for Regulated Entities, where applicable, to ensure that there is a suitable and robust cybersecurity framework in place. The Authority has reviewed the suggestion and amended Rule 3.3 as follows: Regulated entities that are natural persons must ensure that services offered to clients are not carried out in such a way that compromises the confidentiality, integrity and availability of clients data or the regulated entities systems, where applicable. Regulated entities should apply this Rule and consider the corresponding Statement of Guidance (SOG) Cybersecurity for Regulated Entities, where applicable, to ensure that there is a suitable and robust cybersecurity framework in place. . Rule 3.3 revised to read as follows: Regulated entities must ensure that services offered to clients are not carried out in such a way that compromises the confidentiality, integrity and availability of clients data or the regulated entities systems, where applicable. Regulated entities should apply this Rule and consider the corresponding Statement of Guidance (SOG) Cybersecurity for Regulated Entities, where applicable, to ensure that there is a suitable and robust cybersecurity framework in place. 10 Statement of Guidance: Cybersecurity for Regulated Entities 19. General Comment The Acronym MAL is used throughout the document. We note that this should be MAA for Monetary Authority Act. The Authority agrees to the proposed suggestion and notes that, pursuant to Law 56 of 2020, all laws should now be referred to as Acts. Therefore, all references in the Rule and Statement of Guidance will be adjusted to give effect to this change. All mentions of the acronym MAL replaced with MAA throughout the measure. 20. SOG 2.2 SOG 2.2 - Reference to other measures currently includes some which will be repealed. Revise list and/or consider more general capture of the necessary reference to other relevant measures. After consultations, listed regulatory instruments deleted and a general capture of regulatory instruments issued by Authority adopted. SOG 2.3 merged with SOG 2.2 to avert repetition. SOG 2.2 revised to read as follows: This Guidance should be read in conjunction, with other regulatory instruments issued by the Authority from time to time, where applicable. 21. 3.1 Footnote 1, page 3 Exceptions: regulated mutual funds The current Scope of Application at Section 3.1 contains a footnoted exemption for "regulated mutual funds" [as defined under the

Mutual Funds Act]. Accordingly, to ensure that the exemption to the Rule is applied logically and consistently with respect to certain types of regulated entities across all Regulatory Measures, Rules and SOGs, we would suggest that the following types of "regulated entities" should also be included within the list of exempted entities/persons under 3.1 (e.g., for inclusion in the footnote to The Authority has amended the footnote. Footnote 1, Page 3 revised to read as follows: Exceptions are a) Regulated mutual funds as defined in the Mutual Funds Act (as amended); and b) Private Funds as defined in the Private Funds Act (as amended). 11 that provision or listed elsewhere within the SOG): e. regulated EU connected Fund as defined in the Mutual Funds Act. f. private fund as defined in the Private Funds Act; g. restricted scope private fund as defined in the Private Funds Act; and h. controlled subsidiaries as defined under the Banks and Trust Companies Act. 22. SOG 3.2 Removal of additional 3.2 in the May 2022 (pre-con). The Authority agrees to the proposed amendment and reinserted the paragraph that had been inadvertently deleted. SOG 3.2, reinserted and reads as follows: References to any act or regulation shall be construed as references to those provisions as amended, modified, re-enacted or replaced from time to time. 23. SOG 5.4 Regulated entities can consider reputable international standards or frameworks on cybersecurity, IT Security and Technology Risk Management (TRM) in developing an appropriate cybersecurity risk management framework or their risk profile and risk tolerance. The National Institute of Standards and Technology (NIST), Control Objective for Information and Related Technologies (COBIT), regulated entities can consider : Is this a suggestion to regulated entities or is this a requirement? If this is a requirement, this should be re-worded. The Authority has reviewed and amended SOG 5.4 as follows: Regulated entities can consider should take into consideration reputable international standards or frameworks on cybersecurity, IT Security and Technology Risk Management (TRM) in developing an appropriate cybersecurity risk management framework or their risk profile and risk tolerance. The National Institute of Standards and Technology (NIST), Control Objective for Information and Related Technologies (COBIT), SOG 5.4, revised to read as follows: Regulated entities should take into consideration reputable international standards or frameworks on cybersecurity, IT Security and Technology Risk Management (TRM) in developing an appropriate cybersecurity risk management framework or their risk profile and risk tolerance ... 12 Information Technology Infrastructure Library (ITIL) and International Organization for Standardization (ISO) are some examples of recognised standards in these areas, but the reference made to them in this Guidance should not be deemed as an endorsement by the Authority of any one standard or framework. Future standards/frameworks may emerge that are reputable and regulated entities should consider all standards/frameworks that help them develop the most robust and prudent cybersecurity framework to meet their needs and those of their clients. Information Technology Infrastructure Library (ITIL) and International Organization for Standardization (ISO) are some examples of recognised standards in these areas, but the reference made to them in this Guidance should not be deemed as an endorsement by the Authority of any one standard or framework. Future standards/frameworks may emerge that are reputable and regulated entities should consider all standards/frameworks that help them develop the most robust and prudent cybersecurity framework to meet their needs and those of their clients. 24. SOG 5.5 Regulated entities that are natural persons should ensure

that services offered to clients are not carried out in such a way that compromises the confidentiality, integrity and availability of clients data or the regulated entities systems, where applicable, and the Rule along with this Guidance should be considered and applied, where applicable. General guidance at Section 5.5, should also be reworded as it is confusing as currently drafted. The provision refers to "Regulated entities that are natural persons". We would suggest that this paragraph is reworded as follows: "Although natural persons which are subject to regulation under the regulatory laws are not subject to this Guidance, they should nevertheless ensure that services offered to clients are not carried out in such a way that compromises the confidentiality, integrity and availability of clients data or the regulated entities systems, Please see the response provided above for Rule 3.3 by the Authority. No further amendments are required. 13 where applicable, and the Rule along with this Guidance should be considered and applied, where applicable." 25. SOG 7.2.4(g).v establishing of a plan of action to address the identified deficiencies. Consider changing to establishing a plan (removing of) The Authority has reviewed and amended SOG 7.2.4 (g).v as follows: establishing of a plan of action to address the identified deficiencies SOG 7.2.4(g).(v) has been updated and reads as follows: establishing a plan of action to address the identified deficiencies. 26. SOG 9.2. (a). ii 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 and authenticated and secured against exploits such as account takeovers, automated teller machine skimming, card cloning, hacking, phishing and malware This could be expanded to include 2FA hijacking (sim swap attack), ransomware, etc. This could be added to e or a. ii The Authority agrees to the proposed amendment. The list is not intended to be exhaustive but rather sets out examples of online exploits. SOG 9.2. (a). ii revised to read as follows: 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 and authenticated and secured against exploits such as account takeovers, automated teller machine skimming, card cloning, hacking, phishing,2FA hijacking, ransomware and malware. 14 27. SOG 13.3.(e) Regulated entities should monitor and review the security policies, procedures, and controls of the service provider on a regular basis, including commissioning or obtaining periodic independent audits on cybersecurity adequacy and compliance in respect of the operations and services provided. It may be incredibly difficult to comply with this guidance for certain larger cloud hosts, such as amazon web services or other larger cloud computing providers. For example, a regulated entity may not be in a position to request, or even demand, an independent cybersecurity audit on larger cloud platforms. Instead, please consider international certifications as alternatives. Many large outsourcing providers abide and are certified by globally recognized certification standards. It should be sufficient for a regulated entity to ensure that a larger service provider (such as amazon web services) is compliant and has been certified. The Authority agrees to the proposed revisions. SOG 13.3.(e) amended as follows: Regulated entities should monitor and review the security policies, procedures and controls of the service provider on a regular basis to ensure they have robust controls in place to maintain security and compliance in the cloud as per set international standards, including commissioning or obtaining periodic independent

audits on cybersecurity adequacy and compliance in respect of the operations and services provided. SOG 13.3.(e) revised to reads as follows: Regulated entities should monitor and review the security policies, procedures and controls of the service provider on a regular basis to ensure they have robust controls in place to maintain security and compliance in the cloud as per set international standards, including commissioning or obtaining periodic independent audits on cybersecurity adequacy and compliance in respect of the operations and services provided. New Footnote 4, added to read as follows: International certifications include ISO 9001:2015 Compliance, Cloud security alliance, Cyber GRX, Cybervadis, Security standards council etc.

15 Statement of Guidance - Nature, Accessibility and Retention of Records 28. General Comment The Acronym MAL is used throughout the document. We note that this should be MAA for Monetary Authority Act The Authority agrees to the proposed suggestion and notes that, pursuant to Law 56 of 2020, all laws should now be referred to as Acts. Therefore, all references in the Rule and Statement of Guidance will be adjusted to give effect to this change. All mentions of the acronym MAL replaced with MAA throughout the measure. 29. SOG 1.4. Record keeping requirements apply to all relevant persons and entities. relevant persons and entities : term used throughout but not defined. The Authority has reviewed and amended SOG 1.4 as follows: Record keeping requirements apply to all regulated relevant entities. SOG 1.4 revised to read as follows: Record keeping requirements apply to all regulated entities. 30. SOG 3.2 Removal of additional 3.2 in the May 2022 (pre-con). The Authority agrees to the proposed amendment and reinserted the paragraph that had been inadvertently deleted. SOG 3.2 reinserted and reads as follows: References to any act or regulation shall be construed as references to those provisions as amended, modified, re-enacted or replaced from time to time.