VANUATU FINANCIAL SERVICES COMMISSION

Virtual Asset Service Providers Act No. 3 of 2025

CYBERSECURITY REQUIREMENTS FOR VASP APPLICANTS AND LICENSEES

For VASP Cybersecurity Type 2 Applicants

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

Date: March 2026

Derived from the VFSC Cybersecurity Audit Methodology and Findings Report Framework

Developed by SixBlocks Audit for VFSC

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_Requirements_VASP_Applicants_Licensees_Draft_2.docx – draft 2**]** (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

Table of Contents

Part 1: Introduction and Applicability

This document sets out the cybersecurity requirements, obligations, and expectations that apply to Virtual Asset Service Provider (VASP) applicants and licensees under the Vanuatu Virtual Asset Service Providers Act No. 3 of 2025, where the licensed activities involve custody of, or control over, customer virtual assets. It is derived from the VFSC Cybersecurity Audit Methodology and Findings Report Framework, and is provided to assist VASP applicants and licensees in understanding the cybersecurity standards against which they will be assessed, the ongoing obligations they must fulfil, and the reporting requirements they must satisfy.

This document does not replace or override the full VFSC Cybersecurity Audit Methodology, which remains the authoritative reference for the independent cybersecurity auditor and for the VFSC in making licensing and supervisory decisions.

Terminology Note: VFSC Cybersecurity Applicant Types

The VFSC distinguishes between two cybersecurity applicant classifications, 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 document, "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 document applies to VASP Cybersecurity Type 2 applicants and licensees.

Assurance Standard Basis

The VFSC cybersecurity audit is conducted under ISAE 3000 (Revised), the international standard for assurance engagements other than audits or reviews of historical financial information. ISAE 3000 (Revised) supports both reasonable assurance and limited assurance engagements. For VASP cybersecurity licensing audits, reasonable assurance is the default, given the regulatory significance of licensing decisions and the potentially serious consequences of an inappropriate conclusion.

For the initial cybersecurity baseline audit of a VASP applicant, the engagement is a point-in-time assessment ("as at" a specified date) focused on control design and implementation readiness. For ongoing supervision, the engagement is a period-of-time assessment focused on operating effectiveness ("throughout" a defined period), typically covering up to 12 months.

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 will coordinate with the VASP's AML/CFT compliance function to avoid duplication and ensure coherent coverage.

VFSC Cybersecurity Audit Approach

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 Act 2025 + CCSS V9 Level II minimum + ISO/IEC 27001/2 + regulatory expectations
Output	Audit opinion	Examination report with Matters Requiring Attention	Findings report with risk ratings and supervision recommendations

1.1 VFSC-Approved Independent Cybersecurity Auditor

At the time of this report, the VFSC has approved Mr. Marc Krisjanous of Sixblocks Audit as the Independent Cybersecurity Auditor. Mr. Krisjanous is a Certified Cryptocurrency Security Standard (CCSS) Auditor, ISO/IEC 27001 Lead Auditor, NORS Readiness Assessor, and PCI Qualified Security Assessor. He brings 18 years of professional experience in Information Security with 10 years of specialized expertise in auditing.

Mr. Krisjanous may be contacted using the following details:
Telephone: +64 22 370 7990
Email: zaniskiwi@gmail.com
Address: Suite 1, Level 1, iCentre, 50 Manners Street, Wellington 6011, New Zealand

1.2 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 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 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.

1.2.2 Post-Licence Context

This 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.

1.2.3 Audit Scope

The baseline cybersecurity audit covers all VASP products and services in the licence application, including all key material operational cybersecurity controls and supporting operational and governance controls. The audit boundary encompasses all people, processes, and technology components that can directly or indirectly affect the security of key material used by VASP products and services in the licence application.

1.2.4 Evidence Gathering

The audit employs four evidence-gathering techniques:

1. **Review** of documentation, including policies, standards, procedures and Business as Usual (BAU) outputs.
2. **Interviews** with personnel assigned roles that could directly or indirectly impact the security of key material.
3. **Inspection** of control configurations to ensure documented requirements for system configurations are adhered to.
4. **Observation** of processes to ensure personnel follow documented policies and procedures.

1.2.5 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 to achieve a cybersecurity posture sufficient for licensing. It includes a complete list of all Critical and High findings, detailed remediation recommendations, prioritisation guidance, indicative timeframes, and evidence requirements for demonstrating that each finding has been remediated.

Once the applicant has implemented the required remediation actions, the auditor shall verify that each Critical and High finding has been adequately addressed. Upon successful verification, the auditor shall issue a Remediation Verification Letter to the VFSC confirming that the applicant's cybersecurity posture now meets the licensing threshold.

1.2.6 Medium and Low Findings at Baseline

Medium and Low findings identified during the baseline audit do not prevent the grant of a licence. However, the applicant is expected to remediate Medium findings within 60 to 90 days and Low findings within 90 to 180 days following the grant of a licence. Progress on these findings will be monitored through the quarterly compliance reporting process and verified at the first annual audit.

1.3 VASP Licensee Ongoing Obligations

Following the baseline cybersecurity audit and the grant of a VASP licence, the VASP licensee is primarily responsible for maintaining and improving the cybersecurity controls assessed during the baseline audit. The obligations below apply throughout the licence period, with reporting frequency adjusted according to the assigned supervision level.

1.3.1 Compliance Reporting

In accordance with the Virtual Asset Service Providers Act No. 3 of 2025, Section 54, all VASP licensees must submit periodic compliance reports to the VFSC using the template provided in Appendix A of this document. The reporting frequency is determined by the assigned supervision level. From a cybersecurity perspective, each compliance report must address:

1. The status of all open nonconformities and the progress of associated remediation plans.
2. Any cybersecurity incidents that occurred during the reporting period, including root cause analysis and corrective actions taken.
3. Material changes to the people, processes and technology components of the licensed VASP scope, key management architecture, or custody arrangements.
4. The results of any vulnerability scans or penetration tests conducted during the reporting period.
5. Updates to the risk register reflecting new or changed risks.
6. Confirmation that all cybersecurity policies and procedures remain current and have been reviewed within the prescribed cycle.

Standard supervision: Compliance reports must be submitted to the VFSC on a quarterly basis, in accordance with the statutory reporting cycle.

Enhanced supervision: Compliance reports must be submitted on a monthly basis, with sufficient detail to enable the auditor to conduct quarterly desk-based reviews.

Intensive supervision: Compliance reports must be submitted on a weekly or bi-weekly basis as directed by the VFSC, with sufficient detail to enable the auditor to conduct monthly reviews.

1.3.2 Incident Notification

Regardless of supervision level, VASP licensees must notify the VFSC of any material cybersecurity incident within 24 hours of detection, using the templates provided in Appendix B of this document.

A material incident is defined as any event that results in, or could reasonably have resulted in: 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.

The notification must include a preliminary assessment of the incident's scope, immediate containment measures taken, and an estimated timeline for full root cause analysis. A comprehensive incident report must follow within 14 calendar days.

1.3.3 Material Change Notification

VASP licensees must notify the VFSC prior to implementing any material change to their VASP-licensed environment (people, processes and technology components) that could directly or indirectly impact the security of key material managing customer virtual assets,

using the template provided in Appendix C of this document. Material changes include (the examples below are not exhaustive):

1. Changes to the key material management architecture, such as migrating from multi-signature to MPC, implementing single-signer mechanisms, replacing key material management systems and altering fund threshold configurations.
2. Changes to custody arrangements, including onboarding or offboarding of third-party custody providers.
3. Installing the VASP licensees' customers' software within the VASP licensed environment.
4. Significant changes to the technology platform, such as migrating to a new blockchain protocol, adding or changing hosting providers, or deploying a new smart contract system.
5. Changes to the organisational structure that affect security roles, including the departure of the Chief Information Security Officer or equivalent. Note that changes to key persons with cybersecurity responsibilities (CISO, CTO, Chief IT Officer) also trigger the statutory notification requirement under the Virtual Asset Service Providers Act No. 3 of 2025, Section 21, which requires written notice to the Commissioner within 14 days of any change to a key person or their circumstances affecting fit and proper status.
6. Geographic relocation of infrastructure or key material.

The VFSC may require an interim audit or targeted assessment of the changed controls before approving the material change. VASPs must not implement the proposed change until they have received confirmation from the VFSC that it may proceed.

1.3.4 Continuous Improvement Expectations

The VFSC expects licensed VASPs to demonstrate continuous improvement in their cybersecurity posture over successive audit cycles. This expectation is reflected in the Programme Maturity Assessment (see Part 2), 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.

1.3.5 Reporting Frequency Summary

Activity	Standard	Enhanced	Intensive
VASP compliance reporting	Quarterly	Monthly	Weekly or bi-weekly
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
VFSC management meetings	As needed (reactive)	Quarterly	Monthly or more frequently

1.4 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 annual audit 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.

1.4.1 Annual Audit Tiers

The annual cybersecurity audit is conducted at one of three tiers of intensity, aligned with the supervision level categories:

Tier 1: Focused Review (Standard Supervision): Targeted scope focusing on previously identified nonconformities, key management and operational controls, and any material changes since the last audit. Primarily documentary review with targeted interviews. Typical duration: 2 to 3 weeks.

Tier 2: Standard Audit (Enhanced Supervision): Comprehensive scope covering all eight control domains, full CCSS V9 reaudit, and all supplementary control areas. Documentary review, interviews, and inspection of configurations. Typical duration: 4 to 6 weeks.

Tier 3: Comprehensive Audit (Intensive Supervision): All control domains with extended testing procedures and deep-dive into high-risk areas identified by the VFSC. All four evidence-gathering techniques required, with on-site presence required for critical control testing. Typical duration: 6 to 8 weeks.

1.4.2 First Annual Audit Considerations

For all newly licensed VASPs, the first annual audit shall 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.

1.4.3 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). The cybersecurity audit report must be submitted to the VFSC within 30 days of fieldwork completion.

1.4.4 De-Escalation Through Demonstrated Improvement

A VASP may be de-escalated from a higher to a lower supervision level, provided the VASP demonstrates sustained improvement over successive audit cycles. 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 submissions.
5. Independent verification of control improvements by the auditor.
6. Demonstrable improvement in programme maturity level.

De-escalation is not automatic; it requires a formal recommendation from the cybersecurity auditor and approval by the VFSC.

Part 2: Risk Rating and Assessment Framework

This Part explains how the VFSC cybersecurity audit assesses and rates findings, so that VASP applicants and licensees understand the standards against which they are measured and the consequences of identified weaknesses.

2.1 Five-Tier Risk Rating Framework

The 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 the Vanuatu Virtual Asset Service 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 the Vanuatu Virtual Asset Service 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 Control Domains

Audit findings are categorised into eight control domains:

1. **Key Management:** generation, storage, access, usage, and destruction of cryptographic key material.
2. **Wallet Security:** wallet architecture, multi-signature configurations, hot/cold storage segregation.
3. **Access Control:** authentication, authorisation, privilege management, and personnel vetting.
4. **Network and Infrastructure Security:** network architecture, segmentation, perimeter security, DDoS protection, DNS security.
5. **Security Operations:** logging, monitoring, vulnerability management, incident detection.
6. **Business Continuity and Disaster Recovery:** BCP, DR, backup, redundancy, testing.
7. **Third-Party Risk Management:** vendor management, supply chain, custody providers, service providers.

8. **Governance and Compliance:** governance structure, risk management, policies, regulatory compliance.

2.3 Overall Audit Rating

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; intensive supervision (annual audits only)
Critically Deficient (5)	Multiple Critical findings; fundamental inability to safeguard client assets	Conditional licensing; intensive supervision (annual audits only)

Baseline Audits: Only a rating of Strong (1) qualifies for an unconditional licensing recommendation. Ratings of Satisfactory through Critically Deficient all indicate the presence of Critical or High findings, which must be remediated before the initial VASP licence can be granted.

2.4 Programme Maturity Assessment

In addition to individual control findings, auditors evaluate the overall maturity of the VASP's cybersecurity programme. The maturity assessment uses a five-level model aligned with NIST CSF Implementation Tiers:

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; formal risk assessment 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 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

Maturity is assessed across five domains: (1) Governance and Leadership, (2) Risk Management, (3) Control Implementation, (4) Monitoring and Measurement, and (5) Continuous Improvement. The overall programme maturity level is derived using a critical domain anchoring approach, meaning the overall level reflects the lowest domain score among the critical domains (typically Control Implementation and Risk Management), as weaknesses in these domains have the most direct impact on the security of customer virtual assets.

Part 3: Supervision Level Categories

The VFSC adopts a three-tier supervision framework for VASPs. The tiers scale supervisory intensity according to the VASP's risk profile, control maturity, audit outcomes, and supervisory history.

3.1 Standard Supervision (Baseline/Lower Risk)

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

1. Quarterly cybersecurity reporting in accordance with Vanuatu Virtual Asset Service Providers Act No. 3 of 2025, Section 54.
2. Annual independent cybersecurity audit report in accordance with Vanuatu Virtual Asset Service Providers Act No. 3 of 2025, Section 55.
3. Annual independent cybersecurity testing/assurance (e.g., periodic vulnerability assessment/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.

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. In addition to baseline obligations, enhanced supervision includes:

1. 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).
3. Scheduled management engagement (e.g., quarterly meetings) to review remediation status.
4. Targeted on-site inspections where appropriate.
5. Licence conditions specifying remediation milestones, timelines, and evidence requirements.

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. Intensive supervision includes:

1. Close supervisory engagement with frequent reporting (e.g., weekly/bi-weekly).
2. Increased on-site supervisory activity during critical periods.
3. Use of licence conditions or directions to impose risk-mitigations such as restrictions on new onboarding, transaction limits, product/geography constraints, or enhanced custody/controls.
4. Mandatory independent assurance/verification of remediation outcomes for high-impact weaknesses.
5. Escalation to enforcement actions if the VASP fails to remediate or risks remain unacceptably high.

3.4 Risk Score and Tier Placement

Supervision tier placement is determined by a Risk Score calculated as: **Risk Score = Impact Score (1-5) x Probability Score (1-5)**. The Impact Score is derived from the overall audit rating and the Probability Score from the programme maturity assessment.

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

3.4.1 Escalation Triggers

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.

3.4.2 De-Escalation Criteria

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.

Part 4: Cybersecurity Control Requirements

For VASP Cybersecurity Type 2 applicants managing client virtual assets, the 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 requirements across two categories: Cryptographic Asset Management (CCSS V9 aspects 1.01 through 1.06) and Operations (CCSS V9 aspects 2.01 through 2.04), followed by supplementary control areas.

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.

4.1 Key Material Generation (CCSS V9 1.01)

VASPs must ensure that key material is generated securely, maintaining both confidentiality and unpredictable numbers. Requirements include:

- Key material is generated by the actor who will be using it.
- Where automated signing agents use key material generated elsewhere, the key material must be generated within a secure Key Management System, transferred securely, and securely removed from the generation environment.
- A digital signature for the key material generation mechanism must be generated, published, and validated prior to each execution (Level II).
- The methodology for generating key material must be validated prior to use, ensuring software does not restrict values or transmit data to another actor (Level II).
- DRBG compliance with NIST SP 800-90A.
- Key material must be generated on systems with sufficient entropy to prevent bias or deterministic properties.

4.2 Wallet Generation (CCSS V9 1.02)

VASPs must ensure wallets are generated with appropriate security configurations. Requirements include:

- A multi-signer mechanism (e.g., multi-signature or MPC) must be implemented where required by risk assessment.
- Key material redundancy must be maintained so that no single event can destroy all copies of key material required to access funds.
- Key materials must be distributed across geographically separate locations (Level II).
- Key materials for wallets implementing a multi-signer mechanism must be distributed across different entities (Level II).
- A documented wallet generation policy must be in place covering internal policies, procedures, and relevant areas of wallet generation (Level II).

4.3 Key Material Storage (CCSS V9 1.03)

VASPs must ensure key material is stored securely. Requirements include:

- Operational key material must be encrypted at rest using strong encryption (e.g., AES-256) when not in use.
- Backups must exist for all key material used in the wallet (Level II extends beyond operational key material to all key material).
- Backups must be protected against environmental risks; at Level II, backups must be stored in geographically separate locations from operational key material.

- Backups must be protected by access controls that prevent unauthorised access.
- Tamper-evident mechanisms must be implemented on key material backups (Level II).

4.4 Key Material Access (CCSS V9 1.04)

VASPs must maintain formal policies and procedures for granting and revoking access to key material. Requirements include:

- Checklists must cover all tasks completed when personnel vacate or transition into key holder roles, reviewed to ensure least privilege principles.
- All key holder grant/revoke requests must be conducted over Approved Communication Channels (Level II).
- Audit trails must exist for key material grant/revoke actions.

4.5 Key Material Usage (CCSS V9 1.05)

VASPs must ensure the secure use of key material. Requirements include:

- Access to operational key material must require an identifier and at least two distinct types of authentication factors.
- Key material must only be used within the CCSS Trusted Environment, isolated from other operating systems and application processes.
- All individual actors involved in operations with key material must have their references checked, identities verified, and background checks performed prior to being trusted with access.
- All individuals involved in key management operations must complete specific applicable training on hire, before being trusted with access to key material, and annually thereafter.
- Key management roles and responsibilities must be formally acknowledged in writing by each person with access to key material.
- Verification of fund destinations and amounts must be performed via Approved Communication Channels prior to the use of key material (Level II).
- Key material for wallets implementing a multi-signer mechanism must be stored and used on different logical or physical devices.
- Digital signatures must follow best practices for the algorithms implemented by the Key Management System.

4.6 Data Sanitisation (CCSS V9 1.06)

VASPs must ensure the proper removal of key material from digital media. Requirements include:

- A data sanitisation policy and procedure conforming to NIST SP 800-88, defining requirements for sanitising and destroying media that holds key material. All staff with access to key material must have read and understood the policy.
- Audit documentation for media sanitisation events must be maintained.

4.7 Security Tests and Audits (CCSS V9 2.01)

VASPs must engage information security expertise and undergo independent assessment. Requirements include:

- Individuals with information security expertise must be engaged in all stages of the design, development, deployment, and ongoing maintenance of systems providing cryptocurrency functions.

- Regular security assessments including vulnerability and penetration testing must be completed by an independent, qualified third party (Level II). All concerns raised must be evaluated for risk and addressed.
- All smart contract software code versions deployed to production environments must be audited by an external third-party auditor. Audit reports must be accessible to entity stakeholders. All issues with medium or higher severity must be addressed before production deployment.

4.8 Logging and Monitoring (CCSS V9 2.02)

VASPs must maintain comprehensive logging and monitoring. Requirements include:

- Audit trails must exist for actions performed within the CCSS Trusted Environment. At Level II, all actions by all users must be logged and retained for at least one year.
- Audit log information must be periodically backed up to a separate server (Level II).
- Audit logs must be monitored for suspicious activity with alerts generated. At Level II, monitoring must be continuous with real-time alerts.
- Blockchain state monitoring capabilities should be maintained as good practice.

4.9 Governance and Risk (CCSS V9 2.03)

VASPs must maintain appropriate governance and risk management. Requirements include:

- A member of executive management must be responsible for the security of the system and formally acknowledge their responsibilities in writing. Succession arrangements must exist.
- The entity must identify security threats using a threat model with defined controls, reviewed periodically. At Level II, a risk management programme based on industry-recognised standards (e.g., ISO/IEC 27005, NIST SP 800-37) must be implemented.
- Service provider management must be implemented for any vendor or service provider that could impact the security of the CCSS Trusted Environment, including procurement processes and annual review of compliance.

4.10 Key Compromise Protocol (CCSS V9 2.04)

VASPs must be prepared for key compromise scenarios. Requirements include:

- An inventory of all key material must exist, with awareness of which key material is critical.
- A documented Key Compromise Policy (KCP) must cover each classification of key material, detailed compromise response plans using Approved Communication Channels, and identification of actors by role with secondary actors designated.
- The key material inventory must be reviewed at least annually (Level II).
- Key Compromise Policy training and rehearsals should be conducted as good practice.

4.11 Hot/Cold Storage Requirements (VFSC Regulatory)

VASPs must comply with VFSC-specific regulatory requirements for segregation of client virtual assets:

- 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 to 90 days trading volume maximum).

- Insurance coverage of 100% for hot wallet holdings and minimum 50% for cold storage.
- Daily reconciliation between blockchain records, wallet systems, and accounting records.
- Client assets and liabilities must be identified and accounted for separately from each other and from the VASP's own assets and liabilities, in accordance with Virtual Asset Act 2025 Section 62.

4.12 Key Ceremony Procedural Requirements

VASPs must maintain appropriate key ceremony procedures, including:

- **Secure location preparation:** Key generation ceremonies in a controlled environment with restricted access. For Level II, this should be an air-gapped workstation. The environment should be cleared of unauthorised devices before the ceremony.
- **Designated roles and participants:** Formally designated roles including a Ceremony Administrator, Key Custodians, Witnesses, and optionally an External Auditor or Notary.
- **Key share generation and distribution:** Documented threshold configuration, method of share generation, recording method, and immediate secure storage in geographically distributed locations.
- **Audit trail and recording:** Contemporaneous written records signed by all participants, video recording, serial number tracking of hardware devices and tamper-evident materials, and cryptographic attestation of generated public keys.
- **Secure transportation and storage:** Chain-of-custody documentation, tamper-evident packaging, secure courier arrangements, and verification procedures upon receipt.

Part 4A: Supplementary Control Requirements

The following control areas supplement the CCSS V9-specific requirements in Part 4 and address broader information security controls relevant to VASP operations. VASPs must ensure that policies, procedures, and controls are in place for each of the following areas.

4A.1 Cloud Security

For VASPs utilising cloud infrastructure (IaaS/PaaS/SaaS), policies and controls must address: cloud configuration standards (VPCs, security groups, encryption, secure configuration of cloud-native services); identity and access management (MFA, IAM roles, access reviews, API key rotation); shared responsibility model documentation; cloud security monitoring; cloud audit logging forwarded to centralised logging infrastructure; and infrastructure-as-code security where applicable.

Risk if Absent: Medium to High

4A.2 API Security

For VASPs providing APIs, policies and controls must address: authentication and authorisation for all sensitive API endpoints; transport security using TLS 1.2 or higher; input validation and rate limiting; API key management (secure generation, transmission, rotation, revocation); API versioning and deprecation; and webhook and callback security.

Risk if Absent: Medium

4A.3 Endpoint and Mobile Security

Policies and controls must address: endpoint protection (EDR/antivirus, host-based firewalls, full-disk encryption, automated patching, secure configuration baselines); mobile device management where BYOD or corporate mobile devices are used; removable media controls, particularly for systems with access to key material; and privileged workstation controls for workstations used to access the CCSS Trusted Environment.

Risk if Absent: Medium

4A.4 Data Protection and Privacy

Policies and controls must address: data classification (public, internal, confidential, restricted); encryption of sensitive data at rest and in transit; retention and disposal aligned with regulatory requirements; privacy compliance where applicable regulations apply (GDPR, etc.); data breach response; and cross-border data transfer requirements where the VASP operates across jurisdictions.

Risk if Absent: Medium

4A.5 Secure Configuration and Hardening

Policies and controls must address: configuration baselines for all system types referencing industry benchmarks (CIS Benchmarks, DISA STIGs); hardening requirements (disabling unnecessary services, changing default credentials, removing default accounts); configuration management with change control; container and orchestration security where applicable; and database hardening.

Risk if Absent: Medium

4A.6 Human Resources Security

Policies and controls must address: pre-employment screening proportionate to role sensitivity; employment terms including confidentiality obligations and acceptable use; security awareness training at onboarding and annual refreshers covering general security, phishing awareness, and crypto-specific topics; termination and change of role procedures with prompt access revocation; and insider threat programme including monitoring of privileged user activities, segregation of duties for high-value operations, and whistleblowing channels.

Risk if Absent: Medium

4A.7 Travel Rule Data Security

In accordance with FATF Recommendation 16 and Virtual Asset Act 2025 Section 27, policies and controls must address: secure transmission of originator and beneficiary information using encrypted channels; encryption at rest of travel rule data; access controls restricted to authorised compliance personnel; retention and disposal in accordance with AML/CFT record-keeping requirements; counterparty VASP verification before transmitting personal information; and sunrise and sunset risk management for transfers to/from jurisdictions where Travel Rule compliance cannot be verified.

Risk if Absent: Medium

4A.8 Business Continuity and Disaster Recovery

Policies and controls must address: documented business continuity plans covering all critical VASP services with defined RTOs and RPOs, including VASP-specific scenarios (blockchain disruptions, chain forks, oracle failures); disaster recovery for custody infrastructure including wallet recovery procedures, HSM failover, and blockchain node recovery; system backup and recovery for all critical systems and data; redundancy and failover for critical infrastructure; and annual testing and exercising of all plans.

Risk if Absent: High

4A.9 Network and Infrastructure Security

Policies and controls must address: network architecture and segmentation isolating the CCSS Trusted Environment, client-facing services, corporate network, and management infrastructure; perimeter security with deny-by-default firewalls, IDS/IPS, and WAFs; DDoS protection for all client-facing services; secure remote access using encrypted VPN or zero-trust solutions with MFA; and DNS security controls.

Risk if Absent: High

4A.10 Incident Response

Policies and controls must address: a documented incident response plan covering roles, classification criteria, response procedures for VASP-specific incident types, communication procedures (including VFSC notification per Appendix B templates), and evidence preservation; incident detection capabilities with correlation of events from multiple sources and automated alerting; annual incident response testing; post-incident review with documented lessons learned; and evidence collection and preservation procedures.

Risk if Absent: High

4A.11 Vulnerability Management

Policies and controls must address: regular vulnerability scanning (at least monthly for external-facing systems, quarterly for internal systems); patch management with risk-based timelines (Critical CVSS 9.0+ within 48 hours, High CVSS 7.0-8.9 within 14 days, Medium CVSS 4.0-6.9 within 30 days, Low within 90 days); vulnerability tracking and reporting; and threat intelligence monitoring including blockchain-specific advisories.

Risk if Absent: Medium to High

4A.12 Change Management

Policies and controls must address: a formal change control process for all modifications to systems within or connected to the CCSS Trusted Environment, including risk assessment, testing, approval with segregation, rollback procedures, and post-implementation verification; emergency change procedures with retrospective documentation; and a change audit trail.

Risk if Absent: Medium

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

Policies and controls must address: supplier risk assessment for all third parties with access to, or influence over, the security of customer assets or data, extending beyond CCSS Trusted Environment vendors to include blockchain infrastructure providers, oracle providers, travel rule protocol providers, sub-custodians, AML/CFT service providers, and cloud providers; contractual security requirements with right-to-audit clauses; ongoing monitoring of third-party security posture; and concentration risk assessment.

Risk if Absent: Medium

4A.14 Secure Software Development Lifecycle

Where the VASP develops its own software, policies and controls must address: secure coding standards, code review including security-focused review, static and dynamic application security testing, dependency and supply chain scanning; environment separation between development, testing, and production; and security requirements for outsourced development.

Risk if Absent: Medium

4A.15 Physical Security

Policies and controls must address: physical access controls for facilities housing critical VASP infrastructure with access logging; visitor access procedures; environmental controls including fire detection, temperature/humidity control, and power protection; and equipment security including secure disposal of equipment that has held key material.

Risk if Absent: Medium

Appendix A: Periodic Compliance Report Template

The following template shall be used by all VASP licensees when submitting periodic cybersecurity compliance reports to the VFSC in accordance with Virtual Asset Act 2025 Section 54 and the reporting frequency requirements set out in Section 1.3.1 and 1.3.5 of this document. VASPs under standard supervision submit quarterly; VASPs under enhanced supervision submit monthly; VASPs under intensive supervision submit at the frequency directed by the VFSC (weekly or bi-weekly).

REPORT HEADER	
Report Title	VASP Periodic Cybersecurity Compliance Report
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	[Standard/Enhanced/Intensive]
Reporting Period	[Start Date] to [End Date]
Date of Submission	[Date]
Prepared By	[Name, Title]
Approved By	[Name, Title, must be a senior officer or CISO]
SECTION 1: STATUS OF OPEN NONCONFORMITIES	
Finding Reference	[Finding number from most recent audit report]
Original Risk Rating	[Critical/High/Medium/Low]
Control Domain	[One of the eight control domains per Part 2]
Remediation Plan Status	[Not Started / In Progress / Completed / Verified]
Summary of Actions Taken	[Description of remediation steps completed during the period]
Evidence of Remediation	[Documents, configurations, or test results supporting completion]
Revised Target Completion Date	[If original target has changed, state revised date and reason]
SECTION 2: CYBERSECURITY INCIDENTS	
Total Incidents During Period	[Number, or "Nil" if none occurred]
Incident Reference	[Unique identifier, matching any VFSC incident notification submitted]
Date of Detection	[Date]
Incident Category	[Unauthorised access / Key compromise / System disruption / Data breach / IRP activation / Other]

Root Cause Analysis	[Summary of root cause, or "Under investigation" with expected completion date]
Corrective Actions Taken	[Summary of containment and remediation measures]
Current Status	[Resolved / Under remediation / Under investigation]
SECTION 3: MATERIAL CHANGES TO TECHNOLOGY ENVIRONMENT	
Material Changes During Period	[Description of any changes, or "Nil"]
VFSC Prior Notification Reference	[Reference number of Material Change Notification per Section 1.3.3, or "N/A"]
Impact Assessment	[Summary of impact on cybersecurity controls]
SECTION 4: VULNERABILITY AND PENETRATION TESTING	
Vulnerability Scans Conducted	[Number conducted, dates, scope]
Critical/High Vulnerabilities Identified	[Number, summary, and remediation status]
Penetration Tests Conducted	[Number conducted, dates, scope, firm engaged]
Key Penetration Test Findings	[Summary of significant findings and remediation status]
SECTION 5: RISK REGISTER UPDATES	
New Risks Identified	[Description of new risks, or "Nil"]
Risks Closed or Downgraded	[Description with rationale]
Current Top 5 Cybersecurity Risks	[Summary of the five highest-rated cybersecurity risks]
SECTION 6: POLICY AND PROCEDURE CURRENCY	
All Policies Current and Reviewed	[Yes / No; if No, identify overdue policies]
Policies Reviewed This Period	[List of policies reviewed or updated]
Policies Overdue for Review	[List of any policies that have exceeded their prescribed review cycle]
ATTESTATION	
Attestation	I confirm that the information provided in this report is true, complete, and accurate to the best of my knowledge and belief. I understand that providing false or misleading information to the VFSC may constitute a breach of licensing conditions under the Virtual Asset Act 2025.
Name and Title	[Authorised signatory]

Signature	[Signature]
Date	[Date]

Where the VASP is under enhanced or intensive supervision and is required to submit reports more frequently than quarterly, all sections must be completed for each reporting period. Sections with no reportable activity should be completed with "Nil" rather than left blank.

Appendix B: Cybersecurity Incident Notification Templates

The following templates shall be used by all VASP licensees when notifying the VFSC of material cybersecurity incidents. Two templates are provided: (a) the Initial Notification, to be submitted within 24 hours of detection; and (b) the Comprehensive Incident Report, to be submitted within 14 calendar days of detection.

B.1 Initial Notification (24-Hour Requirement)

This template must be completed and submitted to the VFSC within 24 hours of detection of any material cybersecurity incident. The initial notification prioritises speed of reporting over completeness; fields that cannot be fully completed should be marked "Under assessment" and updated in the Comprehensive Incident Report.

NOTIFICATION HEADER	
Notification Title	VASP Cybersecurity Incident Notification, Initial Report
VASP Licensee Name	[Full registered name]
Licence Number	[VFSC licence number]
Licence Class	[D/D.1/D.2/D.3/D.4]
Incident Reference	[Unique reference assigned by the VASP]
Date and Time of Detection	[Date, Time, Time Zone]
Date and Time of Notification	[Date, Time, must be within 24 hours of detection]
Notifying Officer	[Name, Title, Contact Details]
SECTION 1: INCIDENT CLASSIFICATION	
Incident Category	[Unauthorised access to customer virtual assets / Compromise or suspected compromise of key material / Disruption to critical custody or trading systems exceeding 4 hours / Data breach affecting customer personal information / Activation of incident response plan / Other (specify)]
Estimated Severity	[Critical / High / Medium, based on initial assessment]
Incident Response Plan Activated	[Yes / No; if No, explain why activation criteria were not met]
SECTION 2: PRELIMINARY SCOPE ASSESSMENT	
Description of Incident	[Factual description of what occurred, based on information available at time of notification]
Systems Affected	[List of systems, platforms, wallets, or infrastructure components affected or potentially affected]
Customer Assets at Risk	[Estimated value of customer virtual assets at risk or confirmed lost, or "Under assessment"]
Customer Data at Risk	[Description of any personal data affected, or "None identified" / "Under assessment"]

Geographic Scope	[Jurisdictions affected, if known]
SECTION 3: IMMEDIATE CONTAINMENT MEASURES	
Containment Actions Taken	[Description of all containment measures implemented since detection]
Assets Secured or Frozen	[Description of any virtual assets moved to secure storage, transactions halted, or wallets frozen]
Systems Isolated	[Description of any systems taken offline or isolated]
Third Parties Notified	[List of third parties notified (e.g., custody providers, blockchain analytics firms, law enforcement)]
SECTION 4: TIMELINE AND NEXT STEPS	
Estimated Timeline for Root Cause Analysis	[Expected date for completion of root cause analysis]
Comprehensive Report Due Date	[14 calendar days from detection]
Immediate Actions Planned	[Description of next steps in the first 24-72 hours]
External Support Engaged	[Any external incident response firms, forensic specialists, or legal advisers engaged]
ATTESTATION	
Attestation	I confirm that this notification has been submitted within 24 hours of the detection of the incident described above, and that the information provided is true and complete to the best of my knowledge at the time of submission.
Name and Title	[Authorised signatory]
Signature	[Signature]
Date	[Date]

B.2 Comprehensive Incident Report (14-Day Requirement)

This template must be completed and submitted to the VFSC within 14 calendar days of detection. Where the investigation is not yet complete at the 14-day mark, the VASP should submit the report with available information and indicate which sections remain under investigation, providing an expected completion date.

REPORT HEADER	
Report Title	VASP Cybersecurity Incident Report, Comprehensive Report
VASP Licensee Name	[Full registered name]
Licence Number	[VFSC licence number]
Incident Reference	[Same reference as Initial Notification]
Initial Notification Date	[Date the 24-hour notification was submitted]

Date of This Report	[Date, must be within 14 days of detection]
Prepared By	[Name, Title]
SECTION 1: INCIDENT SUMMARY	
Incident Category	[As per Initial Notification, updated if reclassified]
Final Severity Classification	[Critical / High / Medium]
Date and Time of Incident Onset	[If different from detection date]
Date and Time of Detection	[Date, Time, Time Zone]
Date and Time of Containment	[Date, Time]
Date and Time of Resolution	[Date, Time, or "Ongoing"]
SECTION 2: ROOT CAUSE ANALYSIS	
Root Cause	[Detailed description of the root cause]
Attack Vector	[e.g., social engineering, software vulnerability, insider threat, supply chain compromise, misconfiguration]
Contributing Factors	[Environmental, procedural, or human factors that contributed]
Controls That Failed or Were Absent	[Mapped to the eight control domains where applicable]
Controls That Functioned Effectively	[Controls that contributed to detection, containment, or limiting impact]
SECTION 3: IMPACT ASSESSMENT	
Customer Virtual Assets Lost or Compromised	[Value in fiat equivalent and cryptocurrency denominations]
Customer Virtual Assets Recovered	[Value recovered, if any]
Customer Personal Data Affected	[Number of customers affected, categories of data compromised]
Operational Impact	[Duration of service disruption, systems affected]
Financial Impact	[Total estimated financial impact]
Regulatory Impact	[Any regulatory obligations triggered]
Reputational Impact	[Assessment including media coverage and customer communications issued]
SECTION 4: RESPONSE AND REMEDIATION	
Chronological Incident Timeline	[Detailed timeline from onset through detection, containment, eradication, and recovery]

Containment Measures	[Full description of all containment actions taken]
Eradication Measures	[Actions taken to remove the threat from the environment]
Recovery Measures	[Actions taken to restore normal operations]
Customer Communication	[Description of any communications issued to affected customers]
Law Enforcement Engagement	[Whether law enforcement was engaged, jurisdiction, reference numbers]
SECTION 5: REMEDIATION AND PREVENTION	
Immediate Remediation Actions	[Controls implemented or strengthened immediately following the incident]
Long-Term Remediation Plan	[Planned control improvements with responsible parties and target dates]
Lessons Learned	[Key lessons identified from the incident and the response]
IRP Updates Required	[Any updates to the Incident Response Plan identified as necessary]
ATTESTATION	
Attestation	I confirm that this comprehensive incident report has been submitted within 14 days of the detection of the incident described above, and that the information provided is true, complete, and accurate to the best of my knowledge.
Name and Title	[Authorised signatory]
Signature	[Signature]
Date	[Date]

Appendix C: Material Change Notification Template

The following template shall be used by all VASP licensees when notifying the VFSC prior to implementing any material change to their VASP-licensed environment that could directly or indirectly impact the security of key material. This notification must be submitted **before** the proposed change is implemented.

NOTIFICATION HEADER	
Notification Title	VASP Material Change Notification
VASP Licensee Name	[Full registered name]
Licence Number	[VFSC licence number]
Licence Class	[D/D.1/D.2/D.3/D.4]
Notification Reference	[Unique reference assigned by the VASP]
Date of Notification	[Date]
Notifying Officer	[Name, Title, Contact Details]
SECTION 1: CHANGE CLASSIFICATION	
Change Category	[Key management architecture / Custody arrangements / Technology platform / Organisational structure and security roles / Infrastructure relocation / Other (specify)]
Virtual Asset Service Providers Act No. 3 of 2025, Section 21 Notification	[Yes / No; indicate whether this change also triggers the statutory key person notification requirement. If Yes, confirm the Section 21 notification has been or will be submitted within 14 days.]
SECTION 2: DESCRIPTION OF PROPOSED CHANGE	
Current State	[Description of the current arrangement, system, or configuration that will be changed]
Proposed Change	[Detailed description of the proposed change]
Business Rationale	[Explanation of why the change is being made]
Proposed Implementation Date	[Planned date for implementing the change]
Implementation Timeline	[Phased implementation plan, if applicable, with key milestones]
SECTION 3: CYBERSECURITY IMPACT ASSESSMENT	
Control Domains Affected	[Identify which of the eight control domains are affected by the change]
Impact on Key Material Security	[Assessment of how the change directly or indirectly impacts the security of key material]
Impact on Custody Arrangements	[Assessment of impact on the custody of customer virtual assets]

Risk Assessment	[Identification of new risks introduced and assessment of residual risk after planned mitigations]
Mitigating Controls	[Description of controls that will be implemented to mitigate risks]
Impact on Existing Certifications	[Whether the change affects the scope or validity of any existing certifications]
SECTION 4: TESTING AND VALIDATION	
Testing Plan	[Description of testing to be conducted before and after implementation]
Rollback Plan	[Description of the rollback plan if the change causes unforeseen issues]
Independent Review	[Whether independent review or audit of the change has been or will be conducted, and by whom]
SECTION 5: THIRD-PARTY INVOLVEMENT	
Third Parties Involved	[List of any third parties involved in implementing the change]
Third-Party Due Diligence	[Confirmation that due diligence has been conducted on any new third parties]
Contractual Arrangements	[Summary of any new or amended contractual arrangements with third parties]
SECTION 6: SUPPORTING DOCUMENTATION	
Documents Attached	[List of supporting documents attached, e.g., architecture diagrams, risk assessments, testing plans]
ATTESTATION	
Attestation	I confirm that this notification is submitted prior to the implementation of the proposed material change. The information provided is true, complete, and accurate to the best of my knowledge.
Name and Title	[Authorised signatory]
Signature	[Signature]
Date	[Date]

The VFSC will acknowledge receipt of this notification and advise the VASP whether the proposed change may proceed, whether additional information is required, or whether an interim audit or targeted assessment is necessary before implementation. VASPs must not implement the proposed change until they have received confirmation from the VFSC that it may proceed.

Appendix D: Evidence and Documentation Checklist

The following table lists the key documents and artefacts that VASP applicants and licensees should be prepared to provide to the independent cybersecurity auditor. Having these documents current and readily available will facilitate a smooth audit process.

Document/Artefact	Provided	Date/Version	Remarks
Information Security Policy	[Yes/No]	[Version, Date]	
Key Management Policy	[Yes/No]	[Version, Date]	
Wallet Management Policy	[Yes/No]	[Version, Date]	
Access Management Policy	[Yes/No]	[Version, Date]	
Cryptographic Policy	[Yes/No]	[Version, Date]	
Vulnerability Management Policy	[Yes/No]	[Version, Date]	
Patch Management Policy	[Yes/No]	[Version, Date]	
Incident Response Plan	[Yes/No]	[Version, Date]	
Business Continuity Plan	[Yes/No]	[Version, Date]	
Key Ceremony Procedures	[Yes/No]	[Version, Date]	
Latest Penetration Test Report	[Yes/No]	[Version, Date]	
Latest Vulnerability Scan Report	[Yes/No]	[Version, Date]	
Latest Smart Contract Audit Report (if applicable)	[Yes/No]	[Version, Date]	
Third-Party Certifications (ISO 27001, CCSS, SOC 2, etc.)	[Yes/No]	[Version, Date]	
Network Architecture Diagram	[Yes/No]	[Version, Date]	
Cybersecurity Risk Register	[Yes/No]	[Version, Date]	
Change Management Policy	[Yes/No]	[Version, Date]	
HR Security Policy	[Yes/No]	[Version, Date]	
Service Provider Management Policy	[Yes/No]	[Version, Date]	
Travel Rule Data Security Policy	[Yes/No]	[Version, Date]	
Cloud Security Policy (if applicable)	[Yes/No]	[Version, Date]	
Secure Software Development Policy (if applicable)	[Yes/No]	[Version, Date]	
Log and Monitoring Management Policy	[Yes/No]	[Version, Date]	

Data Sanitisation Management Policy	[Yes/No]	[Version, Date]	
Data Classification Management Policy	[Yes/No]	[Version, Date]	
Security Audit Policy	[Yes/No]	[Version, Date]	

Please contact the following person should you have any questions:

Mr. Joshua Tari

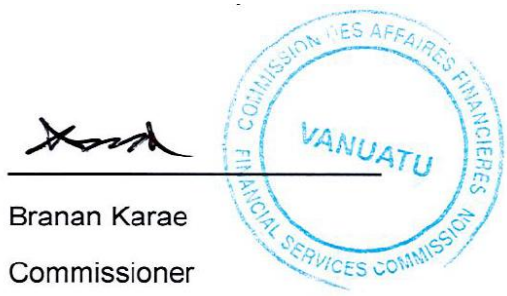
Manager, Supervision Department

Email: tjoshua@vfsc.vu

Phone: (678) 22247

Fax: (678) 22242

Dated this 20th day of March 2026



Branan Karae

Commissioner