MASTER OPERATIONAL STANDARD: SFS-22458

THE SOVEREIGNTY FIDUCIARY STANDARD (SFS) OPERATIONAL BLUEPRINT

Enterprise Controls for Fiduciary De-Linking, Operational Isolation, and Corporate Insider Threat Audit

DOCUMENT CONTROL MASTER REGISTER	
Document Series:	ISO-SFS-22458 (Modules 01 – 04)
Master Title:	Sovereignty Fiduciary Standard Operational Blueprint
Jurisdictional Ref:	Crimes Act 1900 (NSW) Div 6A; Corporations Act 2001 (Cth) s 180; Succession Act 2006 (NSW) s 60; AML/CTF Act 2006 (Cth) s 32
International Ref:	ISO 22458:2022; ISO 37301:2021; ISO 31000:2018
Document Owner:	Chief Risk Officer / Sovereignty Fiduciary Standards Board
Classification:	Public / Enterprise Regulatory & Compliance Standard
Effective Date:	26 July 2026

ANNEXURE A: MODULE 01

STANDARD OPERATING STANDARD: ISO-SFS-22458-MOD01

FIDUCIARY DE-LINKING & SOVEREIGNTY BINDING COVENANT

Document Control Field	Standard Specification
Document ID	ISO-SFS-22458-MOD01
Normative References	ISO 22458:2022 (Cl 4.3, 5.2): FAAA Code of Ethics (St 3); Corporations Avct 2001 9Cth) s 180
Classification	Public / Enterprise Regulatory & Compliance Standard
Effective Date:	26 July 2026

1.0 Control Objective

To establish mandatory fiduciary de-linking controls that insulate an autonomous adult client from familial coercion, un-documented financial extraction, and unauthorised asset access.

2.0 Normative Requirements (Mandatory "SHALL" Statements)

2.1 Separation and Isolation Controls

- **2.1.1** Accredited practitioners **SHALL** conduct all primary client discovery, estate planning executions, and trust distribution sign-offs with the adult individual completely alone.
- **2.1.2** The physical or digital presence of third-party family members, chaperoning parents, or marital partners **SHALL** be excluded during primary assessment windows.
- **2.1.3** Practitioners **SHALL** deploy federal regulatory compliance checks (KYC/AML beneficial ownership rules) as an absolute professional shield ("Friction by Design") to isolate the client without triggering domestic retaliation.

2.2 Digital Perimeter Isolation

- **2.2.1** Practitioners **SHALL** verify that online banking access, digital signing certificates, and advisory communication channels use biometric authentication tied exclusively to the client's personal device.
- **2.2.2** Practitioners **SHALL NOT** disclose asset values, statement trends, or estate

adjustments to any family member without the client's explicit, uncoerced, digitally recorded mandate.

- **2.2.3** If the client's physical identity documentation is flagged as withheld by a family network, the practitioner **SHALL** execute the Document Retrieval Protocol under Module 03.

2.3 Proxy Directorship Veto & Loan Documentation

- **2.3.1** Practitioners **SHALL** refuse to draft, authorize, or support any family trust deed, company directorship, or guarantor arrangement where the client is utilized as an uncompensated or un-consulted corporate proxy.
- **2.3.2** Where capital transfers have occurred between parent and adult child, practitioners **SHALL** mandate the execution of Documented Family Loans to legally destroy the legal *Presumption of Advancement*, insulating client capital from historical family clawbacks.

3.0 Audit Evidence Register

ISO Control Clause	Mandatory Evidence Required	Retention Period
ISO 22458 Cl 4.3 *(Inclusive Service Design)*	Signed Separation Protocol Audit File Note (Isolated Interview)	7 Years
ISO 22458 Cl 5.2 *(Leadership & Governance)*	Biometric Device Verification Token & Single-Name Account Registry	7 Years
ISO 37301 Cl 8.1 *(Operational Control)*	Executed Family Loan Agreement & ASIC Form 370 Duress Affidavit	Permanent

ANNEXURE B: MODULE 02

STANDARD OPERATING STANDARD: ISO-SFS-22458-MOD02

THE SEPARATION PROTOCOL (KYC/AML OPERATIONAL MANUAL & FAQS)

Document Control Field	Standard Specification
Document ID	ISO-SFS-22458-MOD02
Normative References	ISO 22458:2022 (Cl 6.2): AML/CTF Act 2006 (Cth) s 32; **Crimes Act 1900** (NSW) Div 6a
Classification	Restricted / Professional Operational Manual
Effective Date:	26 July 2026

1.0 Control Objective

To provide frontline advisers, bankers, financial brokers and legal officers with calibrated operational workflows and Prescribed Awkward Questions (PAQs) to safely separate vulnerable adult clients from chaperoning family handlers.

2.0 Operational Isolation Workflow

ISO-MOD02 ISOLATION WORKFLOW
Phase 1: Pre-Meeting Communication Lockdown └— Dispatch automated notice citing AML/CTF beneficial ownership rules.
Phase 2: Threshold Pivot (PAQ Friction Script) └— Execute mandatory physical separation at consultation threshold.
Phase 3: Forensic Diagnostic Audit └— Execute calibrated PAQs to screen for credential and liquidity theft.

3.0 Prescribed Diagnostic Enquiries (Forensic Audit Script)

Practitioners **SHALL** integrate these questions naturally into isolated fact-find dialogue:

Diagnostic Category	Prescribed Diagnostic Enquiries (PAQs)
Category 1: Credential & Identity Audit	• *"When updating online banking passwords or accessing MyGov, do you log in directly on your phone, or does another family member hold those access tokens?"* • *"If you decided to go on a spontaneous holiday tomorrow, do you have immediate physical possession of your passport and birth certificate, or are those stored by your parents?"*
Category 2: Liquidity & Revenue Dispersal	• *"Once your salary is paid by your employer, do you maintain total discretionary control over every dollar, or are you required to transfer sums into family-managed accounts?"* • *"If a personal emergency arose today, do you have immediate, un-monitored cash liquidity to pay for it yourself, or would you need to ask a family leader to release funds?"*
Category 3: Social & Career Veto	• *"Outside work hours, are you free to socialize with colleagues, pursue friendships, and seek private medical counsel, or does your family restrict these activities?"* • *"Regarding your career path (such as a placement in border security, logistics, or a corporate directorship), was this choice entirely your own ambition, or did your family structure mandate this position?"*

4.0 Non-Compliance Action Plan (Triage)

If diagnostic responses indicate **Credential Confiscation**, **Zero Personal Liquidity**, or **Autonomy Bifurcation**, the practitioner **SHALL**:

1. Log a **"Sovereignty Exception"** in secure CRM file notes, excluding these entries from shared client portals.
2. Assist the client in establishing an independent **Shadow Account** with digital-only statements routed to a newly created, biometric-secured email address.
3. Initiate confidential referrals to free Australian legal infrastructure (**Anti-Slavery Australia** or **My Blue Sky**).

ANNEXURE C: MODULE 03

STANDARD OPERATING STANDARD: ISO-SFS-22458-MOD03

100-POINT AUTONOMY KIT & DOCUMENT RETRIEVAL PROTOCOL

Document Control Field	Standard Specification
Document ID	ISO-SFS-22458-MOD03
Normative References	ISO 22458:2022 (Cl 7.1): Passports Act 2005 (Cth); Succession Act 2006 9NSW) s 60
Classification	Public / Client Autonomy Standard
Effective Date:	26 July 2026

1.0 Control Objective

To establish an objective 100-Point assessment framework and administrative recovery protocols for replacing withheld primary identity documents and insulating clients from coerced debt.

2.0 100-Point Financial Autonomy Scoring Matrix

100-POINT AUTONOMY ALLOCATION MATRIX
Category A: Primary Accounts & Access (40 Points) [20 Pts] Shadow Liquidity: Single-name account at an independent bank. [20 Pts] Credential Control: Private biometric logins / unshared MyGov access.
Category B: Primary Documentation (40 Points) [20 Pts] Passport Custody: Physical possession of international passport. [20 Pts] Civil Registry: Birth certificate / citizenship papers in hand.
Category C: Social & Structural Veto (20 Points) [10 Pts] Comms Perimeter: Independent mobile contract / zero tracking apps. [10 Pts] Fiduciary De-linking: Independent Will / revoked parental EPOA.
Total Score Range: • 80 – 100 Points: HIGH AUTONOMY (Low Servitude Risk) • 50 – 79 Points: MODERATE RISK (Partial Financial Lockdown)

• 0 – 49 Points: CRITICAL RISK (High Intrafamilial Servitude)

3.0 Identity Retrieval Protocol (Bypassing the Identity Lock)

Where family members withhold primary identity documentation, the client **SHALL** execute an administrative bypass:

1. **Registry Replacement Application:** Apply directly to the state Registry of Births, Deaths and Marriages (BDM) for a replacement birth certificate, selecting domestic coercion criteria for expedited processing.
2. **Passport Security Bypass:** Report the existing physical passport as inaccessible due to extreme domestic circumstances directly to the Australian Passport Office (APO). This invalidates the family-held document and triggers independent issuance to a secure collection point.

4.0 Coerced Debt Insulation & Protection Pathways

- **Credit Bureau Ban:** The client **SHALL** place a permanent ban/fraud alert on credit files via Equifax, Illion, and Experian to prevent family members from fraudulently opening credit facilities.
- **ASIC Corporate Resignation:** The client **SHALL** lodge an ASIC Form 370 directly with the regulator to resign as a director/guarantor of coerced family trust entities, citing duress.
- **Free National Safeguard Pathways:**
  - **Anti-Slavery Australia (ASA):** Confidential legal advice regarding domestic servitude (antislavery.org.au).
  - **My Blue Sky:** Dedicated support for relational coercion and forced marriage (myblueskyorg.au).
  - **National Debt Helpline:** Free financial counseling (1800 007 007) for coerced loans.

ANNEXURE D: MODULE 04

STANDARD OPERATING STANDARD: ISO-SFS-22458-MOD04

COGNITIVE ASSET SABOTAGE (CAS) & INSIDER THREAT AUDIT

Document Control Field	Standard Specification
Document ID	ISO-SFS-22458-MOD04
Normative References	ISO 22458:2022 (Cl 6.2): ISO 37301:2021 (Cl 8.1); Corporations Act 2001 (Cth) s 180
Classification	Public / Client Autonomy Standard
Effective Date:	26 July 2026

1.0 Control Objective

To establish organisational risk screening for identifying and mitigating insider threat vulnerabilities caused by Cognitive Asset Sabotage (CAS), directed career placement, and coerced business / corporate directorships.

2.0 Enterprise Screening Matrix (CAS Audit)

Risk Officers **SHALL** evaluate employees in sensitive placements (e.g., border security, logistics, banking treasury) against these indicators:

Risk Indicator Category	Specific Behavioural and Administrative Triggers	Threat Level
Directed Career Placement	• Recruitment channels or reference contacts are managed or chaperoned by senior family members. • Candidate exhibits zero personal ambition for the sector, but family figures hold deep commercial interests in that domain.	🔴 **CRITICAL** (Insider Threat Risk)

Credential Interception	• Corporate payroll destination is routed to a joint account or family-managed entity. • Corporate IT monitoring logs show employee logins to secure networks occur simultaneously from distinct geographic locations.	🟠 **HIGH** (Compliance Fraud)
Autonomous Veto Collapse	• Employee exhibits high professional capability in isolation, but collapses into submissive or anxious behaviour when family members enter the workplace perimeter. • Employee routinely refuses promotions or interstate travel due to unexplained family limitations.	🟠 **HIGH** (Bonsaied Child Dynamic)
Proxy Directorship Risk	• Employee holds formal directorships or guarantor statuses on external family trust registries, but possesses zero knowledge of the assets or liabilities held within those entities.	🔴 **CRITICAL** (ASIC Governance Breach)

3.0 Governance Remediation Protocols

Where an audit confirms an employee is operating under vertical family coercion, the Board **SHALL** execute immediate remediation:

1. **Access Quarantine:** Revoke solo security clearances for high-risk infrastructure zones (such as border management databases or treasury authorization channels), enforcing a mandatory "two-person rule".

2. **Payroll Diversion Firewall:** Mandate that corporate salary payments be deposited exclusively into a single-name bank account verified via biometric identity checks.
3. **ASIC Directorship Severance:** Facilitate the immediate lodgement of an ASIC Form 370 stating duress to legally sever corporate liability.
4. **Regulatory Disclosure:** Notify relevant regulators (ASIC, AUSTRAC, or Australian Federal Police) if family handlers have weaponized employee credentials, shifting criminal liability directly onto the shadow family handlers.