Virtual Assets Services Providers Act No. 3 of 2025

CYBERSECURITY AUDIT METHODOLOGY

AND

FINDINGS REPORT FRAMEWORK

INDEPENDENT AUDITOR EDITION

For VASP Cybersecurity Type 2 Applicants

(Class D.x Licence Applicants with Custody of or Access to Customer Virtual Assets)

Date: March 2026

Developed by SixBlocks Audit for VFSC Supervision Department

Intellectual Property Assignment and Unrestricted Use (Pro Bono)

Ownership / Assignment (NZ); Rights Warranty; Moral Rights Waiver & Consent; No Injunction

1. Assignment. SixBlocks Audit, a division of Confide Limited NZBN: 9429032598216 ("SixBlocks") hereby **assigns to the Vanuatu Financial Services Commission ("VFSC") all right, title and interest**, including all **intellectual property rights and copyright (present and future)**, in and to the document titled **[VFSC_Cybersecurity_Audit_Methodology_Independent_Auditor_Edition_Draft_1_Release.docx – version 1]** (including any annexes, templates, extracts, working papers and materials, and any updates or revised versions provided by SixBlocks in connection with it) (the "Deliverable"). This assignment is **effective upon creation** of the Deliverable (and, to the extent any rights do not vest immediately, SixBlocks assigns such rights **as they arise**).

2. Pro bono / no fees. The Deliverable is provided **pro bono**. VFSC may **use, reproduce, modify, adapt, publish, distribute, communicate, and otherwise exploit** the Deliverable **without restriction** and **without any payment now or in the future**, regardless of any later change in SixBlocks' policies or the pro bono status of the work.

3. Warranty of rights / non-infringement. SixBlocks **warrants** that:
(a) it **owns or controls** all rights necessary to make the assignment in clause 1;
(b) the Deliverable does not incorporate third-party material except where SixBlocks has all permissions needed for VFSC to use it as contemplated; and
(c) VFSC's use of the Deliverable will **not infringe** any third party's intellectual property or other rights.

4. Moral rights waiver and consent (NZ). To the fullest extent permitted under the **Copyright Act 1994 (NZ)** (and any equivalent laws), SixBlocks **waives, and will procure from each author/creator of the Deliverable a waiver of**, all **moral rights**, including the right to be identified as author, the right to object to derogatory treatment, and rights relating to false attribution. Without limiting the foregoing, SixBlocks **consents (and will procure each author's consent)** to VFSC (and its contractors, auditors, advisers and stakeholders) **editing, adapting, updating, translating, combining with other material, and otherwise using** the Deliverable, and to VFSC **not crediting** any author, and SixBlocks agrees no such acts will be alleged to infringe moral rights.

5. Further assurances. SixBlocks will promptly **do all acts and sign all documents** reasonably required to give full effect to this clause, including confirming the assignment and providing copies of any executed author waivers/consents.

6. No injunctive relief / no stop-use demand. To the fullest extent permitted by law, SixBlocks **waives any right to seek injunctive relief or any other equitable remedy** (including any order requiring VFSC to cease or restrict use) that would **prevent, limit, or interfere with VFSC's use** of the Deliverable as contemplated by this clause.

Marc Krisjanous – Associate Director of Audit – SixBlocks Audit.

4 March 2026

Introduction for Independent Auditors

Purpose of This Document

This document is the Independent Auditor Edition of the VFSC VASP Cybersecurity Audit Methodology and Findings Report Framework. It has been prepared specifically for independent cybersecurity auditors approved by the Vanuatu Financial Services Commission (VFSC) to conduct cybersecurity audits of Virtual Asset Service Provider (VASP) applicants and licensees under the Virtual Assets Services Providers Act No. 3 of 2025 who are classified as VASP Cybersecurity Type 2.

This edition focuses on the auditor's mandate, responsibilities, and required deliverables. It contains the complete audit methodology framework, risk rating system, control testing procedures, and report templates that the auditor must follow when conducting VFSC cybersecurity audits.

Scope of the Auditor's Role

The independent cybersecurity auditor's role encompasses three categories of engagement:

(a) Baseline cybersecurity audits for new VASP licence applicants, evaluating control design and implementation readiness against the applicable cybersecurity criteria.

(b) Ongoing assurance activities between annual audits, including remediation verification, periodic desk-based reviews, and assurance letters to the VFSC, with frequency and depth determined by the VASP's assigned supervision level.

(c) Annual cybersecurity audits of licensed VASPs, evaluating the operating effectiveness of controls over the preceding 12-month period, with scope and intensity determined by the VASP's supervision level.

The auditor may also be directed by the VFSC to conduct event-driven audits in response to specific incidents, threats, or material changes.

Document Structure

This document is organised as follows:

Part 1 sets out the audit methodology framework, including the audit phases, the auditor's ongoing responsibilities between annual audits, and the annual audit tiers.

Part 2 establishes the five-tier risk rating framework that the auditor applies when classifying findings, including the nonconformity classification system, aggregation escalation framework, and the programme maturity audit methodology.

Part 3 defines the supervision level categories and the risk score calculation methodology that the auditor uses to derive supervision level recommendations.

Part 4 contains the CCSS V9-aligned control testing procedures for all ten aspects across Cryptographic Asset Management and Operations.

Part 4A contains supplementary control testing procedures covering broader cybersecurity controls beyond the CCSS V9 scope.

Appendix A provides worked findings examples demonstrating the application of the finding documentation format.

Appendix B explains the programme maturity aggregation methodology (the Critical Domain Principle) that the auditor applies when deriving overall programme maturity from domain-level audits.

Appendix C identifies red flags that should prompt deeper investigation during the audit.

Appendix D provides the audit findings report templates, including the executive summary format, individual finding documentation format, and the complete report structure.

Appendix E provides the quarterly assurance letter template for reporting to the VFSC between annual audits.

Appendix F provides a reference to the VASP-facing reporting templates that are contained in the complete VFSC edition of this methodology.

Key Auditor Obligations

Throughout this document, the auditor's core obligations include: conducting audits in accordance with the methodology and testing procedures set out in Parts 1 through 4A; classifying findings using the five-tier risk rating framework in Part 2; providing supervision level recommendations using the methodology in Part 3; issuing periodic assurance letters to the VFSC using the template in Appendix E; and maintaining independence and professional scepticism throughout all engagements.

VASP and VFSC Reference Material

This Independent Auditor Edition includes summary references to certain VASP licensee obligations and VFSC supervisory activities (Sections 1.2.2.1 and 1.2.2.3, respectively). These summaries provide the auditor with sufficient context to understand the VASP's reporting obligations and the VFSC's supervisory framework. The complete details, including VASP-facing reporting templates, are contained in the full VFSC edition of this methodology.

Table of Contents

Part 1: Audit Methodology Framework

The Vanuatu Financial Services Commission (VFSC) requires a rigorous, internationally aligned methodology to assess cybersecurity controls for a Virtual Asset Service Provider (VASP) seeking a Class D.x licence under the Virtual Asset Service Providers Act No. 3 of 2025, where the licensed activities involve custody of, or control over, customer virtual assets. This framework integrates ISAE 3000 (Revised) assurance principles, supervisory best practices, and virtual-asset-specific cybersecurity control considerations into a comprehensive approach for evaluating the protection of key material and supporting systems.

Terminology Note: VFSC Cybersecurity Applicant Types

This methodology distinguishes VFSC's cybersecurity applicant classification, which is based on whether the applicant can materially affect the security of customer virtual assets:

VASP Cybersecurity Type 1: Applicants that do not control, and do not have access to, customer virtual asset key material and therefore cannot directly or indirectly impact the security of customer funds (e.g., certain non-custodial activity models such as derivatives traders, where custody functions are not performed).

VASP Cybersecurity Type 2: Applicants that can directly or indirectly impact the security of customer funds through custody of, access to, or control over key material (e.g., exchanges, custody providers, staking providers, stablecoin issuers, and token issuers where the issuer retains administrative or technical control that can affect customer assets).

For the purposes of this methodology, "VASP Cybersecurity Type 2" refers to applicants seeking a Class D, Class D.2, or Class D.4 licence, or any other licence class where the applicant performs custody functions or can materially influence the security of key material controlling customer assets. This methodology applies to VASP Cybersecurity Type 2 applicants and licensees.

Assurance Standard Basis and Engagement Scoping (Cybersecurity Only)

Because this methodology addresses cybersecurity controls, the assurance engagement is conducted under ISAE 3000 (Revised) rather than service-organisation reporting standards that are designed for controls relevant to financial reporting.

Under ISAE 3000 (Revised), the auditor's work should be scoped and reported using clear, cybersecurity-appropriate terms, typically in one of the following formats:

1. A point-in-time ("as at") baseline audit evaluates the design and implementation readiness of cybersecurity controls "as at" a specified date (appropriate for initial licensing or pre-licensing baseline audits).
2. A period-of-time ("throughout") operating effectiveness audit evaluates whether cybersecurity controls operated effectively throughout a defined period

(appropriate for ongoing supervision), typically covering up to 12 months or a shorter period when enhanced supervision cadence is required.

1.1 Assurance Standards Foundation

The VFSC VASP cybersecurity audit methodology is performed in accordance with ISAE 3000 (Revised), which applies to assurance engagements other than audits or reviews of historical financial information.

ISAE 3000 (Revised) supports both reasonable assurance and limited assurance engagements. In a reasonable assurance engagement, the practitioner obtains sufficient appropriate evidence to reduce engagement risk to an acceptably low level and expresses the conclusion in a positive form (i.e., "In our opinion, [the subject matter] is [prepared/effective], in all material respects, in accordance with the applicable criteria"). In a limited assurance engagement, conclusions are expressed in a form that conveys whether anything has come to the practitioner's attention to indicate material misstatement (i.e., "nothing has come to our attention…" style).

For VASP cybersecurity licensing audits, this methodology is designed to support reasonable assurance by default, given the regulatory significance of licensing decisions and the potentially serious consequences of an inappropriate conclusion (noting that ISAE 3000 recognises circumstances where those consequences may be so great that reasonable assurance is needed for the assurance to be meaningful). Any use of limited assurance should be explicitly determined/approved as part of the engagement mandate.

This methodology uses the VFSC VASP cybersecurity classification system, which categorises applicants as VASP Cybersecurity Type 1 (no custody of customer funds) or VASP Cybersecurity Type 2 (custody of, or access to, customer funds). This audit methodology applies to VASP Cybersecurity Type 2 applicants and licensees. (This “Type 1 / Type 2” terminology is specific to VFSC’s custody-based classification and is not used in this methodology to describe assurance report formats.)

For the initial cybersecurity baseline audit of a VASP applicant, the engagement scope should be defined as a point-in-time audit (e.g., “as at [date]”) focused on control design and implementation readiness against the applicable cybersecurity criteria. For ongoing supervision, the engagement scope should be defined as a period-of-time audit focused on operating effectiveness (e.g., “throughout the period [start date] to [end date]”), typically over a 12-month period or a shorter period where a higher supervision cadence is required.

This methodology addresses cybersecurity controls for VASP applicants and licensees. AML/CFT compliance obligations are addressed under the Anti-Money Laundering and Counter-Terrorism Financing Act No. 13 of 2014 and related FIU processes and are not the primary focus of this cybersecurity methodology. Where audit controls intersect with AML/CFT obligations, particularly KYC data protection, transaction monitoring system

security, and travel rule data security, the auditor should coordinate with the VASP's AML/CFT compliance function to avoid duplication and ensure coherent coverage.

1.1.1 Hybrid VFSC VASP Cybersecurity Audit Methodology Comparison

Element	Assurance Approach	Regulatory Approach	VFSC VASP Cybersecurity
Objective	Express opinion on controls	Verify compliance, identify violations	Inform licensing decision with risk-based recommendations
Independence	Practitioner independence required	Government authority	VFSC-appointed or approved auditors with independence attestation
Criteria	Professional standards	Statutory requirements	Virtual Asset Service Providers Act No. 3 + CCSS V9 Level II minimum + ISO/IEC 27001/2+ regulatory expectations
Output	Audit opinion	Examination report with Matters Requiring Attention (MRA)	Findings report with risk ratings and supervision recommendations

1.2 Audit Phases for VASP Licensing Audits

The VFSC cybersecurity assurance framework operates as a continuous lifecycle comprising three distinct phases that together provide ongoing assurance over the security of customer virtual assets.

The **Baseline Cybersecurity Audit** (Section 1.2.1) establishes the VASP applicant's initial security baseline posture during the licensing process, applying a point-in-time audit approach to evaluate control design and implementation readiness.

Following the grant of a VASP licence, the **Continuous Monitoring and Improvement** phase (Section 1.2.2) maintains ongoing assurance between formal audits by combining VASP self-reporting obligations, external cybersecurity auditor oversight activities, and VFSC supervisory engagement. The frequency and intensity of these monitoring activities are determined by the supervision level assigned under Part 3 of this methodology.

The **Annual Cybersecurity Audit** (Section 1.2.3) provides periodic independent assurance that the VASP's cybersecurity controls remain effective and that previously identified nonconformities have been appropriately remediated. Critically, the annual cybersecurity audit transitions to evaluating the operating effectiveness of controls over the preceding 12-month period rather than merely the cybersecurity controls design and existence.

The annual audit scope and intensity are risk-proportionate, ranging from a focused review for VASPs under standard supervision to a comprehensive reaudit for those under intensive supervision. This lifecycle approach aligns with the Vanuatu Virtual Assets Services Providers Act No. 3 of 2025 - Section 54 (quarterly compliance reporting) and Section 55 (annual independent audit report), and with Section 59 (Commissioner's power to issue guidelines). The VFSC Cybersecurity Guideline issued pursuant to this power specifies cybersecurity assurance requirements, including annual independent vulnerability audit and penetration testing (and, where relevant, smart contract review).

1.2.1 Baseline Cybersecurity Audit

The baseline cybersecurity audit establishes the VASP applicant's cybersecurity posture at the time of their initial VASP licence application and determines whether the applicant meets the minimum cybersecurity threshold required for licensing.

1.2.1.1 Licensing Threshold Policy

The VFSC will not grant a VASP licence to any applicant whose baseline cybersecurity audit identifies one or more findings rated as Critical or High. This policy reflects the principle that a VASP must demonstrate an adequate cybersecurity posture *before* being entrusted with custody of customer virtual assets, not after. Where the baseline audit identifies Critical or High findings, the auditor shall prepare a Gap and Remediation Report (Section 1.2.1.8) setting out the deficiencies and the remediation actions required. The applicant must remediate all Critical and High findings and undergo verification by the independent auditor before the licence application can proceed.

1.2.1.2 Post-Licence Context

This VASP licensing threshold applies only to baseline audits for new licence applications. For licensed VASPs, Critical or High findings may emerge through continuous monitoring, event-driven audits, thematic reviews or annual cybersecurity audits. In these post-licence contexts, the emergence of Critical or High findings triggers the appropriate supervision response (enhanced or intensive supervision) rather than automatic licence revocation. It is recognised that a licensee's cybersecurity posture may deteriorate over time, and the supervisory framework is designed to address such deterioration through structured remediation and regulatory oversight.

1.2.1.3 Phase 1: Planning and Scoping

The baseline cybersecurity audit begins with a comprehensive scope validation that identifies all VASP products and services covered by the VASP licence application,

including all key material operational cybersecurity controls and supporting operational and governance controls for the VASP cybersecurity Type 2 applicant. Auditors must identify all people, processes and technology components that can directly or indirectly affect the security of key material – this will be the audit boundary (or scope).

1.2.1.4 Phase 2: Fieldwork and Evidence Gathering

Control testing employs four evidence-gathering techniques for cryptocurrency-specific platforms:

1. **Review** of documentation, including policies, standards, procedures and Business as Usual (BAU) outputs. The auditor's goal is to understand the organisation's goals for its cybersecurity posture (policies), awareness and use of industry-recognised best practices (standards), well-documented processes (procedures), and the effective outputs of the execution of documented processes (BAU outputs).
2. **Interviews** with personnel assigned roles that could directly or indirectly impact the security of key material. Interviews involve discussions with personnel about the controls that have been implemented and ongoing maintenance and improvement of the controls.
3. **Inspection** of control configurations to ensure the organisation's documented requirements for system configurations are adhered to, for example, no "shadow IT"[1].
4. **Observation** of processes to ensure personnel follow documented policies and procedures.

Throughout the fieldwork phase, the auditor should record observations relevant to the overall maturity of the VASP's cybersecurity programme. These observations go beyond individual control pass/fail determinations and should capture qualitative indicators such as:

(1) The extent to which security activities are driven by documented policy versus ad hoc decisions.
(2) Whether personnel demonstrate awareness of and commitment to the security programme.
(3) The degree of integration between security processes and business operations.
(4) The sophistication of risk management practices.
(5) The evidence of management engagement with and investment in cybersecurity.

These observations are integrated during the Findings and Maturity Determination phase (Phase 3) to inform the overall programme maturity audit under Section 2.6.

1.2.1.5 Phase 3: Findings and Maturity Determination

Following the completion of fieldwork, the auditor should undertake a structured review of all findings, evidence, and observations before drafting the audit report. This phase

[1] https://en.wikipedia.org/wiki/Shadow_IT

serves two purposes: it ensures that individual findings are considered collectively rather than in isolation, and it establishes the overall programme maturity level that directly informs the supervision level recommendation.

1.2.1.5.1 Findings Aggregation and Pattern Analysis

The auditor should review all individual findings collectively to identify patterns, common root causes, and systemic weaknesses that may not be apparent from individual control audits alone. This analysis directly feeds the aggregation escalation framework described in Section 2.2.3, where the accumulation of minor nonconformities may evidence systemic failure warranting reclassification as a major nonconformity. The auditor should document the aggregation analysis, recording which findings were considered collectively, the pattern or common root cause identified, and whether any classification was escalated.

1.2.1.5.2 Programme Maturity Determination

Using the evidence gathered during fieldwork and the qualitative observations recorded throughout the engagement, the auditor should determine the VASP's cybersecurity programme maturity level in accordance with the five-level model defined in Section 2.6. The determination requires an assessment across each of the five maturity domains: Governance and Leadership, Risk Management, Control Implementation, Monitoring and Measurement, and Continuous Improvement. For each domain, the auditor should assign a maturity level supported by specific evidence from the fieldwork, including references to documents reviewed, interviews conducted, configurations inspected, and processes observed.

The overall VASP cybersecurity programme maturity level is then derived from the domain-level audits, noting that the overall level should reflect the lowest domain score (the weakest link principle[2]) for the domain that represents a critical capability for the protection of customer virtual assets (typically Control Implementation or Risk Management for VASP Cybersecurity Type 2 applicants).

1.2.1.5.3 Supervision Level Preliminary Recommendation

The supervision level preliminary recommendation applies only when the baseline audit identifies no Critical or High findings. In such cases, the maturity determination, combined with the findings aggregation and the risk ratings assigned to individual findings (Medium, Low, and Observation only), enables the auditor to form a preliminary recommendation on the appropriate supervision level. This preliminary recommendation is tested against the risk score calculation methodology in Section 3.4 and the supervision level criteria in Part 3 before being included in the final report.

Where the baseline audit identifies one or more Critical or High findings, the supervision level recommendation is not applicable because the licence application cannot proceed until those findings are remediated. In such cases, the auditor shall prepare a Gap and

[2] See Appendix B.3.3 Critical Domain Anchoring (Weakest Link) for commentary on the "weakest link" approach.

Remediation Report in accordance with Section 1.2.1.8, and the audit output is the Gap and Remediation Report rather than a licensing recommendation with supervision level assignment.

For baseline audits that qualify for a licensing recommendation (no Critical or High findings), the auditor should apply professional judgement where the maturity determination and the findings profile suggest different supervision levels. For example, a Defined maturity level would typically suggest standard supervision, but a pattern of Medium findings indicating systemic weakness might suggest enhanced supervision would be more appropriate. The auditor should document the rationale for the recommendation, giving appropriate weight to the nature and distribution of findings, the trajectory of the VASP's cybersecurity programme, and any compensating controls that mitigate identified weaknesses.

1.2.1.6 Quality Assurance Review

Before proceeding to the reporting phase, the auditor should conduct an internal quality assurance review of the outputs. This review should confirm that:

(1) All findings are supported by documented evidence; risk ratings are consistently applied in accordance with the five-tier framework in Section 2.1.
(2) The aggregation analysis has been performed and documented; the programme maturity determination is supported by domain-level evidence.
(3) The preliminary supervision level recommendation is consistent with the maturity determination and findings profile.
(4) Any areas where professional judgement has been exercised are clearly documented with supporting rationale.

1.2.1.7 Phase 4: Reporting

The baseline cybersecurity audit culminates in a structured findings report enabling VFSC licensing decisions. The report incorporates the individual findings from Phase 2, the aggregation analysis and programme maturity determination from Phase 3, and the supervision level recommendation. The report structure and content requirements are detailed in Appendix D of this document.

1.2.1.8 Gap and Remediation Report

Where the baseline cybersecurity audit identifies one or more findings rated as Critical or High, the auditor shall prepare a Gap and Remediation Report for the VASP applicant. This report serves as the roadmap for the applicant to achieve a cybersecurity posture sufficient for licensing.

The Gap and Remediation Report shall include:

1. A complete list of all Critical and High findings identified during the baseline audit, documented using the individual finding format specified in Appendix D.2.

2. For each Critical or High finding, a detailed remediation recommendation specifying the control improvements, process changes, or technical implementations required to address the deficiency.
3. Prioritisation guidance indicating which findings must be addressed first, particularly where dependencies exist between remediation actions.
4. Indicative timeframes for remediation, recognising that actual implementation timelines will depend on the applicant's resources and the complexity of the required changes.
5. Evidence requirements specifying what documentation, configurations, or test results the applicant must provide to demonstrate that each finding has been remediated.

1.2.1.8.1 Remediation Verification Process

Once the applicant has implemented the required remediation actions, the auditor shall verify that each Critical and High finding has been adequately addressed. The verification approach depends on the nature and severity of the findings:

1. For findings that can be verified through documentary evidence and configuration review, the auditor may conduct a targeted desk-based verification without a full re-audit.
2. For findings that require observing operational processes or testing technical controls, the auditor shall conduct on-site verification or remote testing, as appropriate.
3. Where the baseline audit identified multiple Critical findings or systemic failures across several control domains, the VFSC may require a full re-audit rather than targeted verification.

Upon successful verification that all Critical and High findings have been remediated, the auditor shall issue a Remediation Verification Letter to the VFSC confirming that the applicant's cybersecurity posture now meets the licensing threshold. The licence application may then proceed, with the original VASP cybersecurity baseline audit report, the Gap and Remediation Report, and the Remediation Verification Letter forming a complete audit package for VFSC consideration.

1.2.1.8.2 Medium and Low Findings at Baseline

Medium and Low findings identified during the VASP cybersecurity baseline audit do not prevent the grant of a licence. However, the Gap and Remediation Report should document all Medium and Low findings alongside the Critical and High findings. The applicant is expected to remediate Medium findings within 60–90 days and Low findings within 90–180 days following the grant of a licence. Progress on these findings will be monitored through the quarterly compliance reporting process (Section 1.2.2.1) and verified at the first annual audit (Section 1.2.3).

1.2.2 Continuous Monitoring and Improvement

Following the baseline cybersecurity audit and the grant of a VASP licence, ongoing assurance is maintained through a structured continuous monitoring and improvement framework. This framework assigns responsibilities across three parties: (1) the VASP licensee, (2) the appointed independent cybersecurity auditor, and (3) the VFSC, and operates at an intensity and frequency determined by the VASP's assigned supervision level (Part 3).

The framework is designed to identify emerging risks, verify remediation of prior findings, and provide early warning of control deterioration between formal cybersecurity audit cycles.

1.2.2.1 Summary of VASP Licensee Obligations (Auditor Reference)

The VASP licensee has primary responsibility for maintaining and improving the cybersecurity controls assessed during the baseline audit. The auditor should be familiar with the following VASP obligations, as they define what the auditor must verify during remediation reviews and annual audits:

(a) VASP Compliance Reporting. All VASP licensees must submit periodic compliance reports to the VFSC covering: the status of all open nonconformities and remediation progress; any cybersecurity incidents that occurred during the period, including root cause analysis and corrective actions; material changes to the licensed VASP scope, key management architecture, or custody arrangements; the results of any vulnerability scans or penetration tests; updates to the risk register; and confirmation that all cybersecurity policies and procedures remain current. Reporting frequency is determined by the supervision level: quarterly for standard supervision, monthly for enhanced supervision, and weekly or bi-weekly for intensive supervision.

(b) Incident Notification. Regardless of supervision level, VASP licensees must notify the VFSC of any material cybersecurity incident within 24 hours of detection. A material incident includes unauthorised access to customer virtual assets, compromise or suspected compromise of key material, disruption to critical custody or trading systems exceeding four hours, a data breach affecting customer personal information, or any event requiring activation of the incident response plan. A comprehensive incident report must follow within 14 days.

(c) Material Change Notification. VASP licensees must notify the VFSC prior to implementing any material change to their licensed environment that could directly or indirectly impact the security of key material. Material changes include changes to key management architecture, custody arrangements, technology platform, organisational structure affecting security roles, and geographic relocation of infrastructure or key material. The VFSC may require an interim audit or targeted audit of the changed controls before approving the material change.

The auditor's role in relation to these VASP obligations is set out in Section 1.2.2.2 below.

1.2.2.2 Independent Auditor Responsibilities

The independent cybersecurity auditor appointed in accordance with the VFSC Cybersecurity Guideline, issued under Virtual Asset Act 2025 - Section 59, read together with the annual independent audit obligation under Section 55, has ongoing responsibilities between annual audits. These responsibilities vary depending on the VASP's supervision level and are designed to provide the VFSC with independent assurance that the VASP's cybersecurity posture is maintained.

1.2.2.2.1 Remediation Verification

For all nonconformities identified during the baseline cybersecurity audit or most recent annual cybersecurity audit, the auditor must verify the effectiveness of corrective actions within the timeframes specified in the remediation plan.

1. For **Critical** findings, remediation evidence must be verified within **24** to **48 hours**.
2. For **High** findings, the auditor should conduct a targeted follow-up review within **30 days** to confirm that the corrective action plan has been implemented and is operating effectively.
3. For **Medium** findings, the auditor may accept documentary evidence of remediation at the next quarterly review point or during the annual audit, depending on the supervision level.
4. For **Low** findings, verification is typically deferred to the next annual audit. The auditor should maintain a remediation tracking log and report the status of all open findings to the VFSC at each quarterly review point.

1.2.2.2.2 Periodic Remediation Reviews (All Supervision Levels)

The frequency and depth of periodic remediation reviews between annual audits are determined by the VASP's assigned supervision level, consistent with the reporting frequency summary in Section 1.2.2.4.

Standard supervision. For VASPs under standard supervision, formal remediation verification is conducted at the annual audit. Between annual audits, the auditor should review the VASP's quarterly remediation reports submitted under Section 1.2.2.1 and maintain a remediation tracking log for any open findings. Where the quarterly compliance report discloses a material change, incident, or emerging risk, the auditor should assess whether the matter warrants earlier engagement or notification to the VFSC, even in the absence of a scheduled review.

Enhanced supervision. For VASPs under enhanced supervision, the auditor should conduct quarterly desk-based reviews of the VASP's cybersecurity compliance reports and remediation progress. These reviews do not constitute a full audit but provide an independent audit of whether the VASP is on track with its remediation commitments and whether any new risks have emerged that warrant attention. Following each quarterly review, the auditor should report to the VFSC in accordance with Section 1.2.2.2.3.

Intensive supervision. For VASPs under intensive supervision, the auditor should conduct monthly desk-based reviews of the VASP's cybersecurity compliance reports and remediation progress, with on-site verification as warranted by risk indicators or as directed by the VFSC. The increased review frequency reflects the heightened risk profile and the need for close monitoring of stabilisation actions and remediation evidence. Following each monthly review, the auditor should report to the VFSC in accordance with Section 1.2.2.2.3.

1.2.2.2.3 Auditor assurance letter to VFSC

The auditor's formal reporting to the VFSC between annual audits is determined by the VASP's assigned supervision level, consistent with the reporting frequency summary in Section 1.2.2.4.

Standard supervision. A formal auditor assurance letter is not required for VASPs under standard supervision. The auditor should, however, notify the VFSC promptly if any matter identified during review of the VASP's quarterly compliance reports under Section 1.2.2.2.2 warrants regulatory attention, including emerging risks, unremediated findings approaching or exceeding their remediation deadline, or indicators of control deterioration.

Enhanced supervision. The auditor should issue a quarterly assurance letter to the VFSC using the template provided in Appendix E. The assurance letter should summarise the findings from the quarterly desk-based reviews conducted under Section 1.2.2.2.2, the status of all open nonconformities and associated remediation plans, and any concerns regarding the VASP's cybersecurity posture or emerging risks that may warrant supervisory action.

Intensive supervision. The auditor should issue a quarterly assurance letter to the VFSC using the template provided in Appendix E, or at a higher frequency as directed by the VFSC. Given that VASPs under intensive supervision submit compliance reports on a weekly or bi-weekly basis (Section 1.2.2.1) and that the auditor conducts monthly remediation reviews (Section 1.2.2.2.2), each assurance letter should consolidate the findings from the intervening monthly reviews, provide a current audit of the VASP's cybersecurity posture, and highlight any matters requiring immediate supervisory attention. Where the VFSC directs a higher reporting frequency, the auditor should submit assurance letters at the intervals specified in the supervision plan.

1.2.2.2.4 Event-Driven Audit

The VFSC may direct the auditor to conduct a targeted audit in response to specific events, including:

(1) A material cybersecurity incident was reported by the VASP or another trusted third party.
(2) Intelligence received by the VFSC indicates a potential threat to the VASP's environment.

(3) A material change to the VASP's technology or custody arrangements, or information from the VASP's periodic reporting that raises concerns about the effectiveness of controls.

The scope of an event-driven audit is determined by the VFSC in consultation with the auditor and is limited to the specific area of concern. The cost of event-driven audits is borne by the VASP licensee.

1.2.2.3 VFSC Supervisory Activities (Summary Reference)

The VFSC maintains ongoing supervisory oversight of all licensed VASPs, with the level of engagement determined by the assigned supervision tier. Core VFSC activities relevant to the auditor include: reviewing auditor assurance letters issued under Section 1.2.2.2.3; directing event-driven audits under Section 1.2.2.2.4; conducting management meetings with VASPs; performing on-site inspections; and carrying out thematic reviews across the licensed population. The VFSC retains the final decision on supervision level assignments, taking into account the auditor's recommendation alongside any other relevant supervisory intelligence.

1.2.2.4 Continuous Improvement Expectations

The VFSC expects licensed VASPs to demonstrate continuous improvement in their cybersecurity posture over successive cybersecurity audit cycles. This expectation is reflected in the Programme Maturity Audit (Section 2.6), which tracks the VASP's progression across maturity levels.

A VASP that achieves *Developing* (Level 2) maturity at baseline is expected to demonstrate progress towards *Defined* (Level 3) by the first annual audit and to maintain or improve from that point forward. Stagnation in maturity level across successive audits, even where no new nonconformities are identified, may indicate an ineffective improvement programme and may influence supervision level decisions.

Conversely, demonstrated improvement in programme maturity, particularly when supported by evidence of investment in cybersecurity capabilities, adoption of enhanced controls beyond minimum requirements, and proactive engagement with emerging threats, provides a basis for de-escalation of supervision intensity.

Monitoring Activity	Standard Supervision	Enhanced Supervision	Intensive Supervision
VASP compliance reporting (1.2.2.1)	Quarterly	Monthly	Weekly or bi-weekly
Auditor remediation verification (1.2.2.2.2)	At annual audit	Quarterly desk-based review	Monthly verification with on-site as needed
Auditor assurance letter to VFSC (1.2.2.2.3)	Not required	Quarterly	Quarterly (or more frequent as directed)
VFSC management meetings	As needed (reactive)	Quarterly	Monthly or more frequently
On-site inspections	As warranted by risk	Targeted inspections as needed	On-site presence during critical operations
Formal cybersecurity audit	Annual	Semi-annual	Semi-annual (or more frequent as directed)

Incident notification to VFSC	Within 24 hours	Within 24 hours	Within 24 hours

1.2.3 Annual Cybersecurity Audit

In accordance with the VFSC Cybersecurity Guideline, issued under Virtual Asset Act 2025 Section 59, read together with the annual independent audit obligation under Section 55, all licensed VASPs must undergo an annual cybersecurity audit. Unlike the baseline audit, which evaluates control design and implementation, the VASP Cybersecurity Type 2 approach evaluates the operating effectiveness of controls over the preceding 12-month period.

The scope and intensity of the annual audit are risk-proportionate, determined by the VASP's assigned supervision level at the time the audit is commissioned. This risk-proportionate approach ensures that regulatory resources and VASP audit costs are directed where the risk is greatest, while still providing adequate assurance across the licensed population.

1.2.3.1 Annual Audit Tiers

The annual cybersecurity audit is conducted at one of three tiers of intensity, aligned directly with the supervision level categories established in Part 3 of this methodology. The assigned tier determines the breadth of control testing, the depth of evidence gathering, and the overall engagement effort. The table below provides a detailed comparison across all audit elements.

Audit Element	Tier 1: Focused Review (Standard Supervision)	Tier 2: Standard Audit (Enhanced Supervision)	Tier 3: Comprehensive Audit (Intensive Supervision)
Applicable Supervision Level	Standard (Risk Score 1–6)	Enhanced (Risk Score 7–15)	Intensive (Risk Score 16–25)
Assurance Approach	Type 2 (limited scope)	Type 2 (full scope)	Type 2 (full scope with extended testing procedures)
Control Testing Scope	Targeted: focus on previously identified nonconformities, key management and operational controls (CCSS V9), and any material changes since last audit	Comprehensive: all eight control domains tested; full CCSS V9 reaudit; all supplementary control areas (Part 4A)	Comprehensive plus extended: all control domains, all supplementary controls, and deep-dive into high-risk areas identified by the VFSC
Sampling Approach	Focused sampling: targeted selection based on risk areas and prior findings	Representative sampling: statistically valid samples across all control domains	Extended sampling: larger sample sizes with emphasis on areas of prior weakness; consideration of full-population testing for critical controls
Evidence Gathering Techniques	Primarily documentary review with targeted interviews; remote audit acceptable for majority of testing	Documentary review, interviews, and inspection of configurations; combination of remote and on-site audit	All four techniques required: documentary review, interviews, inspection, and observation; on-site

			presence required for critical control testing
Key Management Deep-Dive	Confirm continued compliance with CCSS V9 requirements at the level achieved; verify remediation of prior findings	Full CCSS V9 reaudit across all applicable aspects; key ceremony observation if conducted during audit period	Full CCSS V9 reaudit with extended testing procedures including live key ceremony observation, verification of key share integrity, and testing of key compromise recovery protocol
Supplementary Controls (Part 4A)	Not routinely included unless prior findings exist or material changes reported	All supplementary control areas assessed	All supplementary control areas assessed with extended testing procedures
Prior Finding Follow-Up	Verify closure of all prior Critical and High findings; sample-test Medium and Low closures	Verify closure of all prior findings; test effectiveness of corrective actions for all High and Critical findings	Verify closure of all prior findings; independently re-test all controls associated with prior Critical and High findings to confirm sustained effectiveness
Programme Maturity Audit	Update maturity audit; confirm maintenance of or improvement from prior level	Full maturity reaudit across all five domains per Section 2.6	Full maturity reaudit with independent benchmarking against industry peers and international standards
Typical Duration	2–3 weeks	4–6 weeks	6–8 weeks
Reporting	Focused findings report covering scope areas tested; updated risk rating and supervision recommendation	Full findings report per Appendix D; comprehensive risk rating and supervision recommendation	Full findings report with supplementary analysis; detailed remediation roadmap; recommendation on continued licensing suitability

1.2.3.1.1 Risk-Proportionate Scope Determination

The tier assignments above reflect a core regulatory principle: the depth and cost of independent assurance should be proportionate to the risk the VASP poses to customers and the broader financial system. A VASP that has consistently demonstrated strong controls, resolved all prior findings, and maintained a stable operating environment should not be subjected to the same audit intensity as one that has experienced incidents or failed to remediate identified weaknesses. This proportionate approach incentivises good practice by reducing the regulatory burden on well-managed VASPs while concentrating supervisory and audit resources on those that pose the greatest risk.

1.2.3.2 First Annual Audit Considerations

The first annual audit following the baseline cybersecurity audit represents a critical transition point. Where the baseline audit evaluated control design and implementation readiness only, the first annual audit must establish whether those controls have operated effectively over the intervening period (the previous 12 months of operation). The auditor should give particular attention to:

(1) The effectiveness of corrective actions for all nonconformities identified during the baseline audit.
(2) The VASP's actual operational performance, including any incidents, near-misses, or control failures that occurred during the first year of licensed operation.
(3) The VASP's progress against the continuous improvement expectations set out in Section 1.2.2.

For all newly licensed VASPs, the first annual audit should be conducted at a minimum Tier 2 (Standard Audit) intensity, regardless of the assigned supervision level, to provide the VFSC with a comprehensive baseline of operational effectiveness, covering the 12 months since the baseline cybersecurity audit. Subsequent annual audits may then be conducted at the tier corresponding to the assigned supervision level.

1.2.3.3 Supervision Level Reaudit

Each annual audit concludes with a recommendation regarding the VASP's supervision level for the following 12 months. The auditor should assess whether the current supervision level remains appropriate in light of the audit findings, the VASP's remediation track record, changes to the risk profile, and the trajectory of programme maturity. The recommendation should be supported by reference to the risk score calculation methodology in Section 3.4 and the escalation and de-escalation criteria established in Part 3. Where the auditor recommends a change in supervision level, the recommendation must include a clear rationale supported by specific audit evidence. The VFSC retains the final decision on supervision level assignment, taking into account the auditor's recommendation alongside any other relevant supervisory intelligence.

1.2.3.4 Annual Audit Cycle Timeline

The completed annual audit report must be submitted to the VFSC Commissioner within three months after the end of the VASP's financial year, in accordance with Virtual Asset Act 2025 Sections 55(1) and 63(2). Where the VFSC Cybersecurity Guideline specifies a different timeline for the cybersecurity component, the auditor should plan accordingly to ensure both statutory and guideline deadlines are met.

The cybersecurity audit report must be submitted to the VFSC within 30 days of fieldwork completion. The VFSC should review the report and confirm the supervision level assignment within 30 days of receipt.

For VASPs under intensive supervision, the VFSC may require semi-annual formal audits in addition to the quarterly auditor reviews described in Section 1.2.2. Where semi-annual audits are required, each should be conducted at Tier 3 (Comprehensive Audit) intensity. The decision to require semi-annual audits rests with the VFSC and is communicated to the VASP and auditor through the supervision plan.

1.2.3.5 De-Escalation Through Demonstrated Improvement

A VASP may be de-escalated from a higher to a lower supervision level and, consequently, from a more intensive to a less intensive annual audit tier, provided the

VASP demonstrates sustained improvement over successive audit cycles. Consistent with the de-escalation criteria established in Part 3, this requires:

1. Sustained remediation of all High and Critical findings.
2. Two consecutive satisfactory audit outcomes (Strong or Satisfactory overall audit).
3. Demonstrated operational stability over a minimum of 12 months with no material incidents.
4. A positive track record on regulatory reporting, including timely and accurate quarterly submissions.
5. Independent verification of control improvements by the auditor.
6. Demonstrable improvement in programme maturity level as assessed under Section 2.6.

De-escalation is not automatic; it requires a formal recommendation from the cybersecurity auditor and approval by the VFSC. A VASP that is de-escalated remains subject to the monitoring and reporting requirements appropriate to its new supervision tier.

1.2.3.6 Relationship Between Baseline and Annual Audits

The annual cybersecurity audit builds on the baseline cybersecurity audit rather than replacing it.

The baseline audit report remains a key reference for the cybersecurity auditor, establishing the control environment as of the point of licensing.

Each annual cybersecurity audit should assess changes from the baseline position, track the resolution of findings over time, and evaluate whether the overall security posture has strengthened, remained stable, or deteriorated.

The cybersecurity auditor should maintain a cumulative findings register that tracks each nonconformity from initial identification through to verified closure, enabling both the auditor and the VFSC to identify patterns such as recurring findings in the same control domain, protracted remediation timelines, or findings that are closed and subsequently reopened. These patterns inform the aggregation escalation framework described in Section 2.2.3 and the overall supervision level recommendation.

Part 2: Five-Tier Risk Rating Framework

This Part employs two complementary domain classification systems that serve distinct purposes within the audit methodology. The auditor must clearly distinguish between these two systems when applying the frameworks described in Sections 2.2 through 2.6.

Eight Control Domains (defined in Section 2.4) categorise individual audit findings by technical and operational control area. These domains are used throughout the nonconformity classification (Section 2.2), the aggregation escalation framework (Section 2.2.3), the finding categorisation process (Section 2.4), and the individual finding documentation format (Appendix D.2).

The eight control domains are: (1) Key Management, (2) Wallet Security, (3) Access Control, (4) Network and Infrastructure Security, (5) Security Operations, (6) Business Continuity and Disaster Recovery, (7) Third-Party Risk Management, and (8) Governance and Compliance.

Five Maturity Domains (defined in Section 2.6) assess the overall capability and maturity of the VASP's cybersecurity programme. These domains are used in the programme maturity audit (Section 2.6) and the critical domain aggregation principle (Appendix B). The five maturity domains are: (1) Governance and Leadership, (2) Risk Management, (3) Control Implementation, (4) Monitoring and Measurement, and (5) Continuous Improvement.

These two systems intersect operationally: individual findings are categorised into the eight control domains during fieldwork and aggregation analysis, and the results of that analysis inform the five-domain programme maturity audit, which determines the supervision level recommendation. Where this methodology refers to "control domain" or "control domains," it means the eight-domain system. Where it refers to "maturity domain" or "maturity domains," it means the five-maturity-domain system.

2.1 Rating Definitions and Criteria

The VFSC VASP cybersecurity audit methodology adopts a five-tier risk rating framework aligned with international IT audit standards, NIST guidance, and financial services regulatory examination practices:

Rating	Definition	Characteristics	Remediation
Critical	Immediate threat to client assets requiring emergency response	Complete system compromise risk; severe service disruption; fundamental breach of Vanuatu Virtual Assets Services Providers Act No. 3 of 2025	Baseline: Licence cannot be granted. Post-licence: Intensive supervision

High	Significant weakness with substantial risk	Could result in elevated privileges or significant asset loss; material non-compliance with Vanuatu Virtual Assets Services Providers Act No. 3 of 2025 - Section 23	Baseline: Licence cannot be granted. Post-licence: Enhanced or intensive supervision
Medium	Moderate weakness requiring planned mitigation	Requires attacker manipulation; provides limited access if exploited; procedural deficiencies	60-90 days; standard licensing with monitoring
Low	Minor weakness with limited impact potential	Minimal exploitation probability; minor procedural issues; control enhancement opportunities	90-180 days; tracked through standard supervision
Observation	Best practice improvement recommendation	No immediate risk; enhancement suggestions to exceed minimum requirements	Next audit cycle; no mandatory action

2.2 Nonconformity Classification and Risk Rating Mapping

To provide auditors with a practical, evidence-based method for determining the risk level of VASP applicants, this methodology adopts a nonconformity classification framework drawn from established ISO audit practice.

In management system auditing, findings are classified as either major or minor nonconformities based on their impact on the system's capability to achieve its intended outcomes.

This section defines these classifications within the VASP cybersecurity audit context, maps them to the five-tier risk rating framework established in Section 2.1, and introduces an aggregation and escalation framework to address scenarios in which the volume or pattern of minor nonconformities indicates systemic failure warranting a higher risk classification.

2.2.1 Definitions

2.2.1.1 Major Nonconformity

A nonconformity that affects the capability of the VASP's cybersecurity programme to achieve its intended outcomes, specifically, the secure custody and management of

customer virtual assets. Derived from ISO/IEC 17021-1:2015 Clause 3.12 and adapted for the VASP licensing context, a major nonconformity arises when:

(a) There is significant doubt that effective process control is in place, or that customer assets will be adequately protected.
(b) A required control element is entirely absent (for example, no key ceremony procedures, no incident response plan, no access control policy).
(c) A control exists in policy but has failed to implement it completely or implementation, rendering it ineffective.
(d) A number of minor nonconformities associated with the same requirement or control domain collectively demonstrate systemic failure (see Section 2.2.3 Aggregation Escalation Framework).

2.2.1.2 Minor Nonconformity

A nonconformity that does not affect the overall capability of the VASP's cybersecurity programme to achieve its intended outcomes. Derived from ISO/IEC 17021-1:2015 Clause 3.13, a minor nonconformity involves:

(a) A single, isolated lapse that does not compromise overall system effectiveness.
(b) A documentation deficiency, such as missing version control, outdated policy details, or incomplete records that do not indicate broader process failure.
(c) A timing deviation where a required activity was performed but not within the prescribed schedule.
(d) An individual record gap, such as one missing training record or one user account not promptly disabled following role change, where no systemic pattern is evident.

2.2.1.3 Observation (Opportunity for Improvement)

An observation is not a nonconformity. It identifies an area where the VASP meets the applicable baseline requirement but could benefit from enhancement to exceed minimum standards or adopt industry best practice. Observations carry no mandatory remediation obligation and are tracked for consideration at the next audit cycle.

2.2.2 Nonconformity-to-Risk Rating Mapping

The following table maps nonconformity classifications to the five-tier risk rating framework. Each finding recorded during the audit should be classified as a nonconformity (major or minor) or an observation, with the corresponding risk rating determined according to the criteria below. Where a finding falls at the boundary between two classifications, the auditor should apply professional judgement and consider the potential impact on the security of customer virtual assets.

NC Classification	Risk Rating	Criteria	VASP-Specific Indicators (non-exhaustive)	Licensing Implication
Major Nonconformity	**Critical**	Complete absence of a critical custody control; active	No key management procedures; signing	Baseline: Licence cannot be granted until resolved.

(Immediate asset risk)		vulnerability enabling key compromise; systemic failure directly threatening customer funds	keys stored in plaintext; no multi-signature enforcement on custody wallets; active exploitation in progress	Post-licence: Intensive supervision; immediate remediation required.
Major Nonconformity (Significant weakness)	**High**	Required control absent or fundamentally ineffective; significant doubt about process control capability; systemic failure in a control domain	Incident response plan exists but never tested and contacts outdated; key ceremony procedures undocumented; access reviews not performed despite policy requirement; multi-sig threshold below documented minimum	Baseline: Licensing not recommended until resolved. Post-licence: Enhanced or intensive supervision; immediate remediation required.
Minor Nonconformity (Planned mitigation)	**Medium**	Control exists but with implementation gaps; partial compliance that limits exposure but requires improvement	Key ceremony performed but incomplete audit trail; penetration testing conducted but remediation of medium findings overdue; backup procedures documented but recovery not tested within required timeframe	Standard licensing with monitoring (60–90 days)
Minor Nonconformity (Limited impact)	**Low**	Isolated procedural lapse; documentation hygiene issue; individual record gap with no systemic pattern	Single user account not disabled within 24-hour policy window; one training record missing from otherwise complete register; minor version control gap in policy document	Tracked through standard supervision (90–180 days)
Observation (No nonconformity)	**Observation**	Control meets baseline requirements; recommendation to exceed minimum standard or adopt industry best practice	CCSS V9 Level II achieved; recommendation to pursue Level III; current threat intelligence feeds adequate but could benefit from additional sources; manual process could be automated for efficiency	Next audit cycle; no mandatory action

2.2.3 Aggregation Escalation Framework

A well-established principle in management system auditing holds that an accumulation of minor nonconformities can evidence systemic failure and thereby warrant reclassification as a major nonconformity. ISO/IEC 17021-1:2015 Clause 3.12 Note 1 explicitly states that “a number of minor nonconformities associated with the same requirement or issue could demonstrate a systemic failure and thus constitute a major nonconformity.” This principle is reinforced by ISACA Standard S12, which directs auditors to consider “the cumulative effect of minor control deficiencies or weaknesses” when assessing overall materiality, and by ISA 450, which requires auditors to evaluate whether uncorrected misstatements are material “individually or in aggregate.”

2.2.3.1 Escalation Trigger Patterns

The auditor should evaluate whether minor nonconformities exhibit any of the following patterns, each of which may indicate systemic rather than isolated failure:

(a) Same Clause or Requirement - Multiple minor nonconformities against the same standard clause or control requirement indicate systemic non-compliance with that requirement.
(b) Same Control Domain - Concentrated minor nonconformities within one of the eight control domains (as defined in Section 2.4) suggest a governance or management failure specific to that area.
(c) Common Root Cause - Minor nonconformities stemming from a shared underlying weakness (for example, inadequate training, under-resourcing, or absent management oversight) indicate a systemic rather than an isolated problem, regardless of which control domains are affected.
(d) Repeat Findings - Any minor nonconformity identified in a prior audit and unresolved at the current audit indicates inadequate corrective action processes and should be escalated.

2.2.3.2 Aggregation Escalation Thresholds

The following thresholds provide structured guidance for auditors. References to “control domain” or “control domains” in this table refer to the eight control domains defined in Section 2.4: (1) Key Management, (2) Wallet Security, (3) Access Control, (4) Network and Infrastructure Security, (5) Security Operations, (6) Business Continuity and Disaster Recovery, (7) Third-Party Risk Management, and (8) Governance and Compliance. These thresholds are not explicit rules; professional judgement must be applied in every case, taking into account the nature of the VASP’s operations, the assets under custody, and the potential impact on customers.

Escalation Scenario	Threshold	Escalated Classification	Escalated Risk Rating	Rationale
Concentration in single control domain	3 or more minor NCs within any single control domain (see Section 2.4 for the eight control domains)	Major Nonconformity	High	Pattern indicates systemic control failure within the domain per ISO/IEC 17021-1 Clause 3.12 Note 1

Concentration in Key Management domain	4 or more minor NCs within the Key Management domain (CCSS V9 1.01–1.06)	Major Nonconformity	**High (consider Critical)**	Key management is the highest-risk domain for custody operations; even minor gaps compound to create material key compromise risk
Volume across multiple domains	8 or more minor NCs distributed across 3 or more control domains	Overall audit escalated by one level	Overall rating worsened by one tier	Volume indicates broader programme immaturity regardless of individual finding severity, consistent with ISACA S12 aggregation principle
Repeat or unresolved findings	Any minor NC from a prior audit that remains unresolved	Escalate individual finding by one severity level	**Low → Medium; Medium → High**	Unresolved findings demonstrate inadequate corrective action processes, a management system failure in itself
Common root cause identified	3 or more minor NCs sharing a demonstrably common root cause	Classify as single Major Nonconformity	**High or Critical (based on impact)**	Common root cause indicates systemic weakness; individual findings are symptoms rather than distinct problems
Critical domain with no controls	Any control domain with zero documented controls where controls are required	Major Nonconformity	**Critical**	Complete absence of controls in a required domain constitutes fundamental inability to manage associated risks

2.2.3.3 Application of Professional Judgement

The aggregation thresholds above provide a structured framework, but they do not replace professional judgement. The auditor must consider the totality of evidence when determining whether an accumulation of minor nonconformities constitutes a major nonconformity. Factors that should inform this judgement include:

1. The nature and value of virtual assets under custody.
2. The sophistication of the threat landscape facing the applicant's specific service model.
3. Whether the applicant demonstrates awareness of the gaps and has initiated remediation.
4. The maturity level of the overall programme (as assessed under Section 2.6).
5. Any compensating controls that may partially mitigate identified weaknesses.

The auditor should document the rationale for any aggregation-escalation decision in the findings report, including the specific pattern or threshold that triggered the escalation and the evidence supporting the determination.

2.2.3.4 Recording Nonconformities During Fieldwork

During fieldwork, the auditor should record each nonconformity using the individual finding documentation format specified in Appendix D.2, classifying each as a major nonconformity, minor nonconformity, or observation at the point of identification.

Upon completion of fieldwork, the auditor should review all findings collectively to determine whether the aggregation escalation thresholds in Section 2.2.3 are triggered. Where escalation applies, the auditor should document the aggregation analysis as a separate finding or as a note within the executive summary, clearly stating: the minor nonconformities that form the basis of escalation; the escalation pattern identified (same domain, common root cause, volume, or repeat finding); and the resulting reclassification and its effect on the overall audit recommendation.

2.3 Likelihood and Impact Audit

The nonconformity to risk mapping classification framework in Section 2.2.2 is the primary method for assigning risk ratings to nonconformities and observations during the cybersecurity audit: each finding is classified as a major nonconformity, minor nonconformity, or observation, and the corresponding risk rating is determined.

The likelihood and impact matrix below serves as a validation and calibration tool. The auditor should use the nonconformity classification as the starting point for the risk rating and then confirm the rating against the likelihood and impact matrix. Where the matrix produces a materially different result from the nonconformity classification, the auditor should adjust the rating with documented justification, giving appropriate weight to the specific circumstances of the finding and the nature of the VASP's operations.

Risk ratings derive from a 5x5 matrix combining likelihood and impact audits. Likelihood is assessed on a scale from Rare (1) to Almost Certain (5), considering adversary capability, motivation, and control effectiveness. Impact is assessed from Negligible (1) to Catastrophic (5), considering potential loss of client assets as a percentage of assets under custody (AUC), service availability, regulatory consequences, and reputational damage.

2.3.1 Risk Determination Matrix

Likelihood / Impact	Negligible	Minor	Serious	Severe	Catastrophic
Almost Certain	Medium	High	Critical	Critical	Critical
Likely	Low	Medium	High	Critical	Critical
Possible	Low	Medium	Medium	High	Critical
Unlikely	Observation	Low	Medium	Medium	High
Rare	Observation	Low	Low	Medium	Medium

2.4 Finding Categorisation by Control Domain

Findings are grouped into eight control domains aligning with CCSS V9 aspects and the VFSC evidence request questionnaire structure:

(1) **Key Management** (CCSS V9 1.01-1.06) covering generation, storage, transmission, backup, usage, compromise protocol, and grant/revoke policies.
(2) **Wallet Security** addressing hot/cold/warm architecture, multi-signer mechanism configuration, and address whitelisting.
(3) **Access Control** for authentication, privileged access management, and segregation of duties.
(4) **Network and Infrastructure Security** for perimeter protection, segmentation, and DDoS mitigation.
(5) **Security Operations** covering monitoring, incident detection, and vulnerability management.
(6) **Business Continuity and Disaster Recovery** for backup procedures, recovery testing, and geographic distribution.
(7) **Third-Party Risk Management** addressing sub-custodian audit, smart contract audits, and vendor oversight.
(8) **Governance and Compliance** for policies, training, regulatory reporting, and audit trails.

2.5 Aggregation to Overall Audit

Individual findings aggregate to an overall audit recommendation using the following framework. The application of these ratings differs between baseline audits and annual audits:

Baseline Audits: For baseline cybersecurity audits of new licence applicants, only a rating of Strong (1) qualifies for an unconditional licensing recommendation. Ratings of Satisfactory (2) through Critically Deficient (5) all indicate the presence of Critical or High findings, which must be remediated before a licence can be granted in accordance with the licensing threshold policy (Section 1.2.1) and the Gap and Remediation Report process (Section 1.2.1.8).

Annual Audits: For annual cybersecurity audits of licensed VASPs, the “Licensing Implication” column applies as stated. Ratings of Satisfactory through Needs Improvement result in continued licensing with appropriate supervision rather than licence revocation, recognising that a licensee’s cybersecurity posture may deteriorate and the supervisory framework addresses such deterioration through remediation and oversight.

Overall Rating	Threshold	Licensing Implication
Strong (1)	No Critical or High findings; fewer than 3 Medium findings; effective controls	Recommend licensing; standard supervision

Satisfactory (2)	No Critical findings; 1–2 High findings with remediation plans; adequate controls (annual audit only; not achievable at baseline)	Conditional licensing; enhanced supervision - annual audits only
Needs Improvement (3)	No Critical findings; 3+ High findings OR pattern of Medium findings indicating systemic weakness (annual audit only; not achievable at baseline)	Conditional licensing; enhanced supervision - annual audits only
Deficient (4)	1+ Critical findings OR 5+ unaddressed High findings; material control gaps	Conditional licensing; intense supervision - annual audits only
Critically Deficient (5)	Multiple Critical findings; fundamental inability to safeguard client assets	Conditional licensing; intense supervision - annual audits only

2.6 Programme Maturity Audit

In addition to individual control findings, auditors should evaluate the overall maturity of the VASP's cybersecurity programme. This provides context for the findings and informs recommendations on supervision intensity. The maturity audit uses a five-level model aligned with NIST CSF Implementation Tiers and industry capability maturity frameworks:

Maturity Level	Definition	Characteristics
1. Initial	Ad hoc and reactive; security activities are unstructured	Few or no documented policies; controls are inconsistent and person-dependent; no formal risk management process; security is treated as an IT function only
2. Developing	Policies emerging but implementation inconsistent	Basic policies documented but not comprehensive; some controls implemented but not uniformly; management awareness exists but commitment varies; reactive incident handling
3. Defined	Standardised processes documented and communicated	Comprehensive policy framework approved by management; controls implemented consistently across organisation; formal

		risk audit conducted; roles and responsibilities clearly assigned; training programme established
4. Managed	Processes measured and controlled; performance monitored	Security metrics collected and reported to management; control effectiveness regularly tested; incident response exercised through drills; continuous monitoring implemented; third-party audits conducted regularly
5. Optimised	Continuous improvement embedded; industry-leading practices	Proactive third-party supplied threat intelligence integration; automated security controls; quantitative risk management; security embedded in business processes; external certifications maintained (ISO 27001, CCSS V9); regular benchmarking against peers

2.6.1 Maturity Audit Domains

Auditors should evaluate maturity across five domains: (1) Governance and Leadership, examining executive accountability, policy framework, and resource allocation; (2) Risk Management, assessing risk identification, audit methodology, and treatment processes; (3) Control Implementation, reviewing technical and operational control deployment; (4) Monitoring and Measurement, evaluating metrics, logging, and performance tracking; and (5) Continuous Improvement, examining lessons learned integration, audit follow-up, and programme evolution.

2.6.2 Maturity and Supervision Correlation

Maturity Level	Typical Supervision	Rationale
4-5 (Managed/Optimised)	Standard	Mature programmes with demonstrated effectiveness require less intensive oversight
3 (Defined)	Standard to Enhanced	Programme structure exists but effectiveness may be untested, monitoring appropriate
2 (Developing)	Enhanced	Significant gaps likely; closer regulatory

		engagement needed to ensure progress
1 (Initial)	Intensive or Defer	Fundamental programme development required; licensing may be premature

Part 3: Supervision Level Categories

Drawing on risk-based supervisory approaches commonly used by financial regulators, VFSC could adopt a three-tier supervision framework for VASPs. The tiers would scale supervisory intensity according to the VASP's inherent risk profile, control maturity, audit outcomes, and supervisory history, while remaining consistent with VFSC's existing statutory powers and published guidance.

3.1 Standard Supervision (baseline/lower risk)

Applied to VASPs demonstrating a mature cybersecurity control environment and no indicators of elevated supervisory concern.

Supervisory approach (baseline + risk-triggered):

1. Quarterly cybersecurity reporting in accordance with the Vanuatu Virtual Assets Services Providers Act No. 3 of 2025 - Section 54.
2. Annual independent cybersecurity audit report in accordance with the Vanuatu Virtual Assets Services Providers Act No. 3 of 2025 - Section 55
3. Annual independent cybersecurity testing/assurance consistent with VFSC cybersecurity requirements (e.g., periodic vulnerability audit/penetration test at least annually).
4. Desk-based monitoring, thematic reviews, and follow-up engagement triggered by incident reporting, credible intelligence, complaints, or emerging risks.

Indicative assignment factors (non-exhaustive):

1. Overall assurance results support a satisfactory or strong cybersecurity posture (using the VFSC VASP cybersecurity audit methodology's risk scoring/rating, if adopted).
2. No unresolved issues that present an immediate risk to customer assets or regulatory objectives.
3. Remediation (where needed) is timely and verifiable.
4. No material compliance breaches or repeated supervisory concerns.
5. Evidence of adequate cybersecurity controls, governance, and operational capability for the scale of activity.
6. VFSC VASP cybersecurity audit methodology maturity is at least *Managed/Optimised* or *Defined,* as defined by this methodology's maturity model.

3.2 Enhanced Supervision (elevated risk/remediation focus)

Applied to VASPs with elevated risk indicators or assurance results showing meaningful cybersecurity weaknesses requiring closer regulatory engagement and structured remediation tracking.

Supervisory approach (scaled-up engagement):

1. Baseline obligations under Vanuatu Virtual Assets Services Providers Act No. 3 of 2025 - Section 54 and Section 55, plus more frequent progress reporting focused on remediation actions and control improvements.
2. More frequent cybersecurity assurance where risk warrants (e.g., additional independent testing, targeted control validation, or expanded scope), consistent with the VFSC VASP cybersecurity audit methodology's risk-based approach.
3. Scheduled management engagement (e.g., quarterly meetings) to review remediation status, governance, and risk controls.
4. Targeted on-site inspections where appropriate, using VFSC's inspection powers.
5. Licence conditions specifying remediation milestones, timelines, and evidence requirements, using VFSC's powers to impose/vary conditions.
6. Enhanced monitoring expectations proportionate to risk (e.g., transaction monitoring uplift, targeted control testing, or independent verification of specific fixes where justified).

Indicative assignment factors (non-exhaustive):

1. One or more high-severity issues identified with credible remediation underway, or a pattern of moderate issues suggesting systemic weakness.
2. New licensees or firms undergoing significant change (e.g., rapid scaling, new products, new geographies, material outsourcing).
3. Credible intelligence, complaints, or supervisory findings indicating elevated compliance or financial crime risk.
4. Prior supervisory history suggests heightened risk or slower remediation performance.
5. VFSC VASP cybersecurity audit methodology maturity is at least *Developing,* as defined by this methodology's maturity model.

3.3 Intensive Supervision (serious risk/potential restrictions)

Applied to VASPs with serious deficiencies, significant compliance breaches, or operational events indicating immediate risk to client assets, market integrity, or AML/CFT objectives.

Supervisory approach (high-intensity, protective):

1. Close supervisory engagement with frequent reporting (e.g., weekly/bi-weekly) focused on stabilisation actions, remediation evidence, and risk containment.
2. Increased use of on-site supervisory activity during critical periods where needed.
3. Use of licence conditions or directions (where available) to impose risk-mitigations such as restrictions on new onboarding, transaction limits, product/geography constraints, or enhanced custody/controls until remediation is proven effective.

4. Mandatory independent assurance/verification of remediation outcomes for high-impact weaknesses (e.g., third-party validation of key controls and security fixes).
5. Escalation to enforcement actions (where applicable) if the VASP licensee fails to remediate or if risks remain unacceptably high.

Indicative assignment factors (non-exhaustive):

1. Any critical weakness indicating immediate and material risk to client assets or regulatory objectives (with escalation presumed unless promptly contained).
2. Multiple high-severity issues are not being remediated within agreed timelines, or failure to meet Enhanced Supervision milestones.
3. Material client asset loss, serious incident, or credible near-miss indicating a breakdown in controls.
4. Significant regulatory breach requiring notification and/or supervisory intervention.
5. Credible intelligence indicating criminal activity, sanctions evasion exposure, or systemic AML/CFT control failures.
6. VFSC VASP cybersecurity audit methodology maturity is at *Initial,* as defined by this methodology's maturity model.

3.4 Risk Score Calculation and Tier Movement

Tier placement considers impact factors (what harm could occur) and probability factors (likelihood of harm). Risk Score = Impact Score (1-5) × Probability Score (1-5) = Risk Score (1-25). Scores of 1-6 result in Standard supervision, 7-15 in Enhanced supervision, and 16-25 in Intensive supervision.

Risk Score	Supervision Tier
1-6	Standard
7-15	Enhanced
16-25	Intensive

Escalation triggers include a cybersecurity incident affecting client assets, a critical finding in a periodic audit, a pattern of recurring findings, intelligence indicating regulatory concern, significant business expansion without prior approval, and a material breach of licence conditions.

De-escalation criteria include sustained remediation of all High/Critical findings, two consecutive satisfactory audits, demonstrated operational stability over 12+ months, no material incidents during the supervision period, a positive track record in regulatory reporting, independent verification of control improvements, and demonstrable improvement in programme maturity level.

3.5 Deriving the Supervision Recommendation

The VFSC VASP cybersecurity audit methodology provides three inputs to the supervision level decision:

(1) The overall audit rating (Section 2.5), which maps to supervision levels through the criteria in Sections 3.1–3.3;
(2) The programme maturity audit (Section 2.6), which maps to supervision levels through the correlation table in Section 2.6; and
(3) The Risk Score calculation (Section 3.4), which maps to supervision tiers through the risk score thresholds. To ensure these three inputs produce a single, coherent supervision recommendation, the Risk Score serves as the integrating mechanism.

The Impact Score (1–5) is derived from the overall audit rating: Strong = 1, Satisfactory = 2, Needs Improvement = 3, Deficient = 4, Critically Deficient = 5. The Probability Score (1–5) is derived from the programme maturity audit: Optimised = 1, Managed = 2, Defined = 3, Developing = 4, Initial = 5. The Risk Score is calculated as Impact Score × Probability Score, producing a value between 1 and 25 that integrates both audit streams into a single number for tier placement.

Where the Risk Score produces a supervision level that differs from the level suggested by either the overall audit rating or the programme maturity audit considered independently, the auditor should adopt the highest (most conservative) supervision level indicated by any of the three inputs, consistent with the “weakest link” principle adopted for programme maturity aggregation in Appendix B. The auditor must document the rationale for the final supervision recommendation in the findings report, including the individual scores for each input and an explanation of any divergence between them.

3.5.1 Worked Examples

The following worked examples demonstrate how the supervision recommendation is derived by integrating the three audit inputs. Each example shows the step-by-step calculation process and explains the auditor’s reasoning.

Example 1: Well-Managed VASP - Standard Supervision

Scenario: CryptoVault Ltd is a licensed cryptocurrency exchange that has been operating for 18 months. The annual cybersecurity audit has been completed with the following results: Overall Audit Rating of Strong; Programme Maturity of Managed (Level 4).

Calculation: Impact Score = 1 (Strong). Probability Score = 2 (Managed). Risk Score = 1 × 2 = 2.

Determination: The Risk Score of 2 falls within the 1-6 range for Standard Supervision. The Strong overall audit rating aligns with standard supervision per Section 3.1. The Managed maturity level (Level 4) maps to Standard supervision per the correlation table in Section 2.6.2. All three inputs converge; no adjustment is required.

Recommendation: Standard Supervision. Rationale: Strong audit outcome with a mature programme demonstrates sustained effective cybersecurity controls.

Example 2: Newly Licensed VASP with Minor Weaknesses - Enhanced Supervision

Scenario: DigiAsset Holdings received its licence 12 months ago. The first annual audit reveals an Overall Audit Rating of Satisfactory (with two High findings under remediation) and Programme Maturity of Defined (Level 3).

Calculation: Impact Score = 2 (Satisfactory). Probability Score = 3 (Defined). Risk Score = 2 × 3 = 6.

Determination: The Risk Score of 6 falls at the upper boundary of the 1–6 range for Standard Supervision. However, the Satisfactory rating with High findings under remediation indicates Enhanced supervision per Section 3.2 ("one or more high-severity issues identified with credible remediation underway"). The Defined maturity level maps to "Standard to Enhanced" per Section 2.6.2. The inputs diverge slightly; the auditor applies the conservative approach.

Recommendation: Enhanced Supervision. Rationale: Although the Risk Score of 6 falls within the Standard range, the presence of two High findings requiring remediation warrants closer regulatory engagement until remediation is verified.

Example 3: Significant Weaknesses Identified - Enhanced Supervision

Scenario: BlockChain Trust is an established custody provider whose annual audit identifies a pattern of Medium findings across multiple control domains, indicating systemic weaknesses. Overall Audit Rating: Needs Improvement (no Critical findings; three High findings; eight Medium findings triggering aggregation escalation). Programme Maturity: Developing (Level 2).

Calculation: Impact Score = 3 (Needs Improvement). Probability Score = 4 (Developing). Risk Score = 3 × 4 = 12.

Determination: The Risk Score of 12 falls within the 7–15 range for Enhanced Supervision. The Needs Improvement overall audit rating maps to "Conditional licensing; enhanced supervision" per Section 2.5. The Developing maturity level maps to Enhanced supervision per Section 2.6.2. All three inputs converge on Enhanced Supervision.

Recommendation: Enhanced Supervision. Rationale: The pattern of findings across multiple control domains indicates systemic weaknesses in programme execution. Monthly compliance reporting and quarterly management meetings with the VFSC are required. The VASP must demonstrate progress towards Defined (Level 3) maturity by the next annual audit.

Example 4: Critical Findings Post-Licence - Intensive Supervision

Scenario: VirtualWallet Services experienced a security incident six months ago that was contained without customer asset loss. The subsequent audit has identified Critical weaknesses in the key management architecture. Overall Audit Rating: Deficient (one

Critical finding regarding key ceremony procedures; three High findings). Programme Maturity: Developing (Level 2), with Control Implementation as the critical domain floor.

Calculation: Impact Score = 4 (Deficient). Probability Score = 4 (Developing). Risk Score = 4 × 4 = 16.

Determination: The Risk Score of 16 falls at the lower boundary of the 16–25 range for Intensive Supervision. The Deficient overall audit rating triggers Intensive supervision per Section 3.3 (“any critical weakness indicating immediate and material risk to client assets”). The Developing maturity level maps to Enhanced supervision per Section 2.6.2. The inputs diverge between the maturity audit (Enhanced) and the other inputs (Intensive). Following the methodology’s requirement to adopt the most conservative level, Intensive Supervision is recommended.

Recommendation: Intensive Supervision. Rationale: The Critical finding in key ceremony procedures represents an immediate risk to customer assets. Weekly progress reporting to the VFSC is required. Remediation of the Critical finding must be verified within 48 hours. Semi-annual audits at Tier 3 intensity are required until de-escalation criteria are met.

Example 5: Divergent Inputs Requiring a Conservative Approach

Scenario: StableCoin Holdings has strong governance and monitoring practices but significant gaps in control implementation. Domain-level maturity scores: Governance and Leadership (Level 4), Risk Management (Level 3), Control Implementation (Level 2), Monitoring and Measurement (Level 4), Continuous Improvement (Level 3). Applying the critical domain principle (Appendix B), the overall programme maturity is anchored to the lowest critical domain score: Level 2 (Developing) from Control Implementation. Overall Audit Rating: Satisfactory.

Calculation: Impact Score = 2 (Satisfactory). Probability Score = 4 (Developing, after critical domain anchoring). Risk Score = 2 × 4 = 8. Note: The arithmetic mean of domain scores would be 3.2 (Level 3 Defined), but the critical domain principle correctly anchors the overall maturity to Level 2.

Determination: The Risk Score of 8 falls within the 7–15 range for Enhanced Supervision. The Satisfactory overall audit rating suggests Standard to Enhanced supervision. The Developing maturity level (after critical domain anchoring) maps to Enhanced supervision. The Risk Score integration correctly identifies the need for Enhanced Supervision, reflecting the weakness in Control Implementation that would be masked if the maturity domains were simply averaged.

Recommendation: Enhanced Supervision. Rationale: Despite strong governance and monitoring practices, the Control Implementation domain weakness (Level 2) creates material risk to customer assets. The VASP should prioritise control deployment and demonstrate progress towards Level 3 in Control Implementation.

Example 6: Baseline Audit - Licence Cannot Be Granted

Scenario: NewExchange Ltd is a VASP applicant undergoing its baseline cybersecurity audit. The audit identifies one Critical finding (no documented key management procedures; keys generated on internet-connected workstations) and four High findings. Overall Audit Rating: Deficient. Programme Maturity: Initial (Level 1).

Calculation: Impact Score = 4 (Deficient). Probability Score = 5 (Initial). Risk Score = 4 × 5 = 20.

Determination: Per Section 1.2.1.1 (Licensing Threshold Policy), the VFSC will not grant a licence to any applicant whose baseline audit identifies Critical or High findings. The presence of one Critical finding and four High findings means the licence cannot be granted until these are remediated.

Recommendation: Supervision Level: Not Applicable. Outcome: Licence cannot be granted. The auditor shall prepare a Gap and Remediation Report per Section 1.2.1.8. The applicant must remediate all Critical and High findings and undergo verification before the licence application can proceed. The Risk Score of 20 is recorded for reference but does not determine a supervision level as the licensing threshold has not been met.

3.5.2 Risk Score Reference Matrix

The following matrix shows the Risk Score and resulting supervision level for all combinations of Impact Score and Probability Score. For baseline audits where Critical or High findings are identified, the licensing threshold policy applies regardless of the calculated Risk Score.

Impact \ Probability	1 (Opt.)	2 (Man.)	3 (Def.)	4 (Dev.)	5 (Init.)
1 (Strong)	1 – Std	2 – Std	3 – Std	4 – Std	5 – Std
2 (Satisfactory)	2 – Std	4 – Std	6 – Std	8 – Enh	10 – Enh
3 (Needs Improvement)	3 – Std	6 – Std	9 – Enh	12 – Enh	15 – Enh
4 (Deficient)	4 – Std	8 – Enh	12 – Enh	16 – Int	20 – Int
5 (Critically Deficient)	5 – Std	10 – Enh	15 – Enh	20 – Int	25 – Int

Key: Std = Standard Supervision (Risk Score 1–6); Enh = Enhanced Supervision (Risk Score 7–15); Int = Intensive Supervision (Risk Score 16–25). Probability headers: Opt. = Optimised; Man. = Managed; Def. = Defined; Dev. = Developing; Init. = Initial.

Part 4: CCSS V9-Aligned Control Testing Procedures

For VASP Cybersecurity Type 2 applicants managing client virtual assets, VFSC requires a minimum of CCSS V9 Level II compliance, with enhanced requirements for custody services that exceed specified thresholds. This part sets out the control testing procedures for each of the 10 CCSS V9 aspects across two categories: Cryptographic Asset Management (aspects 1.01 through 1.06) and Operations (aspects 2.01 through 2.04). Each section identifies the Level I and Level II requirements applicable to each control, together with the testing procedures the auditor should perform.

Where a Level II requirement states "there are no additional requirements beyond those specified for Level I", the auditor tests against the Level I requirement only. Where a control states "not required for Level I", the requirement applies at Level II only. All Level I requirements are cumulative at Level II, meaning that Level II compliance requires satisfaction of both the Level I requirement and any additional Level II requirement for each control.

Category 1: Cryptographic Asset Management

4.1 Key Material Generation (CCSS V9 1.01)

Aspect Objective: This aspect covers the generation of key material that will be used within a digital asset and blockchain protocol. The secure generation of key material requires two things to be secure: confidentiality and unpredictable numbers. Confidentiality is required to ensure that the newly generated key material is not read/copied by an unintended party. Nondeterministic and unpredictable numbers are required to ensure the newly generated key material cannot be guessed or determined by an unintended party. Each of the goals listed provide assurance that the key material is generated in a confidential and unguessable manner.

1.01.1 Actor-generated Key Material

Level I Requirement: 1.01.1.1 Key material is generated by the actor who will be using it.

Level I Requirement: 1.01.1.2 Where an automated signing agent will use key material, and the place of generation of key material is different from the place of use. The following criteria are addressed: 1. The key material is generated within a secure Key Management System that meets applicable CCSS requirements. 2. The key material is transferred securely to the automated signing agent from the place of generation that meets applicable CCSS requirements. 3. The key material is securely removed from the place of generation that meets applicable CCSS requirements.

Level II Requirement: 1.01.1.3 A digital signature for the key material generation mechanism is generated, published, and validated prior to each execution.

Testing Procedures

Observe or review video documentation of key generation ceremony. Verify that key material is generated by the actor who will use it, with no transfer to another actor post-generation. For automated signing agents, verify secure generation, secure transfer, and secure removal from generation environment. Verify that digital signatures for the key generation mechanism are generated, published, and validated prior to each execution. Inspect signature validation logs and confirm the published signature matches the generation software in use.

1.01.2 Validation of Generation Methodology

Level I Requirement: Not required for Level I.

Level II Requirement: 1.01.2.1 The methodology for generating key material is validated prior to use. Software does not include features that restrict which values can be used. Software does not include features that store or transmit data to another actor, unless that feature enhances security.

Level II Requirement: 1.01.2.2 In cases where key material is generated without the use of software, the generation methodology is validated to ensure determinism is not present.

Testing Procedures

Review the key material generation methodology documentation. Verify software does not include features restricting entropy or transmitting data to another actor (unless security-enhancing). For non-software generation methods, confirm the methodology has been validated to ensure no determinism is present (e.g., verify dice are not weighted, cards are unique). Inspect validation records and any third-party audits of the generation methodology.

1.01.3 Deterministic Random Bit Generator (DRBG) Compliance

Level I Requirement: Not required for Level I.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Verify DRBG compliance with NIST SP 800-90A. Review DRBG configuration documentation and test outputs against NIST Statistical Test Suite (STS) or equivalent. Inspect cryptographic library versions and confirm they implement approved DRBG algorithms.

1.01.4 Entropy Pool

Level I Requirement: 1.01.4.1 Key material is generated on a Key Management System with sufficient entropy to ensure key material is not generated with any bias towards a reduced range of values, or other deterministic properties.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Review entropy source configuration on Key Management Systems used for key generation. Verify sufficient entropy is available to prevent bias or deterministic properties. Inspect entropy pool configuration, test entropy source independence, and review any hardware random number generator (HRNG) certifications.

4.2 Wallet Generation (CCSS V9 1.02)

Aspect Objective: This aspect covers the generation of wallets or addresses that can receive digital assets. Wallets are generated using cryptographic signing methodologies that can support single-signer and multi-signer mechanisms. Furthermore, wallets can be generated individually (commonly referred to as “Just a Bunch Of Keys” or JBOK wallets) or in a deterministic way that allows a set of addresses/key pairs to be generated from a single master seed. Security of wallet generation is derived from the integrity of the wallet in the face of various risks such as a lost/stolen/compromised key material and the confidentiality of the wallet that would make it difficult to associate a wallet with a particular actor.

1.02.1 Signing Configuration

Level I Requirement: Not required for Level I.

Level II Requirement: 1.02.1.1 When considering the application of a single-signer mechanism to a wallet, the following criteria are addressed: 1. The criticality of the wallet to the CCSS Trusted Environment. 2. The impact of loss of customer funds controlled by the wallet. 3. The risk of a wallet compromise is included in the threat model defined in requirement 2.03.2.1. 4. The effectiveness of the security controls implemented to protect the wallet.

Testing Procedures

Where a single-signer mechanism is applied to a wallet, review the documented risk audit covering: criticality of the wallet to the CCSS Trusted Environment, impact of loss of customer funds controlled by the wallet, inclusion of wallet compromise risk in the threat model (requirement 2.03.2.1), and effectiveness of security controls protecting the wallet. Verify that wallets managing the bulk of customer funds implement a multi-signer mechanism.

1.02.2 Key Material Redundancy

Level I Requirement: Not required for Level I.

Level II Requirement: 1.02.2.1 A wallet that has implemented a multi-signer mechanism has at least one redundant key for recovery purposes.

Testing Procedures

For wallets implementing a multi-signer mechanism, verify that at least one redundant key exists for recovery purposes. Confirm the threshold configuration provides redundancy (e.g., 2-of-3 ensures one redundant key). Test the recovery procedure using the redundant key to confirm operability.

1.02.3 Geographic Key Material Distribution

Level I Requirement: Not required for Level I.

Level II Requirement: 1.02.3.1 Key materials for a wallet that implements a multi-signer mechanism are stored in different locations.

Testing Procedures

Verify that key materials for wallets implementing a multi-signer mechanism are stored in different geographic locations. Review the risk audit for co-location risks. Inspect physical or logical separation evidence and confirm that localised disruptions (fire, flood, earthquake, break-in) at any single location would not compromise the signing threshold.

1.02.4 Entity Key Material Distribution

Level I Requirement: Not required for Level I.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Verify that key materials for wallets implementing a multi-signer mechanism are distributed across different entities where applicable. Confirm no single entity holds sufficient key material to meet the signing threshold unilaterally.

1.02.5 Wallet Generation Policy Documentation

Level I Requirement: Not required for Level I.

Level II Requirement: 1.02.5.1 The entity has a documented policy in place which details the company's internal policies and procedures and covers the relevant areas of wallet generation.

Testing Procedures

Review the documented wallet generation policy covering internal policies, procedures, and relevant areas of wallet generation. Verify the policy is current, approved by management, and accessible to relevant personnel. Confirm operational practices align with the documented policy.

4.3 Key Material Storage (CCSS V9 1.03)

Aspect Objective: This aspect covers the secure storage and backup of key material to ensure it remains protected, recoverable, and inaccessible to unauthorized parties. Key material is encrypted and backed up, with backups stored securely and protected from

environmental threats. To prevent unauthorized use or tampering, access to operational key material and its backups is tightly controlled.

1.03.1 Encryption of Operational Key Material

Level I Requirement: 1.03.1.1 Key material is stored with the use of strong encryption when not in use.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Verify that operational key material is encrypted at rest using strong encryption when not in use. Inspect encryption configuration on all storage media holding key material. Confirm encryption algorithms meet current industry standards (e.g., AES-256). Review key management for encryption keys themselves.

1.03.2 Key Material Backup(s)

Level I Requirement: 1.03.2.1 A backup(s) of the operational key material exists.

Level II Requirement: 1.03.2.2 A backup(s) exists for all key material used in the wallet. The backup can take any form (e.g., paper, digital, metal).

Testing Procedures

Verify that backups exist for operational key material (Level I) and for all key material used in the wallet (Level II). Confirm backup media type (paper, digital, metal) and verify backup completeness. Test backup restoration procedures to confirm recoverability.

1.03.3 Environmental Protection for Key Material Backup(s)

Level I Requirement: 1.03.3.1 The backup(s) is protected against environmental risks.

Level II Requirement: 1.03.3.2 The backup(s) of key material is stored in a geographically separate location(s) from the storage and usage of operational key material.

Testing Procedures

Verify environmental protections for key material backups (Level I: protection against environmental risks; Level II: geographically separate storage from operational key material). Inspect protective measures (waterproof containers, fireproof safes) and, for Level II, verify geographic separation with evidence of distinct physical locations.

1.03.4 Key Material Backup(s) Have Access Control

Level I Requirement: 1.03.4.1 The backup(s) is protected by access controls that prevent unauthorized parties from accessing it.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Verify access controls protecting key material backups prevent unauthorised access. Inspect physical access controls (safes, safe deposit boxes, locked storage) and confirm only authorised operators hold keys or combinations. Review access logs where available.

1.03.5 Tamper-evident Key Material Backup(s)

Level I Requirement: Not required for Level I.

Level II Requirement: 1.03.5.1 The backup(s) implements some form of tamper-evident mechanism that allows an operator to determine if it has been accessed.

Testing Procedures

Verify tamper-evident mechanisms on key material backups (Level II). Inspect serial-numbered tamper-evident bags, sealed envelopes with signatures over seals, or equivalent mechanisms. Confirm operators can determine if a backup has been accessed. Review tamper-evidence inspection logs and procedures.

1.03.6 Key Material Backup(s) Encryption

Level I Requirement: Not required for Level I.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Verify encryption of key material backups where applicable. This control has no additional Level I or Level II requirements beyond the base standard but should be verified as good practice where digital backup media is used.

4.4 Key Material Access (CCSS V9 1.04)

Aspect Objective: This aspect covers the policies and procedures surrounding granting and revoking access to key material. Personnel typically have greater access to the CCSS Trusted Environment with respect to accessing its information, invoking privilege-restricted actions, and representing the entity to the public. Improper management of the onboarding and offboarding of personnel introduces risks of privileged accounts remaining when personnel depart, as well as unrevoked key material that persists in signing authority for certain transactions.

1.04.1 Grant/Revoke Documentation

Level I Requirement: 1.04.1.1 The entity maintains checklists that cover all tasks that are completed when personnel vacate or transition into key holder roles within the entity.

These checklists have been reviewed by knowledgeable personnel to ensure “least privilege principles” are applied to the system, as well as necessary access where required.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Review grant/revoke checklists covering all tasks completed when personnel vacate or transition into key holder roles. Verify checklists have been reviewed by knowledgeable personnel to ensure least privilege principles are applied. Sample recent personnel transitions and confirm checklist completion.

1.04.2 Approved Communication Channel

Level I Requirement: Not required for Level I.

Level II Requirement: 1.04.2.1 All key holder grant/revoke requests are conducted over Approved Communication Channels.

Testing Procedures

Verify that all key holder grant/revoke requests are conducted over Approved Communication Channels (Level II). Review sample grant/revoke requests and confirm the communication channel used. Verify the channel provides high confidence of the identities of communicating parties.

1.04.3 Grant/Revoke Audit Trail

Level I Requirement: Not required for Level I.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Verify the existence and completeness of audit trails for key material grant/revoke actions. Review recent grant/revoke events against the audit trail. This control has no additional Level I or Level II requirements beyond the base standard.

4.5 Key Material Usage (CCSS V9 1.05)

Aspect Objective: This aspect covers the secure use of key material that minimizes the risks to the confidentiality of key material and the integrity of funds. This section does not cover the usage of key material backup(s) which are only used in the event operational key material is lost/damaged/inaccessible. A variety of risks are present when using key material that can lead to the loss of funds, including dirty signature vulnerabilities (i.e. re-used ‘R’ values), the opportunity for malware to copy or modify key material, and malicious insiders who use their authorized access to send unauthorized transactions.

1.05.1 Access Authentication to Key Material

Level I Requirement: 1.05.1.1 Access to the operational key material requires an identifier and at least 2 (two) distinct types of authentication factors.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Verify that access to operational key material requires an identifier (username, email, GUID) and at least two distinct types of authentication factors. Test authentication controls by confirming multi-factor authentication is enforced. Review authentication factor types in use (e.g., hardware tokens, digital signatures, biometrics, TOTP).

1.05.2 Operational Key Material Environment

Level I Requirement: 1.05.2.1 Key material is only used within the CCSS Trusted Environment.

Level I Requirement: 1.05.2.2 The key material is isolated from other operating systems and application processes to avoid unauthorized access or leakage of key material.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Verify that key material is only used within the CCSS Trusted Environment (1.05.2.1). Confirm that key material is isolated from other operating systems and application processes (1.05.2.2). Inspect the use of Hardware Security Modules (HSMs), Trusted Execution Environments (TEEs), or equivalent isolation mechanisms. Review system architecture documentation and test for process isolation.

1.05.3 Operator Reference Checks

Level I Requirement: 1.05.3.1 All individual actors involved in operations with key material, or with the ability to impact the security of key generation, management, or usage have had their references checked prior to the actor being trusted with access to key material or operations.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Verify that all individual actors involved in operations with key material have had their references checked prior to being trusted with access. Review reference check records for all current key holders and operators.

1.05.4 Operator ID Checks

Level I Requirement: 1.05.4.1 All individual actors involved in operations with key material, or with the ability to impact the security of key generation, management, usage, or storage have undergone identity verification to ensure they are who they say they are. These checks are conducted prior to the actor being trusted with access to key material.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Verify that all individual actors involved in operations with key material have undergone identity verification prior to being trusted with access. Review identity verification records (government-issued ID checks) for all current key holders.

1.05.5 Operator Background Checks

Level I Requirement: 1.05.5.1 All individual actors involved in operations with key material, or with the ability to impact the security of key generation, management, usage, or storage have had background checks performed by law enforcement personnel or investigative firms. These checks are conducted prior to the actor being trusted with access to key material or operations and periodically; as allowed by local laws and regulations.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Verify that all individual actors involved in operations with key material have had background checks performed by law enforcement or investigative firms prior to being trusted with access, and periodically thereafter as permitted by local laws. Review background check records and confirm currency.

1.05.6 Key Management Training

Level I Requirement: 1.05.6.1 All individuals involved in key management operations, or with the ability to impact the security of key material, complete specific applicable training. This training is to be conducted on hire and conducted before the actor being trusted with access to Key Material, and then annually.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Verify that all individuals involved in key management operations complete specific applicable training on hire, before being trusted with access to key material, and

annually thereafter. Review training records, confirm training content covers CCSS-specific threats, risks, and controls, and verify annual refresher completion.

1.05.7 Key Management Responsibilities

Level I Requirement: 1.05.7.1 Key management roles and responsibilities are formally acknowledged in writing by each person who has access to key material. This includes personnel who have been delegated key management responsibilities.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Verify that key management roles and responsibilities are formally acknowledged in writing by each person with access to key material, including delegated responsibilities. Review signed acknowledgement documents for all current key holders and delegates.

1.05.8 Spend Verification

Level I Requirement: Not required for Level I.

Level II Requirement: 1.05.8.1 Verification of fund destinations and amounts is performed via Approved Communication Channels prior to the use of key material.

Testing Procedures

Verify that verification of fund destinations and amounts is performed via Approved Communication Channels prior to the use of key material (Level II). Review sample transactions and confirm out-of-band verification was performed. Test the verification process for completeness and timeliness.

1.05.9 Multi-Signer Mechanism Usage

Level I Requirement: 1.05.9.1 Key material for a wallet that implements a multi-signer mechanism is stored and used on different logical or physical devices.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Verify that key material for wallets implementing a multi-signer mechanism is stored and used on different logical or physical devices. Inspect device inventories and confirm no single device holds sufficient key material to meet the signing threshold. Review system architecture documentation.

1.05.10 Deterministic Random Bit Generator (DRBG) Compliance

Level I Requirement: 1.05.10.1 Digital signatures follow best practices for the algorithm(s) implemented by the Key Management System.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Verify that digital signatures follow best practices for the algorithms implemented by the Key Management System. Confirm DRBG compliance with NIST SP 800-90A or deterministic scheme compatible with RFC 6979. Review cryptographic library configurations and verify secure generation of critical values (e.g., DSA k-values).

4.6 Data Sanitisation (CCSS V9 1.06)

Aspect Objective: This aspect covers the removal of key material from digital media. Due to the manner in which file systems allocate data on digital media, digital forensic techniques can be employed to read old data that has previously been sanitized. Proper sanitization of digital media ensures the proper removal of all key material, eliminating the risk of information leakage from decommissioned devices like servers, hard disk drives, and removable storage.

1.06.1 Data Sanitization Policy Existence

Level I Requirement: 1.06.1.1 Policy and procedure document(s) exist that conform to NIST SP 800-88 by defining the requirements for sanitizing and the destruction of media that holds key material. The policy and procedure documentation is read/understood by all staff who have access to key material.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Review the data sanitisation policy and procedure documents for conformity with NIST SP 800-88. Verify the policy defines requirements for sanitising and destroying media that holds key material. Confirm all staff with access to key material have read and understood the policy. Review training acknowledgement records.

1.06.2 Media Sanitization Audit Documentation

Level I Requirement: Not required for Level I.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Review audit documentation for media sanitisation events. Verify records of sanitisation and destruction activities are maintained. This control has no additional Level I or Level II requirements beyond the base standard but should be verified as good practice.

Category 2: Operations

4.7 Security Tests and Audits (CCSS V9 2.01)

Aspect Objective: This aspect covers third-party reviews of the security systems, technical controls, and policies that protect the CCSS Trusted Environment from all forms of risk as well as vulnerability and penetration tests designed to identify paths around existing controls. Regardless of the technical skills, knowledge, and experience of personnel who build and maintain the CCSS Trusted Environment, it has been proven that third-person reviews often identify risks and control deficiencies that were either overlooked or underestimated by personnel. For the same reasons that development companies require different people to test a product from those who write it, different people than those who implement a cryptocurrency system should assess its security. Third parties provide a different viewpoint and are independent of the technical controls and can be objective without risk of retaliation.

2.01.1 Security Development and Documentation

Level I Requirement: 2.01.1.1 An individual(s) with expertise in information security must be engaged in all stages of the design, development, deployment, and ongoing maintenance of systems providing cryptocurrency functions.

Level II Requirement: 2.01.1.2 A regular security audit that includes vulnerability and penetration testing has been completed by an independent, qualified third-party. Documentation shows that all concerns raised by the audit have been evaluated for risk and addressed by the entity.

Testing Procedures

Verify that individuals with information security expertise are engaged in all stages of design, development, deployment, and ongoing maintenance of systems providing cryptocurrency functions (Level I). For Level II, verify that regular security audits including vulnerability and penetration testing have been completed by an independent, qualified third party. Review audit reports and confirm all concerns raised have been evaluated for risk and addressed.

2.01.2 Smart Contract Software Code Audit Documentation

Level I Requirement: 2.01.2.1 All smart contract software code versions deployed to the environment(s) where the entity stakeholders interact with the smart contract have been audited by an external third-party auditor skilled in the development languages used for the smart contract software. NOTE: the requirement is not applicable to any environments used for development, testing, or staging. This requirement applies to smart contracts deployed to the "production" network or the like.

Level I Requirement: 2.01.2.2 All smart contract software code audit reports are accessible to the entity stakeholders. The audit reports cover the currently deployed versions to the environment(s) where the entity stakeholders interact with the smart contract. NOTE: the requirement is not applicable to any environments used for development, testing, or staging. This requirement applies to smart contracts deployed to the "production" network or the like.

Level I Requirement: 2.01.2.3 All issues with a severity of medium or higher identified in a code audit of the smart contract software are addressed by the entity before deployment to the environment(s) where the entity stakeholders interact with the smart contract. NOTE: the requirement is not applicable to any environments used for development, testing, or staging. This requirement applies to smart contracts deployed to the "production" network or the like.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Verify that all smart contract software code versions deployed to production environments have been audited by a qualified external third-party auditor (2.01.2.1). Confirm audit reports are accessible to entity stakeholders and cover currently deployed versions (2.01.2.2). Verify that all issues with medium or higher severity identified in code audits have been addressed before production deployment (2.01.2.3). Where the VASP does not deploy smart contracts, document the non-applicability with supporting rationale.

4.8 Logging and Monitoring (CCSS V9 2.02)

Aspect Objective: This aspect covers monitoring the CCSS Trusted Environment's technical components audit logs for suspicious activity. When suspicious activity is identified, alerts must be generated so that personnel can triage and respond to the event to detect and respond to suspicious activity proactively.

2.02.1 Application Audit Logs

Level I Requirement: 2.02.1.1 Audit trails exist for a subset of actions performed within the CCSS Trusted Environment.

Level II Requirement: 2.02.1.2 All actions performed by all users within the CCSS Trusted Environment are logged. Audit logs are retained for at least one year in a trusted environment.

Testing Procedures

Verify that audit trails exist for actions performed within the CCSS Trusted Environment (Level I: subset of actions; Level II: all actions by all users, retained for at least one year in a trusted environment). Review audit log configuration, sample log entries, and confirm retention periods meet requirements.

2.02.2 Audit Log Backup

Level I Requirement: Not required for Level I.

Level II Requirement: 2.02.2.1 In addition to recording all actions performed within the CCSS Trusted Environment, this audit information is periodically backed up to a separate server.

Testing Procedures

Verify that audit log information is periodically backed up to a separate server (Level II). Confirm backup frequency, verify backup integrity, and test backup restoration. Review backup server access controls and separation from the primary CCSS Trusted Environment.

2.02.3 Audit Log Monitoring

Level I Requirement: 2.02.3.1 The CCSS Trusted Environment's audit logs are monitored for suspicious activity, and alerts are generated when suspicious activity is detected. Appropriate personnel address the alerts generated. The monitoring frequency is defined by the entity and meets all components of requirement 2.03.2.1.

Level II Requirement: 2.02.3.2 The CCSS Trusted Environment's audit logs are continuously monitored for suspicious activity, and alerts are generated in real time when suspicious activity is detected. Appropriate personnel address the alerts generated.

Testing Procedures

Verify that the CCSS Trusted Environment's audit logs are monitored for suspicious activity (Level I: at defined frequency per threat model; Level II: continuously with real-time alerts). Confirm alerts are generated when suspicious activity is detected and that appropriate personnel address alerts. Review alert response procedures and sample alert resolution records.

2.02.4 Blockchain State Monitoring

Level I Requirement: Not required for Level I.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Verify blockchain state monitoring capabilities where applicable. This control has no additional Level I or Level II requirements beyond the base standard but should be assessed as good practice for detecting on-chain anomalies such as unexpected transactions or address activity.

4.9 Governance and Risk (CCSS V9 2.03)

Aspect Objective: This aspect covers the governance policies, standards, and procedures that guide and control an entity to ensure its CCSS Trusted Environment is effective, efficient, and secure. It also includes the requirements for a comprehensive risk management program to identify potential risks to the CCSS Trusted Environment and apply appropriate risk treatments.

2.03.1 Governance

Level I Requirement: 2.03.1.1 A member of executive management is responsible for the security of the system and formally acknowledges their responsibilities in writing.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Verify that a member of executive management is responsible for the security of the system and has formally acknowledged their responsibilities in writing. Confirm succession arrangements exist so that if the assigned executive is unavailable, another executive takes over the role immediately. Review the written acknowledgement and succession documentation.

2.03.2 Risk Management

Level I Requirement: 2.03.2.1 The entity has identified security threats to the CCSS Trusted Environment and have defined and implemented controls to reduce the residual risk of an attack to an acceptable level using a threat model. The following considerations are addressed: 1. The entity reviews the threat model periodically to ensure it is up to date, the controls currently implemented are still effective, and the risk of an attack is reduced. 2. If a procedure requires a defined frequency to perform tasks for a control, such as reviewing audit logs, the threat model specifies the task frequency.

Level II Requirement: 2.03.2.2 The entity implements a risk management program based on industry recognized risk management standards and frameworks such as ISO/IEC 27005 and NIST SP 800-37.

Testing Procedures

Verify that the entity has identified security threats to the CCSS Trusted Environment and defined and implemented controls using a threat model (Level I). Confirm the threat model is reviewed periodically, control effectiveness is reassessed, and task frequencies for procedures are specified. For Level II, verify the entity implements a risk management programme based on industry-recognised standards (e.g., ISO/IEC 27005, NIST SP 800-37). Review the threat model, risk register, and risk treatment plans.

2.03.3 Service Provider Management

Level I Requirement: 2.03.3.1 Service provider management is implemented for any vendor or service provider that could impact the security of the CCSS Trusted Environment and addresses: 1. Procurement processes to ensure any vendor or service provider meets applicable CCSS requirements before contractual engagement. 2. Annual review of the vendor or service provider's compliance with applicable CCSS requirements. The frequency of review may increase from at least annually based on the entity threat model as defined in requirement 2.03.2.1.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Verify that service provider management is implemented for any vendor or service provider that could impact the security of the CCSS Trusted Environment. Confirm procurement processes ensure vendors meet applicable CCSS requirements before engagement and that annual reviews of compliance are conducted. Review vendor due diligence records, contractual requirements, and annual review documentation.

4.10 Key Compromise Protocol (CCSS V9 2.04)

Aspect Objective: This aspect covers the existence and use of documented policies and procedures that define the actions that must be taken in the event key material or its operator/holder are believed to have become compromised. Entities must be prepared to deal with a situation where key material has – even potentially – become known, determinable, or destroyed. Policies and procedures to govern these events decrease the risks associated with lost funds and increase the availability of the system to its users. Examples of when a Key Compromise Policy (KCP) would be invoked include the identification of tampering of a tamper-evident seal placed on the media that stores key material, the apparent disappearance of an operator whose closest friends and family cannot identify their whereabouts, or the receipt of communication that credibly indicates an operator or key material is likely at risk of being compromised. The execution of KCP makes use of Approved Communication Channels to ensure KCP messages are only sent/received by authenticated actors.

2.04.1 Key Compromise Policy Existence

Level I Requirement: 2.04.1.1 An inventory of all key material exists and the entity has an awareness of which key material is critical to the successful operation of the CCSS Trusted Environment.

Level I Requirement: 2.04.1.2 A Key Compromise Policy and procedures are documented. The following is addressed: 1. Each specific classification of key material used throughout the CCSS Trusted Environment. 2. A detailed plan of dealing with its compromise that includes the use of Approved Communication Channels during execution. 3. Identities of actors via roles (not names) and includes secondary actors in the event any primary actor is unavailable to carry out the KCP.

Level II Requirement: 2.04.1.3 The key material inventory is reviewed at least annually to ensure that all key material has been recorded and that the recorded information for key material is accurate and up to date.

Testing Procedures

Verify that an inventory of all key material exists with awareness of which key material is critical (2.04.1.1). Review the documented Key Compromise Policy (KCP) covering each

classification of key material, detailed compromise response plans using Approved Communication Channels, and identification of actors by role with secondary actors designated (2.04.1.2). For Level II, verify the key material inventory is reviewed at least annually and recorded information is accurate and up to date (2.04.1.3). Review the KCP document, inventory records, and annual review evidence.

2.04.2 Key Compromise Policy Training and Rehearsals

Level I Requirement: Not required for Level I.

Level II Requirement: There are no additional requirements beyond those specified for Level I.

Testing Procedures

Verify that Key Compromise Policy training and rehearsals have been conducted where applicable. This control has no additional Level I or Level II requirements beyond the base standard but should be assessed as good practice. Review training records and rehearsal documentation if available.

4.11 Hot/Cold Storage Requirements (VFSC Regulatory)

This section addresses VFSC-specific regulatory requirements for the segregation of client virtual assets between hot (online) and cold (offline) storage. These requirements supplement the CCSS V9 controls above and are aligned with international custody standards.

Requirements include: minimum 90% cold storage for client assets (aligned with Singapore MAS and Hong Kong SFC standards); hot wallet limits based on operational liquidity needs (30–90 days trading volume maximum); insurance coverage of 100% for hot wallet holdings and minimum 50% for cold storage; and daily reconciliation between blockchain records, wallet systems, and accounting records.

Testing Procedures

Verifying storage allocation percentages against policy; testing automated sweeping procedures to cold storage; reviewing insurance policy coverage and exclusions; performing independent reconciliation testing; and verifying client asset segregation from operational wallets. In accordance with Virtual Asset Act 2025 Section 62, the auditor must verify that the VASP maintains a complete and reconciled record of client virtual asset holdings, demonstrating that client assets and liabilities are identified and accounted for separately from each other and from the VASP's own assets and liabilities.

4.12 Key Ceremony Procedural Requirements

Auditors should verify the following elements of key ceremony procedures in connection with the key material generation controls tested under Section 4.1.

Secure Location Preparation: Key generation ceremonies should occur in a controlled environment with restricted access. For Level II compliance, this should be an air-gapped workstation with no network connectivity. Level III implementations may require a Faraday-shielded room to prevent electromagnetic emanations. The environment should be inspected and cleared of unauthorised devices (mobile phones, recording equipment) before the ceremony commences.

Designated Roles and Participants: Ceremonies should have formally designated roles including a Ceremony Administrator responsible for overall coordination, Key Custodians who will hold key shares, Witnesses who observe and attest to proper procedure, and optionally an External Auditor or Notary for independent verification. No single participant should have access to sufficient key material to compromise the wallet.

Key Share Generation and Distribution: Where Shamir's Secret Sharing or similar threshold schemes are employed, the ceremony procedure should document the threshold configuration (e.g., 3-of-5), the method of share generation, how shares are recorded (encrypted USB, paper backup in tamper-evident envelope, hardware security module), and the immediate secure storage of each share in geographically distributed locations. For MPC-based systems, the procedure should document the distributed key generation protocol and participant coordination requirements.

Audit Trail and Recording: All key ceremonies should be documented through contemporaneous written records signed by all participants, video recording of the ceremony (stored securely with restricted access), serial number tracking of all hardware devices and tamper-evident materials used, and cryptographic attestation of generated public keys.

Secure Transportation and Storage: Procedures should address how key material is transported from the ceremony location to long-term storage, including chain-of-custody documentation, use of tamper-evident packaging, secure courier arrangements for geographically distributed storage, and verification procedures upon receipt at storage locations.

Part 4A: Supplementary Control Testing Procedures

The following control areas supplement the CCSS V9-specific procedures in Part 4 and address broader information security controls relevant to VASP operations. These supplementary procedures ensure comprehensive coverage of the eight control domains defined in Section 2.4, including areas not directly addressed by the CCSS V9 framework. Auditors should evaluate these areas against the applicable standards indicated.

4A.1 Cloud Security Policy Audit

For VASPs utilising cloud infrastructure (IaaS/PaaS such as AWS, Azure, GCP, or SaaS platforms), auditors should verify the existence and adequacy of cloud security policies and controls.

Audit Criteria

Cloud Configuration Standards: Policies should mandate use of Virtual Private Clouds (VPCs) with appropriate network segmentation, security group configurations following least privilege principles, encryption of cloud storage (server-side and client-side where appropriate), and secure configuration of cloud-native services. Reference: ISO 27017 (Cloud Security), CSA Cloud Controls Matrix (CCM), NIST CSF PR.DS, PR.AC.

Identity and Access Management: Policies should require MFA for all console and programmatic access, use of IAM roles rather than static credentials where possible, regular access reviews, prohibition of root account usage for routine operations, and API key rotation procedures. Reference: ISO/IEC 27001:2022 A.5.18, NIST CSF PR.AC-1, PR.AC-4.

Shared Responsibility Model: The VASP should demonstrate understanding of the cloud provider's shared responsibility model and document which security controls are provider-managed versus customer-managed. Auditors should verify that customer-responsible controls are appropriately addressed.

Cloud Security Monitoring: Policies should require use of cloud-native security services (AWS GuardDuty, Azure Security Center, GCP Security Command Center) or equivalent third-party tools, with alerts integrated into the security operations workflow. Reference: NIST CSF DE.CM-1, DE.AE-2.

Cloud Audit Logging: Policies should require enablement of cloud provider audit logging (AWS CloudTrail, Azure Activity Log, GCP Cloud Audit Logs) with logs forwarded to the VASP’s centralised logging infrastructure and retained in accordance with the audit log retention requirements tested under Part 4, Section 4.8. Reference: ISO/IEC 27001:2022 A.8.15; NIST CSF DE.AE-3.

Infrastructure-as-Code Security: Where VASPs use infrastructure-as-code (Terraform, CloudFormation, or equivalent), policies should address security review of IaC templates before deployment, version control of infrastructure definitions, and prohibition of hard-

coded secrets in IaC configurations. Reference: ISO/IEC 27001:2022 A.8.25; NIST CSF PR.IP-1.

Risk if Absent: Medium to High

Cloud misconfigurations are a leading cause of data breaches. Lack of formal cloud security governance increases the likelihood of exposed storage, compromised credentials, or inadequate logging.

4A.2 API Security Policy Audit

For VASPs providing APIs (trading APIs, integration APIs, internal microservices), auditors should verify API security controls.

Audit Criteria

Authentication and Authorisation: All API endpoints handling sensitive operations should require authentication (OAuth 2.0, API keys with secure storage, or equivalent). Authorisation should ensure proper scoping so users cannot access other users' data or exceed their permissions. Reference: ISO/IEC 27001:2022 A.8.27, NIST CSF PR.AC-4, OWASP API Security Top 10.

Transport Security: All API traffic should be encrypted using TLS 1.2 or higher. Certificate validation should be enforced. Policies should address certificate management and rotation. Reference: ISO/IEC 27001:2022 A.5.14, NIST CSF PR.DS-2.

Input Validation and Rate Limiting: APIs should implement input validation to prevent injection attacks, rate limiting to prevent abuse and denial-of-service, and anomaly detection for unusual access patterns. Reference: ISO/IEC 27001:2022 A.8.27, NIST CSF PR.IP-1.

API Key Management: Where API keys are issued to clients, policies should address secure generation, secure transmission to clients, rotation requirements, and revocation procedures. Reference: ISO/IEC 27001:2022 A.8.24.

API Versioning and Deprecation: Policies should address secure API versioning practices, including timelines for deprecation of older API versions and communication to clients regarding version lifecycle. Outdated API versions may contain known vulnerabilities and should be retired within defined timeframes. Reference: ISO/IEC 27001:2022 A.8.27; OWASP API Security Top 10.

Webhook and Callback Security: For VASPs using webhooks for transaction notifications or third-party integrations, policies should address webhook signature verification, validation of callback URLs, and protection against server-side request forgery (SSRF) via callback mechanisms. Reference: ISO/IEC 27001:2022 A.8.27.

Risk if Absent: Medium

Insecure APIs are common attack vectors for account takeover, data exfiltration, and fraudulent transactions in cryptocurrency exchanges.

4A.3 Endpoint and Mobile Security Policy Audit

Auditors should verify controls over endpoint devices (workstations, laptops) and mobile devices used by employees, particularly those with access to sensitive systems or key material.

Audit Criteria

Endpoint Protection: Policies should require endpoint detection and response (EDR) or antivirus software, host-based firewalls, full-disk encryption for all portable devices, automated patching, and secure configuration baselines. Reference: ISO/IEC 27001:2022 A.8.7, A.7.10, NIST CSF PR.PT-1.

Mobile Device Management: For organisations permitting BYOD or corporate mobile devices, policies should require mobile device management (MDM) enrolment, remote wipe capability, PIN/biometric enforcement, prohibition of jailbroken/rooted devices, and application whitelisting or containerisation for corporate data. Reference: ISO/IEC 27001:2022 A.8.1, NIST CSF PR.AC-3.

Removable Media Controls: Policies should address USB device restrictions, particularly for systems with access to key material or sensitive data. Reference: ISO/IEC 27001:2022 A.7.10.

Privileged Workstation Controls: For workstations used to access the CCSS Trusted Environment or signing infrastructure, policies should require enhanced hardening beyond standard endpoint controls, including application whitelisting, restricted internet access, and dedicated-use requirements. This complements the CCSS V9 1.05.2 requirement for key material isolation tested under Part 4, Section 4.5. Reference: ISO/IEC 27001:2022 A.8.19, A.8.7; NIST CSF PR.PT-1.

Risk if Absent: Medium

Compromised endpoints can serve as entry points for network intrusion or credential theft. Lost or stolen devices without encryption may expose sensitive data.

4A.4 Data Protection and Privacy Policy Audit

Auditors should verify policies addressing the protection of customer data and personal information, particularly KYC data collected under AML/CFT requirements.

Audit Criteria

Data Classification: Policies should define classification levels (e.g., public, internal, confidential, restricted) and handling requirements for each level. Customer personal data and KYC information should be classified as confidential or restricted. Reference: ISO/IEC 27001:2022 A.5.12, NIST CSF ID.AM-5.

Encryption Requirements: Policies should mandate encryption of sensitive data at rest (in databases, file storage) and in transit. Encryption standards should be specified (e.g., AES-256 for data at rest, TLS 1.2+ for transit). Reference: ISO/IEC 27001:2022 A.8.24, NIST CSF PR.DS-1, PR.DS-2.

Retention and Disposal: Policies should specify retention periods aligned with regulatory requirements (minimum 5-7 years for AML records) and secure disposal procedures for data no longer required. Reference: ISO/IEC 27001:2022 A.7.10, A.8.10 (Information deletion), A.5.33 (Protection of records); NIST CSF PR.IP-6.

Privacy Compliance: Where applicable privacy regulations apply (GDPR for EU customers, etc.), policies should address lawful basis for processing, data subject rights, and breach notification requirements. Reference: ISO/IEC 27001:2022 A.5.34.

Data Breach Response: Data breaches involving customer personal information trigger specific notification obligations under applicable privacy regulations and should be addressed in both the incident response plan (see Section 4A.10) and the data protection policy. The policy should define the criteria for determining whether a breach is notifiable and the process for notification to affected individuals and regulators. Reference: ISO/IEC 27001:2022 A.5.24, A.5.34.

Cross-Border Data Transfer: For VASPs operating across jurisdictions or using cloud infrastructure in multiple regions, policies should address cross-border data transfer requirements, including any data localisation obligations, adequacy determinations, and appropriate safeguards (such as standard contractual clauses or binding corporate rules) for international transfers of customer personal data. Reference: ISO/IEC 27001:2022 A.5.34; applicable privacy regulations.

Risk if Absent: Medium

Data breaches exposing customer personal information result in regulatory penalties, reputational damage, and potential identity theft affecting customers.

4A.5 Secure Configuration and Hardening Policy Audit

Auditors should verify policies requiring secure configuration of systems and adherence to hardening standards.

Audit Criteria

Configuration Baselines: Policies should mandate the use of secure configuration baselines for all system types (servers, workstations, network devices, databases). Reference to industry benchmarks such as CIS Benchmarks, DISA STIGs, or vendor hardening guides should be included. Reference: ISO/IEC 27001:2022 A.5.37, NIST CSF PR.IP-1.

Hardening Requirements: Baselines should address disabling unnecessary services and protocols, changing default credentials, removing or disabling default accounts, applying

security-relevant configuration settings, and minimising installed software. Reference: ISO/IEC 27001:2022 A.8.19, A.8.32.

Configuration Management: Policies should require documentation of approved configurations, change control for configuration modifications, and regular configuration audits or automated compliance checking. Reference: ISO/IEC 27001:2022 A.8.32, NIST CSF PR.IP-3.

Container and Orchestration Security: Where VASPs use containerised infrastructure (Docker, Kubernetes, or equivalent), hardening policies should extend to container image security (base image selection, vulnerability scanning of images before deployment, prohibition of running containers as root), orchestration platform hardening (CIS Benchmarks for Kubernetes, network policies between pods, RBAC for cluster access), and container runtime security (read-only filesystems, resource limits, seccomp profiles). Reference: ISO/IEC 27001:2022 A.8.19; CIS Benchmarks for Docker and Kubernetes.

Database Hardening: Given that VASPs hold sensitive customer data and financial records, database-specific hardening should be addressed, including removal of default schemas and sample databases, restriction of database administrative access to named accounts with MFA, encryption of sensitive columns containing customer personal data or credentials, and audit logging of all administrative and data-modifying operations. Reference: ISO/IEC 27001:2022 A.8.19, A.8.24; CIS Benchmarks for relevant database platforms.

Risk if Absent: Medium

Unhardened systems with default configurations are susceptible to common attacks and known exploits.

4A.6 Human Resources Security Policy Audit

Auditors should verify that security is integrated into HR processes throughout the employee lifecycle.

Audit Criteria

Pre-Employment Screening: Policies should require background verification checks proportionate to role sensitivity and regulatory requirements. For positions with access to customer assets or key material, enhanced screening, including identity verification, criminal record checks, and reference verification, should be mandated. Reference: ISO/IEC 27001:2022 A.6.1.

Employment Terms: Employment contracts should include confidentiality obligations, acceptable use requirements, and acknowledgment of security policies. NDAs should be in place for employees and contractors with access to sensitive information. Reference: ISO/IEC 27001:2022 A.6.2, A.6.6.

Security Awareness Training: Policies should mandate security awareness training at onboarding and periodic refreshers (at least annually). Training content should cover general information security, phishing awareness, and crypto-specific topics (secure handling of keys, recognising social engineering targeting crypto assets). Reference: ISO/IEC 27001:2022 A.6.3, NIST CSF PR.AT-1.

Termination and Change of Role: Policies should require prompt revocation of access upon termination or role change, return of company assets, exit interviews, and continued confidentiality obligations. Reference: ISO/IEC 27001:2022 A.6.5, A.5.18.

Insider Threat Programme: Given the sensitivity of VASP operations, where employees may have direct access to customer assets through key material, policies should address insider threat risk management beyond standard HR lifecycle controls. This should include monitoring of privileged user activities (particularly signing and withdrawal operations), enforcement of segregation of duties for high-value operations (ensuring no single individual can initiate and approve large-value transactions), and provision of confidential whistleblowing channels. Reference: ISO/IEC 27001:2022 A.5.7 (Threat intelligence), A.5.10 (Acceptable use); NIST CSF PR.IP-11.

Risk if Absent: Medium

Inadequate HR security controls increase insider threat risk and may result in delayed access revocation for departing employees.

4A.7 Travel Rule Data Security Audit

FATF Recommendation 16 (the Travel Rule) requires originator and beneficiary information to be transmitted with virtual asset transfers. Virtual Asset Act 2025 Section 27 implements this requirement for cross-border transfers. The VFSC has published Travel Rules Guidelines setting out the specific obligations for licensed VASPs. The security of travel rule data, its transmission, storage, and protection, is a cybersecurity concern that falls within the scope of this methodology. Auditors should verify that VASPs have implemented adequate controls over travel rule data.

Audit Criteria

Secure Transmission: Originator and beneficiary information must be transmitted between VASPs using encrypted channels. Policies should specify the transmission protocols used and the encryption standards applied. Reference: FATF Recommendation 16; Virtual Asset Act 2025, Section 27; ISO/IEC 27001:2022 A.5.14.

Encryption at Rest: Travel rule data containing originator and beneficiary personal information must be encrypted at rest in accordance with the VASP’s data classification policy. This data should be classified as confidential or restricted given its sensitivity. Reference: ISO/IEC 27001:2022 A.8.24; NIST CSF PR.DS-1.

Access Controls: Access to travel rule data must be restricted to authorised compliance personnel on a need-to-know basis. The auditor should verify that role-based access

controls are in place and that access logs are maintained. Reference: ISO/IEC 27001:2022 A.5.18; NIST CSF PR.AC-4.

Retention and Disposal: Travel rule records must be retained in accordance with AML/CFT record-keeping requirements (minimum five years per FATF Recommendation 11; seven years recommended) and securely disposed of when no longer required. Reference: ISO/IEC 27001:2022 A.7.10; NIST CSF PR.IP-6; AML/CFT Act No. 13 of 2014.

Counterparty VASP Verification: Before transmitting travel rule data to a counterparty VASP, the originating VASP should verify the identity and legitimacy of the counterparty. Policies should address how the VASP authenticates counterparty VASPs within Travel Rule protocol networks and what due diligence is performed before establishing data-sharing relationships with new counterparties. The auditor should verify that procedures are in place to prevent the transmission of originator and beneficiary personal information to unverified or fraudulent entities. Reference: FATF Recommendation 16; VFSC Travel Rules Guidelines.

Sunrise and Sunset Risk: Policies should address how the VASP handles transfers to or from jurisdictions or counterparties where Travel Rule compliance is not yet mandated (sunrise issue) or where compliance cannot be verified. This is a known gap in the global Travel Rule implementation landscape and the auditor should assess how the VASP manages the associated risk, including any enhanced due diligence measures applied to transfers where counterparty Travel Rule compliance cannot be confirmed. Reference: FATF Recommendation 16; FATF Updated Guidance on the Travel Rule (2021).

Risk if Absent: Medium

Failure to secure travel rule data exposes originator and beneficiary personal information to interception or unauthorised access and may constitute a supervisory gap identifiable during APG mutual evaluation against FATF Immediate Outcome 3 (supervision).

4A.8 Business Continuity and Disaster Recovery Audit

Auditors should verify that the VASP has established and tested business continuity and disaster recovery capabilities adequate for the protection and recovery of customer virtual assets. The absence of tested recovery procedures is particularly acute for multi-signature and MPC-based custody architectures where reconstruction requires coordinated recovery across multiple parties and locations.

Audit Criteria

Business Continuity Planning: Policies should require documented business continuity plans (BCPs) covering all critical VASP services, including trading platform availability, withdrawal processing, custody operations, and client communications during disruption. Plans should define Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for each critical service. The BCP should address VASP-specific scenarios

including blockchain network disruptions, chain forks, oracle failures, and loss of connectivity to blockchain nodes. Reference: ISO/IEC 27001:2022 A.5.29, A.5.30; NIST CSF PR.IP-9.

Disaster Recovery for Custody Infrastructure: Disaster recovery plans should specifically address wallet recovery procedures (including reconstruction of multi-signature configurations from geographically distributed key shares), HSM failover and replacement procedures, blockchain node recovery and resynchronisation, and restoration of signing capabilities from backup key material. Recovery procedures should be documented with sufficient detail that authorised personnel who were not involved in the original deployment could execute them. Reference: ISO/IEC 27001:2022 A.5.30; NIST CSF RC.RP-1.

System Backup and Recovery: Policies should mandate regular backups of all critical systems, databases, and configuration data (distinct from the key material backups tested under CCSS V9 1.03 in Part 4). Backup scope should include transaction databases and ledger records, client account and KYC data, system configurations and infrastructure-as-code, audit logs and monitoring data, and smart contract deployment records. Backup integrity should be verified through regular restoration testing. Reference: ISO/IEC 27001:2022 A.8.13; NIST CSF PR.IP-4.

Redundancy and Failover: Critical information processing facilities should have sufficient redundancy to meet availability requirements. For VASPs, this should include redundant blockchain nodes, redundant API gateway infrastructure, database replication and failover, and geographically distributed processing capabilities where the scale of operations warrants it. Reference: ISO/IEC 27001:2022 A.8.14; NIST CSF PR.PT-5.

Testing and Exercising: Business continuity and disaster recovery plans should be tested at least annually, with tabletop exercises or functional tests covering the VASP-specific scenarios identified above. Test results should be documented and lessons learned incorporated into plan updates. Reference: ISO/IEC 27001:2022 A.5.30; NIST CSF PR.IP-10.

Risk if Absent: High

Custodial VASPs that cannot recover signing capabilities or restore access to customer assets following a disruption risk permanent loss of customer funds. The absence of tested recovery procedures for multi-signature and MPC-based custody architectures, where reconstruction requires coordinated recovery across multiple parties and locations, presents a direct threat to the safeguarding of client assets.

4A.9 Network and Infrastructure Security Audit

Auditors should verify that the VASP has implemented network security controls adequate to protect the CCSS Trusted Environment and supporting infrastructure from external and internal threats. This section addresses the broader network and

infrastructure security controls referenced in the Network and Infrastructure Security control domain (Section 2.4).

Audit Criteria

Network Architecture and Segmentation: Policies should require network segmentation isolating, at minimum, the CCSS Trusted Environment (key management and signing infrastructure), client-facing services (trading platform, API endpoints, web application), corporate network (staff workstations, email, productivity tools), and management and monitoring infrastructure. Segmentation should be enforced through firewalls, VLANs, or software-defined networking with explicit allow-list rules between zones. Reference: ISO/IEC 27001:2022 A.8.22; NIST CSF PR.AC-5.

Perimeter Security: Policies should mandate firewall configurations following deny-by-default principles, intrusion detection and/or prevention systems (IDS/IPS) at network boundaries, web application firewalls (WAFs) protecting client-facing services, and regular review of firewall rules to remove stale or overly permissive entries. Reference: ISO/IEC 27001:2022 A.8.20; NIST CSF PR.PT-4.

DDoS Protection: Given the high-profile nature of cryptocurrency exchanges as DDoS targets, policies should address DDoS mitigation measures for all client-facing services, including volumetric attack mitigation (CDN or upstream scrubbing services), application-layer attack detection and rate limiting, and tested failover procedures for DDoS events. Reference: ISO/IEC 27001:2022 A.8.20; NIST CSF PR.PT-4, DE.CM-1.

Secure Remote Access: Where staff or contractors access VASP systems remotely, policies should require encrypted VPN or zero-trust network access solutions, MFA for all remote access, endpoint compliance verification before granting access, and logging of all remote access sessions. Reference: ISO/IEC 27001:2022 A.8.20; NIST CSF PR.AC-3.

DNS Security: Policies should address DNS security controls including DNSSEC where applicable, DNS monitoring for domain hijacking or BGP route manipulation (a known attack vector against cryptocurrency services), and protection against DNS-based attacks targeting customer-facing domains. Reference: ISO/IEC 27001:2022 A.8.20, A.8.21.

Risk if Absent: High

Inadequate network security enables lateral movement from compromised client-facing systems to custody infrastructure. DDoS attacks against exchanges can serve as cover for simultaneous targeted intrusions. DNS hijacking has been used in multiple cryptocurrency exchange compromises to redirect customer traffic and intercept credentials.

4A.10 Incident Response Audit

Auditors should verify that the VASP has established and tested incident response capabilities adequate for the timely detection, containment, and resolution of cybersecurity incidents affecting customer virtual assets. This section complements the incident notification requirements set out in the Virtual Asset Act 2025 Section 61 and the VFSC's incident notification templates (see Appendix F) by testing the VASP's operational capability to detect and respond to incidents in the first instance.

Audit Criteria

Incident Response Plan: Policies should require a documented incident response plan (IRP) covering roles and responsibilities (including escalation paths to executive management and the VFSC), classification criteria for security events and incidents (aligned with the methodology's risk rating framework in Part 2), response procedures for VASP-specific incident types (key compromise, unauthorised transactions, exchange platform breach, smart contract exploit, insider theft), communication procedures (internal, regulatory per VFSC incident notification templates (see Appendix F), customer, and law enforcement), and evidence preservation requirements. Reference: ISO/IEC 27001:2022 A.5.24; NIST CSF RS.RP-1; Virtual Asset Act 2025 Section 61.

Incident Detection Capabilities: The VASP should demonstrate capabilities to detect security incidents in a timely manner, including correlation of security events from multiple sources (network, endpoint, application, blockchain), automated alerting for high-severity events (such as unauthorised signing attempts, anomalous withdrawal patterns, and credential compromise indicators), and on-chain monitoring for suspicious transaction patterns. Reference: ISO/IEC 27001:2022 A.5.25; NIST CSF DE.AE-1 through DE.AE-5.

Incident Response Testing: The IRP should be tested at least annually through tabletop exercises or simulated incidents. Exercises should include threat vectors to the environment defined by the risk audit process. Test results should be documented and used to update the IRP. Reference: ISO/IEC 27001:2022 A.5.24; NIST CSF RS.IM-2.

Post-Incident Review: Policies should require post-incident reviews following any security incident, with documented lessons learned, root cause analysis, and corrective actions. For any incident reportable to the VFSC under the VFSC Virtual Asset Act 2025 Section 61, the post-incident review should be completed and available to the auditor. Reference: ISO/IEC 27001:2022 A.5.27; NIST CSF RS.IM-1.

Evidence Collection and Preservation: Procedures should address forensic evidence collection and preservation in a manner suitable for potential regulatory investigation or legal proceedings. This includes chain-of-custody procedures for digital evidence and preservation of blockchain transaction records relevant to the incident. Reference: ISO/IEC 27001:2022 A.5.28; NIST CSF RS.AN-3.

Risk if Absent: High

The absence of tested incident response procedures increases the likelihood that a security incident will result in greater customer asset loss, delayed regulatory notification, and destruction of forensic evidence. The VFSC's incident notification requirements (see Appendix F) are dependent on the VASP having the capability to detect and assess incidents in the first instance.

4A.11 Vulnerability Management Audit

Auditors should verify that the VASP has implemented ongoing vulnerability management processes to identify, assess, and remediate technical vulnerabilities across all systems within scope. This section complements the third-party penetration testing requirements tested under CCSS V9 2.01 in Part 4, Section 4.7, by addressing the continuous vulnerability management activities between formal audit cycles.

Audit Criteria

Vulnerability Identification and Scanning: Policies should require regular vulnerability scanning of all systems within scope, including external-facing infrastructure (API endpoints, web applications, VPN gateways), internal infrastructure (servers, databases, network devices), and container and cloud infrastructure where applicable. Scanning frequency should be at least monthly for external-facing systems and quarterly for internal systems, with ad-hoc scanning following significant changes. Reference: ISO/IEC 27001:2022 A.8.8; NIST CSF DE.CM-8.

Patch Management: Policies should define patch management procedures with risk-based prioritisation, specifying timelines for remediation: critical vulnerabilities (CVSS 9.0 or above) within 48 hours or with documented compensating controls; high vulnerabilities (CVSS 7.0 to 8.9) within 14 days; medium vulnerabilities (CVSS 4.0 to 6.9) within 30 days; and low vulnerabilities within 90 days. Patch management for systems within the CCSS Trusted Environment should include additional controls to ensure patches do not compromise key material security. Reference: ISO/IEC 27001:2022 A.8.8; NIST CSF PR.IP-12.

Vulnerability Tracking and Reporting: Vulnerabilities should be tracked in a register or vulnerability management platform, with evidence of remediation or documented risk acceptance for vulnerabilities that cannot be patched within the defined timelines. Reporting to management should be at least quarterly. Reference: ISO/IEC 27001:2022 A.8.8; NIST CSF ID.RA-1.

Threat Intelligence and Responsible Disclosure: Policies should address the VASP's approach to monitoring relevant threat intelligence feeds (including blockchain-specific advisories, smart contract vulnerability disclosures, and wallet software security bulletins) and, where the VASP offers public-facing services, a responsible disclosure or bug bounty programme. Reference: ISO/IEC 27001:2022 A.5.7 (Threat intelligence); NIST CSF ID.RA-2.

Risk if Absent: Medium to High

Unpatched vulnerabilities in VASP infrastructure are a primary attack vector. The absence of ongoing vulnerability management between annual penetration tests (tested under CCSS V9 2.01) leaves extended windows of exposure. Cryptocurrency-specific threat intelligence is essential given the frequency and sophistication of targeted attacks against VASPs.

4A.12 Change Management Audit

Auditors should verify that the VASP has implemented formal change management controls for all modifications to systems within or connected to the CCSS Trusted Environment. Changes to custody infrastructure, signing processes, wallet configurations, and blockchain node software carry direct risk to customer assets.

Audit Criteria

Change Control Process: Policies should require a formal change management process for all modifications to systems within or connected to the CCSS Trusted Environment, including risk audit prior to implementation, testing in non-production environments, approval by authorised personnel (with segregation between requester and approver), rollback procedures, and post-implementation verification. Changes to signing configurations, wallet thresholds, or key management systems should require enhanced approval (such as dual authorisation or committee approval). Reference: ISO/IEC 27001:2022 A.8.32; NIST CSF PR.IP-3.

Emergency Change Procedures: Policies should address expedited change procedures for emergency situations (such as critical security patches or active incident response) with appropriate controls to prevent abuse, including retrospective documentation, management review, and post-implementation verification within a defined timeframe. Reference: ISO/IEC 27001:2022 A.8.32.

Change Audit Trail: All changes should be logged with sufficient detail to support audit and forensic investigation, including the identity of the requester and approver, description of the change, date and time of implementation, and evidence of testing and verification. Reference: ISO/IEC 27001:2022 A.8.32; NIST CSF PR.IP-3.

Risk if Absent: Medium

Uncontrolled changes to custody infrastructure are a significant source of operational risk. Inadequate change management has contributed to cryptocurrency losses where wallet configurations were modified without proper testing or approval.

4A.13 Third-Party and Supply Chain Risk Management Audit

Auditors should verify that the VASP has implemented supplier and supply chain risk management extending beyond the CCSS Trusted Environment scope addressed in Part 4, Section 4.9 (CCSS V9 2.03.3). VASPs rely on a broader ecosystem of third-party providers with distinct risk profiles that require dedicated audit.

Audit Criteria

Supplier Risk Audit: Policies should require risk audit of all third parties with access to, or influence over, the security of customer assets or data. This extends beyond the CCSS Trusted Environment vendors (covered in Part 4, Section 4.9) to include blockchain infrastructure providers (node providers, RPC endpoints, block explorers), market data and oracle providers, Travel Rule protocol providers (complementing Section 4A.7), sub-custodians or custody technology providers, AML/CFT screening and transaction monitoring service providers, and cloud service providers (complementing Section 4A.1). Reference: ISO/IEC 27001:2022 A.5.19, A.5.21; NIST CSF ID.SC-2.

Contractual Security Requirements: Agreements with third parties handling sensitive data or providing critical services should include security requirements, right-to-audit clauses, incident notification obligations, and data protection provisions. For sub-custodians or custody technology providers, contractual requirements should address the applicable CCSS V9 controls. Reference: ISO/IEC 27001:2022 A.5.20; NIST CSF ID.SC-3.

Ongoing Monitoring: Policies should require ongoing monitoring of third-party security posture, including review of SOC 2 reports or equivalent assurance where available, monitoring for material changes in the third party's ownership, operations, or security posture, and defined procedures for terminating or transitioning away from a third party whose security is no longer adequate. Reference: ISO/IEC 27001:2022 A.5.22; NIST CSF ID.SC-4.

Concentration Risk: The auditor should assess whether the VASP has identified and documented concentration risks arising from dependence on a single third party for critical services (such as sole reliance on one blockchain node provider, one custody technology platform, or one cloud provider for all infrastructure). Mitigation strategies for identified concentration risks should be documented. Reference: NIST CSF ID.SC-1.

Risk if Absent: Medium

VASP supply chains introduce risks distinct from those in traditional financial services. Compromised blockchain infrastructure providers, oracle manipulation, and sub-custodian failures have resulted in significant losses across the industry. The narrow scope of CCSS V9 2.03.3 does not adequately address the breadth of the VASP supply chain.

4A.14 Secure Software Development Lifecycle Audit

Where the VASP develops its own software (including trading platforms, wallet applications, APIs, or smart contracts), auditors should verify that secure development lifecycle controls are in place. This section extends beyond the smart contract audit requirements in Part 4, Section 4.7 (CCSS V9 2.01) to address the broader software development process.

Audit Criteria

Secure Development Policy: Policies should require secure coding standards appropriate to the development languages in use, code review procedures including security-focused review by personnel other than the original developer, static application security testing (SAST) integrated into the build pipeline, dynamic application security testing (DAST) performed prior to production deployment, and dependency and supply chain scanning for third-party libraries and components. Reference: ISO/IEC 27001:2022 A.8.25, A.8.28; NIST CSF PR.IP-2.

Environment Separation: Development, testing, and production environments should be separated, with controls to prevent unauthorised migration of code to production and to ensure that test environments do not use production data containing real customer information or key material. Reference: ISO/IEC 27001:2022 A.8.31.

Outsourced Development: Where software development is outsourced, the VASP should apply security requirements to the development process, including the right to review source code and security testing results, requirements for secure coding practices, and contractual obligations regarding vulnerability notification and remediation. Reference: ISO/IEC 27001:2022 A.8.30.

Risk if Absent: Medium

Application-layer vulnerabilities in VASP-developed software (exchange platforms, wallet interfaces, APIs) are a primary attack vector for account takeover, unauthorised withdrawals, and data exfiltration.

4A.15 Physical Security Audit

Auditors should verify that the VASP has implemented physical security controls adequate to protect facilities housing critical infrastructure, including server rooms, cold storage vaults, and HSM locations. This section addresses the broader physical security requirements beyond the key ceremony context tested in Part 4, Section 4.12.

Audit Criteria

Physical Access Controls: Policies should define physical security perimeters for facilities housing critical VASP infrastructure, including server rooms, cold storage vaults, and HSM locations. Access should be restricted to authorised personnel using physical access control systems (card, biometric, or combination) with access logging. Visitor access to secure areas should require sign-in procedures, escort requirements, and prohibition of unsupervised access to areas housing key material or critical infrastructure. Reference: ISO/IEC 27001:2022 A.7.1, A.7.2, A.7.6; NIST CSF PR.AC-2.

Environmental Controls: Facilities housing critical infrastructure should have appropriate environmental protections including fire detection and suppression, temperature and humidity control, power protection (UPS and generator backup where warranted), and water and flood detection. Reference: ISO/IEC 27001:2022 A.7.5, A.7.8.

Equipment Security: Policies should address the secure siting and protection of equipment, including positioning of critical equipment to reduce risk from environmental threats and unauthorised access, secure disposal or repurposing of equipment that has held key material (complementing the data sanitisation requirements in Part 4, Section 4.6), and clear desk and clear screen policies for workstations with access to sensitive systems. Reference: ISO/IEC 27001:2022 A.7.7, A.7.8, A.7.10.

Risk if Absent: Medium

Physical security breaches can bypass all logical controls. For VASPs with on-premises cold storage or HSM infrastructure, physical access to these systems could enable key extraction or tampering.

Appendix A: Worked Findings Examples

The following examples illustrate the expected format and level of detail for individual findings documentation:

A.1 Example Finding 1: Inadequate Multi-Signature Enforcement

FINDING 2025-001: Inadequate Multi-Signature Enforcement for High-Value Wallets	
Control Domain:	Wallet Security / Key Management
Risk Rating:	HIGH
CCSS V9 Aspect:	1.02 Wallet Creation
Standards Reference:	CCSS V9 Level I and II; ISO/IEC 27001:2022 A.8.24; NIST CSF PR.AC-4
CONDITION:	The cold wallet holding approximately 80% of customer assets is designed to use a 3-of-5 multi-signer scheme. However, review of transaction records and interviews with key custodians revealed that one of the five key shares is held as a dormant backup and not required for transaction signing in practice. Operational procedures effectively require only 2-of-4 signatures for withdrawals. Sample testing confirmed that a withdrawal of 50 BTC was authorised and executed with only two signatures from senior executives.
CRITERIA:	CCSS V9 Level II requires minimum 2-of-n multi-signer configuration with redundant keys. Best practice for institutional custody requires at least 3-of-5 threshold to provide adequate segregation of duties and collusion resistance.
CAUSE:	Implementation gap. The wallet was correctly configured at 3-of-5, but operational procedures evolved to routinely exclude one key holder for convenience, effectively reducing the threshold. Procedures were not updated to reflect actual practice, and no monitoring exists to detect threshold deviations.
EFFECT/RISK:	The reduced signature threshold significantly weakens controls against insider threat and key compromise. If the two routinely-used key holders collude or their credentials are simultaneously compromised, an unauthorised transfer of the entire cold storage balance could

	occur without detection. Given the value at risk (estimated USD 45M), this represents a material threat to customer assets.
RECOMMENDATION:	(1) Immediately enforce 3-of-5 threshold for all cold wallet transactions. (2) Update operational procedures to require three distinct approvers for withdrawals exceeding defined thresholds. (3) Implement transaction monitoring to alert if fewer than required signatures are attempted. (4) Consider requiring an external participant or independent observer for high-value transfers. (5) Conduct training for all key custodians on proper procedures.

A.2 Example Finding 2: Untested Incident Response Plan

FINDING 2025-002: Incident Response Plan Not Tested	
Control Domain:	Security Operations
Risk Rating:	MEDIUM
CCSS V9 Aspect:	1.05 Key Compromise Protocol
Standards Reference:	ISO/IEC 27001:2022 A.5.24-A.5.28; NIST CSF RS.RP-1, RS.IM-1
CONDITION:	The VASP maintains a documented Incident Response Plan (IRP) dated March 2025 that addresses cybersecurity incidents including key compromise scenarios. However, there is no evidence that the plan has been tested through tabletop exercises or simulated incidents since its creation. Interviews with the designated Incident Response Team members confirmed no drills have been conducted. Additionally, the contact list within the IRP is outdated, listing two former employees who departed in Q2 2025.
CRITERIA:	ISO/IEC 27001:2022 A.5.24 requires that incident response procedures be tested regularly to ensure effectiveness. NIST CSF RS.IM-1 requires that response plans incorporate lessons learned. Industry practice recommends at least annual testing of incident response capabilities.
CAUSE:	Process gap. The organisation prioritised plan documentation but did not establish a schedule for testing and maintenance.

	No owner was assigned responsibility for ongoing plan validation.
EFFECT/RISK:	During an actual security incident, response team members may be unfamiliar with their roles and responsibilities, leading to delays or errors in containment. Outdated contact information could prevent timely notification of key personnel. These factors could extend incident duration and increase potential losses or regulatory non-compliance with notification requirements.
RECOMMENDATION:	(1) Conduct a tabletop exercise within 30 days simulating a key compromise or exchange breach scenario. (2) Update the IRP contact list immediately and establish a quarterly review process. (3) Schedule at least two incident response exercises annually, including one focused on cryptocurrency-specific scenarios. (4) Document lessons learned from each exercise and update procedures accordingly. (5) Assign a named owner responsible for IRP maintenance and testing.

Appendix B: Programme Maturity Aggregation - The Critical Domain Principle

B.1 Purpose

This appendix explains the methodological basis for how the auditor derives an overall programme maturity level from individual domain-level audits under Section 2.6 of this methodology. The Programme Maturity Audit evaluates the VASP's cybersecurity programme across five domains: Governance and Leadership, Risk Management, Control Implementation, Monitoring and Measurement, and Continuous Improvement. Each domain is independently assessed against the five-level maturity model (Initial through Optimised). The question this appendix addresses is how those five domain-level scores are combined into a single overall programme maturity level that informs the supervision level recommendation.

B.2 The Aggregation Problem in Multi-Domain Maturity Models

Any maturity model that assesses multiple domains independently must confront the aggregation problem: how to aggregate potentially divergent domain scores into a single overall level for decision-making. This problem is not unique to cybersecurity. It arises in

capability maturity models across software engineering (CMMI), information security (ISO/IEC 21827 SSE-CMM), and process management (COBIT). The significance of the aggregation method chosen is that it directly determines the supervision level recommendation and, consequently, the regulatory burden placed on the VASP and the level of assurance provided to the VFSC.

In the VFSC context, the consequences of the aggregation choice are particularly acute because the Programme Maturity Audit feeds directly into a regulatory decision with tangible consequences: the supervision level determines the frequency and intensity of formal audits, the reporting burden on the VASP, the cost of regulatory compliance, and the degree of constraint on the VASP's operations. An aggregation method that produces an inflated overall maturity level risks under-supervision of a VASP whose control environment is weaker than the aggregate score suggests. An aggregation method that is overly conservative risks imposing disproportionate regulatory costs on VASPs that are well managed overall but have isolated areas for improvement.

B.3 Common Aggregation Approaches

Three principal approaches to maturity aggregation are used across audit and assurance practice. Each produces a different result when domain scores diverge, and each carries a different risk profile for the regulator.

B.3.1 Arithmetic Mean (Averaging). The simplest approach is to calculate the arithmetic mean of all domain scores. This method treats all domains as equally weighted and produces a central tendency. Its advantage is simplicity and consistency. Its limitation is that it permits strong performance in less consequential domains to mask weakness in domains that are critical to the protection of customer assets. For example, a VASP scoring Level 4 for Governance, Level 4 for Monitoring, Level 3 for Continuous Improvement, Level 3 for Risk Management, and Level 2 for Control Implementation would achieve a mean of 3.2, rounding to Level 3 (Defined). This result obscures the fact that the domain most directly responsible for preventing asset loss is materially weaker than the aggregate suggests.

B.3.2 Modal or Majority Approach. This approach assigns the overall level as the level achieved by the majority of domains. It is sometimes used in frameworks where domains are considered broadly equivalent in importance. Its limitation is similar to that of averaging: it permits a single weak critical domain to be outvoted by stronger but less consequential domains. Using the same example above, the modal level would be Level 3 or Level 4 (depending on how ties are resolved), again masking the Level 2 Control Implementation score.

B.3.3 Critical Domain Anchoring (Weakest Link). This approach anchors the overall maturity level to the lowest score among those domains identified as critical to the programme's primary objective. It does not take the lowest score across all domains indiscriminately; rather, it identifies which domains are most consequential to the

protection of customer virtual assets and ensures that the overall audit cannot exceed the maturity of those critical domains. This is the approach adopted by this methodology.

B.4 Rationale for the Critical Domain Approach

The decision to adopt critical domain anchoring rather than averaging or modal aggregation rests on five considerations, each grounded in established audit and assurance principles.

B.4.1 The Primary Objective is Asset Protection. A VASP's cybersecurity programme exists primarily to protect customer virtual assets from theft, loss, unauthorised access, and compromise. While all five maturity domains contribute to this objective, they do not contribute equally. Governance and Leadership create the conditions for effective security; Continuous Improvement ensures the programme evolves over time. These are important enablers, but they are not the direct line of defence. Control Implementation, the actual deployment and operation of technical and operational controls such as key management procedures, multi-signature enforcement, cold storage architecture, and access controls, is the domain where failure has the most direct and immediate consequences for customer assets. Risk Management is similarly critical because a VASP that cannot reliably identify, assess, and treat risks to its custody environment is unlikely to maintain effective controls as the threat landscape evolves. An aggregation method that permits weakness in these domains to be masked by strength in enabling domains would produce a maturity level that does not accurately represent the VASP's ability to protect customer assets.

B.4.2 Alignment with the Materiality Principle. The critical domain approach is conceptually aligned with how materiality operates in financial and non-financial assurance engagements. Under ISA 450, a material weakness in a specific area cannot be offset by strong performance elsewhere when forming the overall audit opinion. Similarly, under ISAE 3000 (Revised), the practitioner's conclusion on subject matter information must address whether the information is free from material misstatement in all material respects. The ISAE 3000 (Revised) framework, which underpins this methodology, requires the auditor to consider whether exceptions in testing are indicative of a failure in the design or operating effectiveness of controls, rather than treating them as offset by controls that operated effectively. The critical domain approach applies the same logic to the maturity audit: a material weakness in the design or operation of controls (Control Implementation) or in the ability to identify and manage risks (Risk Management) cannot be offset by maturity in governance or monitoring.

B.4.3 Alignment with ISO/IEC 27001 Risk-Based Thinking. ISO/IEC 27001:2022 adopts a risk-based approach to information security management, requiring organisations to identify risks to the confidentiality, integrity, and availability of information and to implement controls that are proportionate to those risks. The standard does not permit an organisation to claim conformity on the basis that it has strong governance if the controls necessary to treat identified risks are not implemented and are not operating effectively. The critical domain approach applies the same risk-based

logic: the maturity level that matters most for regulatory decision-making is the maturity of the domains that directly address the risks to customer virtual assets.

B.4.4 Consistency with the NIST CSF Tiering Model. The maturity model used in Section 2.6 aligns with the NIST CSF Implementation Tiers, which assess an organisation's cybersecurity risk management practices across multiple dimensions. The NIST framework emphasises that an organisation's tier should reflect its actual risk management practices and the degree to which those practices are integrated into its overall risk management processes. The framework does not aggregate by averaging; rather, it considers the weakest aspects of the organisation's risk management practices when assigning an overall tier, particularly where those weaknesses relate to the organisation's ability to manage cybersecurity risk in a manner commensurate with the risk to its operations and assets.

B.4.5 Regulatory Conservatism for Custodial Operations. VASP Cybersecurity Type 2 applicants hold custody of or have access to customer virtual assets. The irreversibility of blockchain transactions means that a successful attack resulting in the transfer of customer assets to an attacker-controlled address is, in the vast majority of cases, unrecoverable. This characteristic distinguishes virtual asset custody from traditional financial services, where transactions can often be reversed, frozen, or recovered through intermediary cooperation. The consequences of a false positive in supervision level assignment (classifying a VASP as lower risk than it actually is) are therefore more severe than in many traditional financial services contexts. This asymmetry favours a conservative aggregation approach that prioritises the domains most directly relevant to preventing irreversible asset loss.

B.5 Identification of Critical Domains

Under this methodology, Control Implementation and Risk Management are identified as the domains that typically represent critical capabilities for VASP Type 2 applicants. The following table sets out the rationale for the classification of each domain.

Maturity Domain	Classification	Rationale
Control Implementation	Critical	Directly encompasses the deployment and operation of technical and operational controls that prevent unauthorised access to customer virtual assets. Includes key management procedures, multi-signature enforcement, cold storage architecture, access controls, and incident response capabilities. Failure in this domain has the most direct and immediate consequences for customer assets.
Risk Management	Critical	Determines whether the VASP can reliably identify, assess, and treat risks to its custody environment. A weak risk management function means

		that even well-implemented controls today may become inadequate as the threat landscape evolves, the business model changes, or new vulnerabilities emerge. Directly underpins the sustainability of the control environment assessed under Control Implementation.
Governance and Leadership	Enabling	Creates the organisational conditions for effective security through executive accountability, policy frameworks, and resource allocation. Essential for long-term programme sustainability but does not directly prevent asset loss in the short term. A VASP with strong governance but weak controls is exposed; a VASP with strong controls but developing governance is operationally protected in the near term.
Monitoring and Measurement	Enabling	Provides the feedback mechanisms (metrics, logging, performance tracking) that allow the organisation to detect control failures and measure programme effectiveness. Important for identifying emerging weaknesses, but a monitoring gap does not itself cause asset loss in the way that a control implementation gap can.
Continuous Improvement	Enabling	Ensures the programme evolves through lessons learned, audit follow-up, and programme refinement. Determines the trajectory of the programme over time but does not represent a direct risk to customer assets in the current audit period.

The classification of domains as critical or enabling is not absolute. The auditor retains professional judgement to reclassify a domain as critical where the specific circumstances of the VASP warrant it. For example, for a VASP operating in a rapidly evolving threat environment or one that has experienced a recent security incident, Monitoring and Measurement may be elevated to critical status if the auditor determines that the VASP's ability to detect and respond to threats is fundamental to the protection of customer assets in the current risk environment. Any such reclassification must be documented with a supporting rationale in the audit report.

B.6 How the Principle Operates in Practice

The critical domain principle operates as follows. Having completed the domain-level maturity audits, the auditor identifies the lowest score among the critical domains

(Control Implementation and Risk Management). The overall programme maturity level is set at the lowest critical domain score. The enabling domain scores are then considered for context: if all enabling domains score below the critical domain floor, the overall level may be adjusted downward at the auditor's discretion, as this may indicate broader programme weakness. If the enabling domains score above the critical domain floor, they do not raise the overall level but may be noted as positive observations in the audit report.

To illustrate, consider the following worked example.

Maturity Domain	Classification	Domain Score
Governance and Leadership	Enabling	Level 4 (Managed)
Risk Management	Critical	Level 3 (Defined)
Control Implementation	Critical	Level 2 (Developing)
Monitoring and Measurement	Enabling	Level 3 (Defined)
Continuous Improvement	Enabling	Level 3 (Defined)
Overall Programme Maturity		**Level 2 (Developing)**

In this example, the arithmetic mean of all domain scores is 3.0, which would suggest an overall maturity of Level 3 (Defined) and a supervision recommendation of Standard to Enhanced. The modal level is Level 3. Under the critical domain principle, however, the overall maturity is Level 2 (Developing) because Control Implementation, a critical domain, scored at Level 2. This produces a supervision recommendation of Enhanced, which more accurately reflects the risk that the VASP's actual control deployment is not yet commensurate with the custodial responsibilities of a licensed VASP.

The practical effect of this result is that the VASP is assigned to enhanced supervision, which includes semi-annual cybersecurity audits, monthly compliance reporting, quarterly management meetings with the VFSC, and a Tier 2 (Standard Audit) at the next annual audit cycle. The VASP would be expected to demonstrate progress in Control Implementation towards Level 3 (Defined) by the next annual audit, in line with the continuous improvement expectations set out in Section 1.2.2 of the methodology. Once the VASP achieves Level 3 across both critical domains and meets the de-escalation criteria in Part 3, it would be eligible for de-escalation to standard supervision.

B.7 Comparison of Aggregation Outcomes

The following table demonstrates how the three aggregation approaches produce different results using the worked example above, and the regulatory consequences of each.

Aggregation Method	Overall Level	Supervision Recommendation	Risk to Regulator
Arithmetic Mean	Level 3 (Defined)	Standard to Enhanced	Under-supervision: the Level 2 Control Implementation score is masked by stronger enabling domains. The VASP receives less scrutiny than its actual

			control deployment warrants.
Modal / Majority	Level 3 (Defined)	Standard to Enhanced	Same as averaging in this scenario. The single critical domain weakness is outvoted by three domains at Level 3 or above.
Critical Domain Anchoring	Level 2 (Developing)	Enhanced	Appropriate supervision: the overall level reflects the genuine state of control deployment. The VASP receives closer regulatory engagement commensurate with the risk posed by its developing control environment.

B.8 Limitations and Professional Judgement

The critical domain principle is a structured approach to aggregation, not a mechanical formula. The auditor retains professional judgement in its application and should consider the following factors when determining the overall programme maturity level.

B.8.1 Proximity of Scores. Where the critical domain score is at the boundary of a maturity level (for example, a domain that meets most but not all characteristics of the next level), the auditor may note this as a mitigating factor in the supervision recommendation, even though the overall maturity level remains anchored to the lower score. This is particularly relevant where the VASP can demonstrate concrete plans and timelines for closing the remaining gap.

B.8.2 Compensating Controls. Where a weakness in a critical domain is partially mitigated by strong performance in another domain or by specific compensating controls, the auditor should document this in the findings report. The compensating control does not change the domain score or the overall maturity level, but it may influence the specific supervision conditions recommended. For example, a VASP with Level 2 Control Implementation but Level 4 Monitoring and Measurement may be better positioned to detect and respond to a control failure than one with Level 2 across both domains, and this distinction may appropriately influence the supervision approach.

B.8.3 Trajectory and Commitment. The direction of travel matters. A VASP that has progressed from Level 1 to Level 2 in Control Implementation over the preceding 12 months, with clear evidence of investment and a credible plan to reach Level 3, presents a different risk profile from one that has stagnated at Level 2 across successive audits. While the overall maturity level remains Level 2 in both cases, the auditor's narrative in the report and the specific supervision conditions recommended may appropriately differ.

B.8.4 VASP Cybersecurity Type 1 Applicants. This methodology applies to VASP Cybersecurity Type 2 applicants (those with custody of or access to customer funds). For VASP Cybersecurity Type 1 applicants (no custody), the identification of critical

domains may differ because the primary risk is not the loss of custodied assets. If the VFSC extends this methodology to VASP Type 1 applicants in future, the critical domain classification should be revisited to reflect the different risk profile.

B.8.5 Documentation Requirement. Regardless of the aggregation outcome, the auditor must document the domain-level scores, the identification of critical domains, the application of the critical domain principle, and any exercise of professional judgement in the findings report. This documentation enables the VFSC to understand the basis for the overall maturity determination and to exercise its own judgment in confirming the supervision level assignment.

Appendix C: Red Flags for Supervision

C.1 Purpose

This appendix identifies fifteen red flags that the VFSC auditor and VFSC supervisory staff should be alert to when assessing VASP licence applicants and conducting ongoing supervision of licensed VASPs. These red flags are drawn from real-world audit observations across the Web3 industry and represent patterns of behaviour or operational characteristics that are strongly correlated with weak cybersecurity posture. The presence of one or more of these red flags does not automatically disqualify a VASP from licensing; however, each flag should prompt the auditor to undertake deeper investigation into the relevant control area and should be documented in the audit findings report. Collectively, these red flags serve as early warning indicators that a VASP may pose elevated risk to its customers' virtual assets and to the integrity of the VFSC's licensing regime.

C.2 Red Flags

Red Flag 1: No written policies or procedures, especially for key management. The absence of documented policies and procedures is one of the most fundamental indicators of an immature cybersecurity programme. Policies establish the organisation's security objectives, risk appetite, and management expectations, whilst procedures translate those objectives into repeatable, auditable processes. Without written key management policies and procedures, there is no authoritative reference against which personnel can verify correct behaviour, no baseline against which an auditor can assess compliance, and no mechanism for ensuring consistency across personnel changes or operational disruptions. A VASP that cannot produce documented key management policies and procedures is operating on an ad-hoc basis, which means that security outcomes are entirely dependent on the knowledge and discipline of individual staff members at any given moment, a condition that is neither sustainable nor verifiable.

Red Flag 2: Cannot provide an inventory of their critical key material. A key material inventory is the foundational artefact upon which all other key management controls depend. If a VASP cannot produce a comprehensive, current inventory of its critical key material, including private keys, seed phrases, key shares, and backup key

material, it cannot demonstrate that it knows what it is protecting. Without this inventory, the VASP cannot verify that all key material is accounted for, that appropriate security controls are applied to each item, that access is restricted to authorised personnel, or that backup and recovery arrangements are complete. The inability to produce this inventory should be treated as a strong indicator that the VASP has not established basic custodial control over the virtual assets entrusted to it by its customers.

Red Flag 3: Cannot provide a list of all personnel who have access to key material. Knowing precisely who has access to key material is a prerequisite for effective access control, segregation of duties, personnel vetting, and incident investigation. If a VASP cannot produce a complete and accurate list of every individual, whether employee, contractor, or founder, who has access to key material, it cannot enforce the principle of least privilege, it cannot ensure that departing personnel have their access revoked, and it cannot identify the scope of exposure in the event of a compromise. This red flag frequently indicates that key material access has been granted informally, without governance oversight, and that the VASP has no reliable mechanism for tracking or revoking access.

Red Flag 4: Have anonymous third parties in key roles on their team, such as developers. The use of anonymous or pseudonymous individuals in roles that could impact the security of key material, particularly software developers, system administrators, and key custodians, is a significant governance and accountability risk. Where team members operate under pseudonyms, the VASP cannot conduct meaningful background checks, cannot enforce legal accountability through employment or contractor agreements, and cannot provide the auditor with evidence that personnel vetting controls are in place. Anonymous developers who write or maintain code that interacts with key material represent an unquantifiable insider threat, as there is no verified identity against which to assess trustworthiness or to pursue recourse in the event of malicious action. This practice is particularly prevalent in decentralised and early-stage Web3 organisations and should prompt the auditor to examine the VASP's personnel security controls in depth.

Red Flag 5: Never had a cybersecurity third-party audit or audit on their systems. A VASP that has never engaged an independent third party to assess or audit its cybersecurity controls has no external validation of its security posture. Internal audits, whilst valuable, are inherently limited by the knowledge and objectivity of the personnel who designed and operate the controls being assessed. Third-party audits including penetration testing, smart contract audits, and cybersecurity programme audits provide an independent perspective that is essential for identifying blind spots, testing assumptions, and validating that controls function as intended under adversarial conditions. The absence of any third-party audit history suggests that the VASP has not invested in verifying its security posture and may have undetected vulnerabilities in its systems and processes.

Red Flag 6: The founders still have access to key material and participate in cold wallet transactions. As a VASP matures and establishes formal operational structures, the continued involvement of founders in operational key management activities, particularly cold wallet transaction signing, represents a governance failure. Founders typically hold executive or board-level roles and their continued access to key material creates concentration risk, undermines segregation of duties, and places critical operational functions outside the oversight of the security operations team. Audit experience has shown that security operations teams are often reluctant to challenge founders on their key material security practices, resulting in a blind spot where some of the most privileged access in the organisation is subject to the least scrutiny. The auditor should verify whether any founder access to key material is formally documented, subject to the same controls as other key custodians, and visible to the security operations function.

Red Flag 7: They have built their own key management system and the software code has not been audited by a third party. Custom-built key management systems carry inherently higher risk than established, well-audited commercial or open-source solutions because they have not been subjected to the same breadth of independent scrutiny and real-world testing. When a VASP develops its own key management system and that code has not been independently audited, the VASP is effectively asking its customers to trust software that has only been reviewed by the people who wrote it. Cryptographic key management is a specialist discipline where subtle implementation errors, such as weak random number generation, improper key derivation, or insecure memory handling, can be catastrophic and may not be apparent through functional testing alone. The auditor should determine whether the VASP's custom key management code has been subjected to independent security code review by a qualified third party and whether all identified issues have been remediated.

Red Flag 8: "Security through hiding it from outsiders" - refusing transparency with auditors due to intellectual property concerns. A VASP that resists providing auditors with access to its systems, code, or architectural documentation on the grounds of intellectual property protection is exhibiting a fundamental misunderstanding of the assurance process. Auditors operate under professional obligations of confidentiality, and non-disclosure agreements can be established to protect legitimately sensitive intellectual property. When a VASP invokes intellectual property as a reason to withhold information from the auditor, the practical effect is to prevent independent verification of security controls, which defeats the purpose of the audit. This behaviour pattern often masks underlying security weaknesses that the VASP does not wish to expose. The auditor should make clear that obstruction of the audit process will be reported to the VFSC and that the inability to verify controls due to restricted access will result in those controls being assessed as not implemented.

Red Flag 9: Hosting their client's key management software within their own infrastructure. Where a VASP hosts key management software provided by a third-party custody or wallet provider within its own infrastructure, the security boundary

between the VASP and its service provider becomes blurred. This arrangement means that the VASP's infrastructure security controls directly impact the integrity of the key management system, and any compromise of the VASP's environment could potentially expose the key management software and the key material it protects. It also complicates the allocation of responsibility for patching, configuration management, access control, and monitoring of the key management system. The auditor should examine the contractual and technical arrangements governing such deployments, verify that responsibilities are clearly delineated, and assess whether the VASP's infrastructure security controls are commensurate with the sensitivity of the key management software it hosts.

Red Flag 10: Security awareness training or content has not been updated in over a year. The Web3 threat landscape evolves rapidly, with new attack vectors, social engineering techniques, and exploitation methods emerging on a continuous basis. Security awareness training that has not been reviewed and updated within the past twelve months is likely to omit coverage of current threats, leaving personnel unprepared for the attack techniques they are most likely to encounter. Stale training content is a particularly acute concern in the Web3 context, where novel attack vectors such as AI-enhanced phishing, supply chain compromises through malicious dependencies, and social engineering attacks targeting key custodians are constantly evolving. The auditor should verify that the VASP's security awareness training programme is reviewed at least annually and that the content reflects current threat intelligence relevant to the VASP's operations.

Red Flag 11: No secure coding techniques training for developers. Software vulnerabilities are a leading cause of Web3 security incidents, and developers who have not received formal training in secure coding techniques are significantly more likely to introduce exploitable flaws into the codebase. This is particularly critical for code that interacts with key material, handles transaction signing, or implements smart contract logic, where a single vulnerability can result in the irreversible loss of customer funds. Secure coding training must be specific to the programming languages and frameworks used by the VASP's development team and should cover common vulnerability classes relevant to Web3, including reentrancy, integer overflow, improper access control, and insecure key handling. The absence of secure coding training for developers indicates that the VASP has not taken reasonable steps to prevent vulnerabilities at the point of introduction, which is the most cost-effective stage at which to address them.

Red Flag 12: Heavy use of AI development tooling and use of AI agents in operational key management activities. The use of AI-assisted coding tools and AI agents in environments that interact with key material introduces a category of risk that many VASPs have not yet adequately assessed. AI coding assistants can generate code faster than development teams can review it, increasing the likelihood that subtle vulnerabilities, including those that may be difficult to detect through standard code review, are introduced into production systems. AI agents with transactional authority, such as those involved in automated trading, rebalancing, or withdrawal processing, can

be manipulated through adversarial inputs (prompt injection) or may produce erroneous outputs (hallucination) that result in irreversible on-chain losses. The auditor should determine the extent to which the VASP uses AI tooling in its development and operational processes, whether the VASP has assessed the risks associated with this usage, and whether appropriate controls, such as mandatory human review of AI-generated code that interacts with key material, are in place.

Red Flag 13: Vague responses to auditor's direct questions regarding key material lifecycle management. When VASP personnel provide evasive, vague, or inconsistent responses to direct questions about how key material is created, stored, used, backed up, and destroyed, this is a strong behavioural indicator of inadequate controls. Personnel who are responsible for managing key material and who operate under well-documented procedures should be able to describe those procedures clearly and consistently. Vague responses may indicate that documented procedures do not exist, that personnel have not been trained, that actual practices deviate from documented procedures, or that the VASP is attempting to obscure weaknesses from the auditor. The auditor should note instances of vague or inconsistent responses and use corroborating evidence, such as documentation review, system inspection, and process observation, to determine whether the vagueness reflects a genuine control deficiency.

Red Flag 14: One person performing multiple roles that impact the security of key material. Segregation of duties is a fundamental security control that prevents any single individual from having sufficient access or authority to compromise the security of key material without detection. When one person performs multiple roles that collectively impact key material security, for example, acting as both a software developer and a key custodian, or serving as both a system administrator and a transaction approver, the effectiveness of segregation of duties is undermined. This concentration of roles creates opportunities for both unintentional error and intentional abuse, and it eliminates the independent verification that segregation of duties is designed to provide. The auditor should examine the VASP's role assignments to identify instances where a single individual holds a combination of roles that could enable them to compromise key material security unilaterally and should assess whether compensating controls are in place where full segregation is not operationally feasible.

Red Flag 15: Heavy use of open-source software and the assumption that someone else is checking the code (the Diffusion of Responsibility principle). Open-source software offers significant benefits in terms of transparency, community review, and cost efficiency. However, VASPs that rely heavily on open-source components, particularly for functions that interact with key material or process transactions without conducting their own due diligence on the security of those components are falling victim to the Diffusion of Responsibility principle: the assumption that because the code is publicly available, someone else must be reviewing it for security issues. In practice, many open-source libraries receive little to no independent security review, and the recent history of supply chain attacks in the Web3 ecosystem (including malicious packages injected into popular repositories) demonstrates that this

assumption is dangerous. The auditor should determine whether the VASP maintains a software bill of materials for its critical systems, whether it has a process for evaluating the security of open-source dependencies before adoption, and whether it monitors those dependencies for newly disclosed vulnerabilities on an ongoing basis.

Appendix D: Audit Findings Report Templates

D.1 Executive Summary Format

The executive summary enables VFSC decision-makers to understand audit outcomes without reading the full report. The template below should be used for all cybersecurity audit reports:

EXECUTIVE SUMMARY TEMPLATE

CONFIDENTIAL - VFSC LICENSING AUDIT
VASP CYBERSECURITY AUDIT REPORT

[Applicant Name] - Class [D/D.1/D.2/D.3/D.4] Licence Application
Audit Period: [Start Date] to [End Date]
Report Date: [Date] Auditor: [Firm Name]

OVERALL AUDIT: [Strong/Satisfactory/Needs Improvement/Deficient/Critically Deficient]
PROGRAMME MATURITY: [Initial/Developing/Defined/Managed/Optimised]
LICENSING RECOMMENDATION: [Recommend/Conditional/Defer/Deny]
SUPERVISION LEVEL: [Standard/Enhanced/Intensive]

D.2 Individual Finding Documentation Format (nonconformity)

Each finding follows the Condition-Criteria-Cause-Effect-Recommendation structure adapted for VASP audits:

Field	Content
FINDING [Number]:	[Descriptive Title]
Control Domain:	[Domain from 8 categories]
Nonconformity Rating:	[Major/Minor/Observation]
CCSS V9 Requirement:	[If applicable]
Standards Reference:	[ISO 27001 control / NIST CSF category / VASP Act section]
CONDITION:	[Factual description of the identified weakness based on evidence gathered]
CRITERIA:	[Applicable standard or requirement against which the condition is measured]
CAUSE:	[Root cause - Process gap / Implementation gap / Design gap / Resource gap / Knowledge gap]

EFFECT/RISK:	[Potential impact on client assets, operations, or compliance]
RECOMMENDATION:	[Specific corrective action to address root cause and mitigate risk]
MANAGEMENT RESPONSE:	[Applicant's response: Agree / Partially Agree / Disagree]
ACTION PLAN:	[Remediation steps with responsible party, target date, evidence of completion]
AUDITOR EVALUATION:	[Acceptable / Acceptable with conditions / Inadequate]

D.3 Report Sections Structure

The complete findings report should include the following sections:

(1) Executive Summary (1-2 pages).
(2) Scope and Methodology (2-3 pages) covering licence class, standards applied, evidence sources, and limitations.
(3) Applicant Overview (1-2 pages) with business description, technology architecture, and key personnel.
(4) Risk Audit Summary (2-3 pages) addressing inherent risk profile and control environment maturity.
(5) Detailed Findings (variable length) organised by control domain with findings in order of significance.
(6) Positive Observations (1 page) noting controls exceeding minimum requirements and areas of strong practice.
(7) Programme Maturity Audit (1-2 pages) with level determination and domain analysis.
(8) Supervision Level Recommendation (1-2 pages) with recommended tier and justification.
(9) Remediation Tracking Matrix (1-2 pages).
(10) Appendices including documents reviewed, personnel interviewed, testing samples, management representation letter, and auditor independence attestation.

D.3.1 Guidance on Positive Observations

Auditors should document areas where the VASP demonstrates strong practice or exceeds minimum requirements. Positive observations contribute to a balanced audit and may support lower supervision intensity recommendations. Examples include existing ISO 27001 or CCSS V9 certifications, implementation of CCSS V9 Level III controls where Level II is minimum, proactive threat intelligence integration, mature incident response capabilities demonstrated through regular exercises, and industry-leading key management practices such as MPC or advanced threshold signatures.

D.4 Evidence Documentation Table

Auditors should maintain a structured record of all documents and artefacts reviewed during the audit. The following table format should be included in the report appendices:

Document/Artefact	Provided	Date/Version	Remarks
Information Security Policy	[Yes/No]	[Version, Date]	[Audit notes]
Key Management Policy	[Yes/No]	[Version, Date]	[Audit notes]
Access Management Policy	[Yes/No]	[Version, Date]	[Audit notes]
Incident Response Plan	[Yes/No]	[Version, Date]	[Audit notes]
Business Continuity Plan	[Yes/No]	[Version, Date]	[Audit notes]
Wallet Architecture Documentation	[Yes/No]	[Version, Date]	[Audit notes]
Key Ceremony Procedures	[Yes/No]	[Version, Date]	[Audit notes]
Latest Penetration Test Report	[Yes/No]	[Date]	[Audit notes]
Latest Vulnerability Scan Report	[Yes/No]	[Date]	[Audit notes]
Smart Contract Audit Report (if applicable)	[Yes/No/N/A]	[Date]	[Audit notes]
Third-Party Certifications (ISO 27001, SOC 2, etc.)	[Yes/No]	[Validity dates]	[Scope and remarks]
Network Architecture Diagram	[Yes/No]	[Date]	[Audit notes]
Risk Register	[Yes/No]	[Last updated]	[Audit notes]
[Additional documents as applicable]			

Appendix E: Auditor Quarterly Assurance Letter Template

The following template shall be used by independent cybersecurity auditors when issuing quarterly assurance letters to the VFSC for VASPs under enhanced or intensive supervision, in accordance with Section 1.2.2.2 of this methodology. The assurance letter provides the VFSC with an independent audit of the VASP's cybersecurity posture, remediation progress, and any emerging concerns between annual audits.

Field	Content
LETTER HEADER	
Letter Title:	Independent Auditor Quarterly Cybersecurity Assurance Letter
Addressee:	The Commissioner, Vanuatu Financial Services Commission
VASP Licensee Name:	[Full registered name]
Licence Number:	[VFSC licence number]
Licence Class:	[D/D.1/D.2/D.3/D.4]
Current Supervision Level:	[Enhanced/Intensive]
Review Period:	[Start Date] to [End Date]
Date of Letter:	[Date]
Auditor Firm:	[Firm name]
Lead Auditor:	[Name, qualifications]
SECTION 1: SCOPE OF REVIEW	
Review Basis:	This review was conducted in accordance with the ongoing auditor responsibilities established in Section 1.2.2.2 of the VFSC Cybersecurity Audit Methodology.
Documents Reviewed:	[List of VASP compliance reports, remediation evidence, and other documents reviewed]
Interviews Conducted:	[Names and titles of VASP personnel interviewed, if any]
Limitations:	[Any limitations on the scope of the review, including documents requested but not provided]
SECTION 2: STATUS OF OPEN NONCONFORMITIES	
Total Open Nonconformities:	[Number from most recent audit]
Remediation Verified This Quarter:	[Number of findings for which remediation has been independently verified]
Remediation On Track:	[Number of findings where remediation is progressing within agreed timeframes]
Remediation Overdue or At Risk:	[Number of findings where remediation is delayed or at risk of missing target dates, with details]
Findings Recommended for Escalation:	[Any findings where the auditor recommends escalation of the risk rating due to inadequate or delayed remediation]
SECTION 3: COMPLIANCE REPORT AUDIT	
VASP Compliance Reports Received:	[Confirm receipt and completeness of quarterly/monthly compliance reports for the review period]
Audit of Report Quality:	[Audit of whether the VASP's compliance reports are accurate, complete, and submitted within required timeframes]
Discrepancies Identified:	[Any discrepancies between the VASP's self-reported information and the auditor's independent audit]

SECTION 4: EMERGING RISKS AND CONCERNS	
New Risks Identified:	[Any new cybersecurity risks identified during the review period that were not present at the last audit or prior quarterly review]
Incidents of Concern:	[Any cybersecurity incidents during the review period that the auditor considers material or indicative of control weaknesses]
Material Changes Assessed:	[Any material changes to the VASP's environment that the auditor has reviewed, and audit of their impact on the cybersecurity control framework]
SECTION 5: ASSURANCE OPINION	
Overall Audit:	[The auditor's overall audit of the VASP's cybersecurity posture for the review period: On Track / Concerns Identified / Significant Concerns]
Summary of Concerns:	[If concerns are identified, a concise summary of the key issues requiring VFSC attention]
Supervision Level Recommendation:	[Whether the current supervision level remains appropriate, or whether the auditor recommends escalation or de-escalation, with rationale]
SECTION 6: AUDITOR ATTESTATION	
Attestation:	This assurance letter has been prepared in accordance with the VFSC VASP Cybersecurity Audit Methodology and represents the independent professional opinion of the undersigned auditor. The review was conducted with due professional care and in compliance with applicable auditing standards.
Lead Auditor Name:	[Name]
Qualifications:	[Professional certifications held]
Signature:	[Signature]
Date:	[Date]

Appendix F: Reference to VASP Reporting Templates

The following VASP-facing reporting templates are contained in the complete VFSC edition of this methodology and are not reproduced in this Independent Auditor Edition:

(a) Cybersecurity Incident Notification Templates (Initial Notification within 24 hours, and Comprehensive Incident Report within 14 days), used by VASP licensees when notifying the VFSC of material cybersecurity incidents.

(b) Material Change Notification Template, used by VASP licensees when notifying the VFSC prior to implementing material changes to their licensed environment.

(c) VASP Quarterly Cybersecurity Compliance Report Template, used by VASP licensees for periodic compliance reporting.

The auditor should be familiar with the content and structure of these VASP reporting templates, as review of the VASP's completed reports forms part of the auditor's ongoing responsibilities under Section 1.2.2.2. Copies of the VASP-facing templates may be obtained from the VFSC upon request.

Please contact the following person should you have any questions:

Mr. Joshua Tari

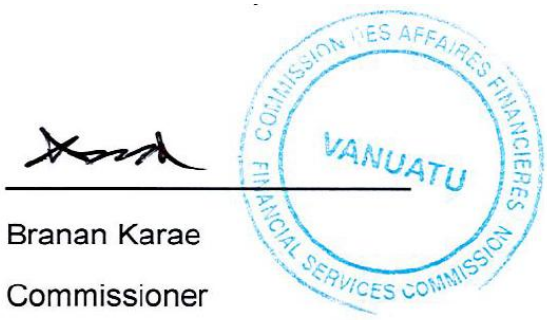
Manager, Supervision Department

Email: tjoshua@vfsc.vu

Phone: (678) 22247

Fax: (678) 22242

Dated this 20th day of March 2026



Branan Karae

Commissioner