NOVEMBER 5, 2025

FINANCIAL STRESS TESTING AND CONTINGENCY PLANNING MANUAL

Framework for Resilience: Liquidity, Risk Mitigation, and Operational Continuity under Volatile Conditions."

CREATED BY

EUSL AB

Care to Change the World

Table of Contents

Financial Stress Testing and Contingency Planning Manual

These Chapters are issued under the GSIA Charter and shall be read consistently with Documents 00–09 and Chapter 1 of this Manual. They operationalise counterparty and political risk controls and continuity-of-operations arrangements for programmes executed by GSIA AB under SLA and for Hosted Ownership portfolios operated through EUSL or other approved SPVs. The prevalence order remains in force. Publication is treated as a control subject to lawful redaction and reasoned, time-limited exceptions. Data-protection roles (controller/processor), DPIA triggers, IAM, logging, and encryption apply. Domestication gates and readiness certification govern the staged transfer of systems and mandates. Hosted Ownership is ring-fenced with non-attachment, negative pledge, discrete ledgers and bank accounts, and a reversion covenant without private distribution.

Chapter 1 — Liquidity and FX Risk Management

Preamble and Applicability. This Manual operationalises treasury risk management for GSIA-mandated programmes and projects executed by GSIA AB under SLA, and for Hosted Ownership portfolios operated through EUSL or other approved SPVs. It shall be read with the prevalence order affirmed in prior documents, with fiduciary controls, publication doctrine, data-protection roles, and domestication gates fully applicable. The purpose is to maintain sufficient liquidity, preserve purchasing power across currencies, and ensure continuity of obligations without exposure to speculative risk.

1.1 Governance and Separation of Duties. The GSIA SCE sets treasury policy by reasoned resolution. GSIA Holding AB maintains canonical standards, cash-flow modelling templates, hedging policy instruments, and counterparty due-diligence taxonomies. GSIA AB executes day-to-day treasury operations under SLA within authority matrices that enforce four-eyes control, segregation of front, middle, and back office functions, calibrated countersignature thresholds, and discrete ledgers and bank accounts per project. Hosted Ownership SPVs adopt identical controls, customised to ring-fenced perimeters and negative pledge obligations.

1.2 Treasury Objectives and Prohibitions. Objectives are to ensure timely settlement of obligations, maintain prudent liquidity buffers aligned to risk and tranche schedules, match currency of funding to currency of obligations where feasible, hedge material FX exposures, and avoid value leakage. Speculation is prohibited. Hedging is permitted solely for risk reduction, proportionate to documented exposures, and is executed under approved instruments and limits.

1.3 Ring-Fencing and Bank Architecture. Each programme or Hosted Ownership project maintains discrete bank accounts with unique signatory matrices, separate statements, and dedicated sub-ledgers. A negative pledge prohibits pledging project cash or receivables as collateral for unrelated liabilities. Non-attachment clauses prevent third-party claims outside the project perimeter. Cash waterfalls and escrow constructs are defined in SLAs, Implementation Agreements, or Leasing Schedules, with step-in rights preserved for fiduciary breaches.

1.4 Liquidity Buffer and Coverage Metrics. A minimum liquidity buffer is maintained at a level determined by risk class and tranche cadence, ordinarily not less than ninety days of forecast net cash outflows for operating expenditures and critical commitments. A Liquidity Coverage Ratio and a Net Stable Funding-style measure are computed monthly on a look-forward basis, incorporating expected

donor or Member inflows, conditionality, and tranche gates. Shortfalls trigger pre-defined management actions, including drawdown of committed facilities, re-profiling of non-critical spend, or convening the SCE Committee for contingency measures.

1.5 Forecasting and Stress Scenarios. Rolling thirteen-month cash-flow forecasts are maintained, updated monthly, and aligned to procurement plans, MEL-linked tranche conditions, and domestication milestones. Stress testing applies deterministic and stochastic scenarios encompassing delayed inflows, accelerated disbursements, cost inflation, and FX shocks across relevant currency pairs. Results are reasoned, recorded, and drive buffer calibration, hedge ratios, and contingency triggers. Hosted Ownership projects conduct scenario-specific stress tests prior to each major financing tranche and prior to title reversion.

1.6 FX Risk Identification and Netting. FX exposures are identified by currency of committed obligations versus currency of funding, with timing buckets and sensitivity to market rates. Natural hedging through currency matching between inflows and outflows is prioritised. Net exposures are computed after permissible netting and internal matching; residual material exposures are hedged under policy.

1.7 Hedging Policy and Instruments. Approved instruments include deliverable forwards, non-deliverable forwards where necessary, and plain-vanilla options for asymmetric risk where justified by scenario analysis. Complex or leveraged products are prohibited. Hedge tenors align to exposure timing; over-hedging beyond documented exposure is prohibited. Counterparties must meet defined credit standards and documentation requirements. Hedge effectiveness is monitored; ineffectiveness is investigated and reported.

1.8 Counterparty Limits and Due Diligence. Treasury transactions are executed only with approved counterparties that satisfy due-diligence standards on credit quality, sanctions screening, legal capacity, and operational resilience. Concentration limits apply by counterparty and jurisdiction. Where a Member's sovereign rules require state banks, additional mitigants are documented, including reduced tenors, collateralisation where lawful, or backup counterparties. Counterparty breaches or watchlist events trigger enhanced monitoring or suspension.

1.9 Authority Matrices, Approvals, and Records. Authority matrices define initiation, validation, and approval roles for payments, investments, and hedges. Four-eyes approval and segregation of front, middle, and back office functions are mandatory. All transactions are recorded contemporaneously, reconciled to bank statements at least monthly, and subject to independent review. System access follows least-privilege IAM with multi-factor authentication; activity logs are immutable and time-synchronised.

1.10 Investment of Surplus Cash. Surplus cash, if any, is invested only in short-term, highly liquid, capital-preserving instruments permitted by policy and lawful in the relevant jurisdiction. Investments must be callable without undue penalty to support programme liquidity. Yield maximisation is not an objective and shall not compromise safety or availability. Investment decisions follow the same authority matrices and four-eyes doctrine.

1.11 Publication and Transparency. Treasury policy, risk limits, and summary liquidity and FX risk dashboards are published with lawful redaction. Sensitive identifiers, bank details, and hedging counterparties may be redacted for security. Deferrals for security or market-sensitivity reasons are time-limited and reasoned, with sunset review. Internal detailed reports are made available to the SCE Committee and relevant Member authorities under access controls.

1.12 Data-Protection and Security. Where treasury data includes personal data, controller/processor roles are confirmed; GSIA AB and vendors act as processors under a DPA. DPIAs are triggered for high-risk processing or cross-border transfers. Encryption in transit and at rest, secure key management, immutable logs, and periodic access reviews are mandatory. Incident detection leads to escalation under the Compliance, Audit, and Ethics Code and to notification to the controller within statutory timelines.

1.13 Hosted Ownership Specifics. Hosted Ownership treasury is operated within ring-fenced accounts and ledgers, with cash waterfalls aligned to Leasing Schedules and Implementation Agreements. Escrow arrangements secure reversion mechanics. No private distribution of value is permitted beyond agreed service consideration. Prior to title reversion, a treasury readiness assessment confirms account transfers, signatory changes, systems handover, and legal localisation of banking arrangements.

1.14 Domestication Gates and Handover. At shadowing, Member personnel observe treasury processes and controls. At dual-key, joint approvals apply to defined payment types and hedges. At lead-role, the Member assumes day-to-day execution with GSIA oversight. System handover transfers documentation, models, keys, and banking mandates; legal localisation replaces foreign-law instruments as required. Readiness certification is contingent on sustained control performance, reconciliations without material defects, and demonstrated capacity to manage liquidity and FX risks.

1.15 KRIs, Escalation, and Interfaces. Key risk indicators include buffer breaches, unreconciled items, repeated forecast variances, counterparty limit breaches, hedge ineffectiveness, and FX loss thresholds. Breaches trigger escalation per Document 17's risk taxonomy and escalation protocols. Interfaces are maintained with Document 11 for sanctions screening and ethics, with Document 12 for digital trust controls over treasury systems, with Chapter 5 of this Manual on insurance and hedging instruments, and with the Unified MEL Framework where tranche logic is linked to financial readiness.

1.16 Records, Survivals, and Audit. Treasury records, models, reconciliations, hedge documentation, authority matrices, and approvals are archived for the longer of Charter, statutory, or covenant periods. Survivals include audit rights, confidentiality, data-protection obligations, and IP in models and templates. Internal Audit conducts periodic treasury audits; External Audit opines per applicable standards; independent validators may be commissioned under Document 09.

Chapter 2 — Counterparty and Political Risk

2.1 Purpose and Scope. This Chapter establishes the standards, authority matrices, and escalation protocols for identifying, assessing, mitigating, and monitoring counterparty and political risks that may compromise liquidity, payments, custody, FX operations, procurement execution, information security, or project continuity. It binds GSIA SCE organs, GSIA Holding AB as standard-setter, GSIA AB as operator under SLA, and Hosted Ownership SPVs within their ring-fenced perimeters, as well as contracted financial institutions, custodians, vendors, and implementing partners.

2.2 Governance and Separation of Functions. The GSIA SCE, acting through its Risk and Treasury Committees, approves counterparty eligibility criteria, political-risk tolerances, watchlist triggers, and escalation thresholds. GSIA Holding AB maintains canonical counterparty due-diligence taxonomies, beneficial-ownership disclosure standards, sanctions screening matrices, political-risk heatmaps, and continuity playbooks. GSIA AB executes onboarding, KYC/KYB, sanction screening, ongoing surveillance, and exposure monitoring within an authority matrix that enforces four-eyes approvals, segregation of duties, and calibrated countersignature thresholds. Hosted Ownership SPVs mirror these controls, adapted to project perimeters and sovereign constraints.

2.3 Counterparty Categorisation and Eligibility. Counterparties are categorised by function (banking, custody, payments, hedge providers, critical vendors, implementing partners) and by risk tier derived from credit quality, jurisdictional exposure, operational resilience, sanctions profile, compliance culture, and historical performance. Eligibility requires clean ownership vetting, adequate capitalisation, audited financials where applicable, regulatory licensure, and acceptance of GSIA audit, access, and publication clauses. High-risk counterparties may be conditionally onboarded under reduced tenors, collateralisation where lawful, and enhanced monitoring, or otherwise rejected.

2.4 Due Diligence and Onboarding. Due diligence is risk-based and documented. As a minimum it includes corporate identity, beneficial ownership, governance structures, financial condition, regulatory status, sanctions screening of the entity and principals, adverse media review, AML/CTF controls, cybersecurity posture where systems interconnect, and legal capacity to contract under the governing law. For sovereign-mandated state counterparties, residual risks are mitigated through structural safeguards, including escrow, cash waterfalls, joint signatory constructs in dual-key stages, and capped exposure tenors.

2.5 Sanctions, AML/CTF, and Ethics Interlocks. Screening is continuous against designated lists and internal sanctions grids. Confirmed matches, high-confidence alerts, or critical adverse findings trigger immediate escalation, transaction holds, and notification to the SCE Risk Committee and the Compliance, Audit, and Ethics function. Engagement with sanctioned counterparties is prohibited absent a reasoned exemption grounded in mandatory law, humanitarian carve-outs, or public-interest derogations explicitly authorised by the SCE and recorded with publication subject to lawful redaction. Related investigations follow the Ethics Hotline and Investigations protocols without prejudice to this Chapter's protective measures.

2.6 Exposure Measurement and Limits. Aggregate and per-counterparty exposure limits are set by reasoned resolution, considering liquidity buffers, FX hedging needs, tenor, instrument type, and jurisdictional contagion risk. Concentration limits apply across groups and jurisdictions. Exposures are measured daily for banks, weekly for critical vendors, and prior to each drawdown or hedge. Breaches auto-escalate to the middle office, then to the SCE Risk Committee if unresolved within defined windows. Hedging exposures are measured net of natural offsets; speculative positions are prohibited.

2.7 Political Risk Identification and Heat-Mapping. Political risk is tracked via jurisdictional heat-maps combining indicators of sovereign stability, rule of law, transfer and convertibility restrictions, expropriation risk, civil unrest, regulatory volatility, and data-sovereignty constraints. Heat-maps are updated at least quarterly and prior to major tranche decisions, domestication gate transitions, or title reversion. Project-specific overlays consider sector sensitivities (e.g., digital infrastructure, agriculture supply chains) and community dynamics.

2.8 Mitigation Structures. Mitigants are documented and proportionate to risk: diversified banking networks; offshore escrow for FX settlement where lawful; standby arrangements with alternative providers; stepped cash waterfalls; contractual step-in rights; political risk insurance where insurable and cost-effective; independent validation of procurement integrity; localisation of data stores and evidence repositories; and covenant packages that preserve audit, access, and publication rights. For Hosted Ownership, escrow arrangements and reversion mechanics are structured to survive political disruption, with survival clauses and force-majeure-adjusted timelines.

2.9 Triggers and Escalation. Triggers include sovereign rating downgrades beyond tolerance; imposition of capital controls; deterioration of transfer and convertibility indices; sanctions designations; civil

unrest affecting operations; judicial or administrative acts impairing contracts; systemic counterparty outages; or repeated KRI breaches (e.g., hedge ineffectiveness, payment delays, reconciliation breaks). Upon trigger, the operator activates the Counterparty and Political Risk Playbook: freeze on non-essential transactions; activation of backup banking rails; shortening of hedge tenors; tightening of approval matrices; and, where necessary, relocation of functions under the Continuity of Operations Chapter.

2.10 Decision Rights and Documentation. Risk reductions, suspensions, or exits are approved by the SCE Risk Committee or its delegated officers per an authority matrix. Decisions are reasoned, recorded, and published with lawful redaction; deferrals of publication for security or market sensitivity are time-limited with sunset review. Contracts with counterparties incorporate termination and suspension rights grounded in these triggers, with orderly wind-down provisions and cooperation duties.

2.11 Data-Protection and Sovereignty. Political risk responses may require data localisation, split-tunnelling of access, or temporary segregation of datasets. Controller/processor roles are reaffirmed; DPIAs are conducted where risk responses alter processing. Encryption, key management, and immutable logging remain mandatory. Where evidence must be escrowed onshore, cryptographic integrity artefacts and notarised inventories preserve verifiability for external validation and audit.

2.12 Domestication Linkage. At shadowing, political and counterparty risk frameworks are explained to Member personnel; at dual-key, joint monitoring and approvals apply to counterparty onboarding and escalations; at lead-role and handover, Members assume primary decision-making with oversight; legal localisation ensures that contracts, escrow, and banking mandates comply with national law while preserving GSIA standards and survivals. Readiness certification requires demonstrated capability to monitor and mitigate counterparty and political risks per this Chapter.

2.13 Hosted Ownership Safeguards. For Hosted Ownership, counterparty arrangements remain strictly within the ring-fenced perimeter, using discrete accounts and ledgers. Negative pledge and non-attachment clauses are monitored. Any attempted encumbrance or diversion triggers immediate step-in and, if necessary, activation of escrow and protective covenants. No private distribution is permitted; all value flows comply with Leasing Schedules and Implementation Agreements.

2.14 Records, Survivals, and Learning. Due-diligence dossiers, watchlists, exposure reports, trigger logs, escalation records, and decisions are archived per retention rules. Survivals include audit rights, confidentiality, data-protection obligations, IP in taxonomies and playbooks, and publication registers. Lessons learned are incorporated into standards by GSIA Holding AB through periodic circulars.

Chapter 3 — Continuity of Operations

3.1 Purpose and Applicability. This Chapter establishes the business continuity and operational resilience framework for GSIA programmes and Hosted Ownership portfolios, ensuring critical services remain available or are restored within tolerable limits in the face of disruptions including cyber events, facility loss, key supplier failure, civil unrest, natural hazards, or regulatory interventions. It binds GSIA SCE oversight bodies, GSIA Holding AB as standard-setter, GSIA AB as operator under SLA, and Hosted Ownership SPVs.

3.2 Governance and Roles. The GSIA SCE approves continuity policy, Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), and maximum tolerable outages for critical processes. GSIA Holding AB maintains canonical Business Impact Analysis (BIA) templates, dependency maps, DR/BCP

standards, tabletop and live-exercise playbooks, and after-action review taxonomies. GSIA AB owns and operates Business Continuity Plans (BCPs) and Disaster Recovery (DR) runbooks, with designated Continuity Officers per programme. Hosted Ownership SPVs maintain programme-specific BCPs within their ring-fenced perimeters, aligned to sovereign requirements and domestication gates.

3.3 Business Impact Analysis and Criticality. BIAs are conducted at least annually and upon material change. They classify processes by criticality, define RTO/RPO targets, map dependencies (people, facilities, systems, data, vendors, connectivity, power), and identify single-points-of-failure. The outputs drive resourcing of redundancy, DR architecture, and continuity measures. BIAs are approved by the SCE Committee and updated prior to tranche releases, domestication transitions, or title reversion.

3.4 Continuity Architecture. Continuity is achieved through layered measures: redundant processing capability (geographic or cloud-regional), resilient network topologies, failover procedures, secure data replication with tested restore paths, alternate work locations or remote-work contingencies, cross-trained staffing, and supplier redundancy for critical services. For Hosted Ownership, continuity measures respect data sovereignty and local infrastructure constraints, employing localised replicas and escrowed documentation to enable lawful restoration.

3.5 Disaster Recovery (Technology). DR runbooks define incident classification, decision rights, failover criteria, activation steps, communications protocols, and rollback procedures. Backups are encrypted, tested regularly through restore drills, and retained per RPOs. Privileged access for DR is governed by break-glass procedures with immutable logging and post-incident review. Systems hosting MEL, treasury, identity, and evidence repositories are designated Tier-1 and receive priority restoration.

3.6 Operational Continuity (People and Facilities). Workforce continuity is maintained by role-based cross-training, minimum staffing rosters, call-trees, and alternate work arrangements. Facility loss plans include relocation options, remote work enablement, and secure document transport or digitalisation. For contexts with civil unrest or public health emergencies, duty-of-care measures and remote execution protocols are pre-authorised, with clearly defined limitations on field operations and substitution of validation methods where necessary.

3.7 Supplier and Counterparty Continuity. Critical vendors and financial counterparties maintain their own BCPs meeting GSIA standards; compliance is verified during onboarding and annually. Contracts include continuity covenants, audit rights, notification duties, and cooperation obligations during incidents. Backup providers are pre-qualified, and switch-over procedures are rehearsed. For sovereign-mandated providers, contingency options and manual workarounds are documented.

3.8 Activation, Command, and Communications. BCP activation follows a reasoned decision by the designated Incident Commander within an authority matrix. An Incident Management Team coordinates response, logs decisions, and manages stakeholder communications. Internal communications are channelled through secure, resilient platforms with role-based access; external communications follow the publication doctrine, preserving transparency with lawful redaction. Coordination with Member authorities is pre-structured through Implementation Agreements and crisis MOUs.

3.9 Testing, Exercising, and Assurance. Continuity capabilities are exercised via tabletop simulations semi-annually and live technical failovers at least annually for Tier-1 systems. Exercises test cross-border data localisation constraints, Hosted Ownership escrow releases, Member joint-operations in dual-key stages, and restoration of MEL and treasury functions. Results are

documented; deficiencies produce corrective actions tracked to closure. Independent validators may test continuity under Document 09; findings feed domestication readiness.

3.10 Data-Protection and Security in Continuity. Continuity measures do not derogate data-protection obligations. Controllers and processors ensure that replicas, backups, and failover environments comply with lawful bases, localisation rules, and security standards. DPIAs are required for alternate processing sites and cross-border replication. IAM enforces least-privilege; break-glass access is logged and reviewed. Encryption in transit and at rest is mandatory, with key escrow procedures documented and auditable.

3.11 Domestication Alignment. At shadowing, Member personnel participate in continuity planning and exercises; at dual-key, joint authority applies to activation and communications; at lead-role, Members assume operational command with GSIA oversight; at handover and legal localisation, BCPs and DR runbooks are transferred and adapted to national law and infrastructure; readiness certification depends on demonstrated continuity performance meeting RTO/RPO targets without material defects.

3.12 Hosted Ownership Specifics. Within Hosted Ownership, continuity is constrained to the ring-fenced perimeter. Title and evidence registers, treasury accounts, and MEL repositories include escrowed documentation and restoration keys held under dual control to enable lawful reversion or protective step-in. No private distribution of value results from continuity activations; costs follow agreed schedules and are transparently published with lawful redaction.

3.13 KRIs, Escalation, and Interfaces. Continuity KRIs include missed RTO/RPO targets, failed restore tests, prolonged dependency outages, loss of key staff without coverage, and repeated communications breakdowns. Breaches trigger escalation under Document 17's risk taxonomy and may pause tranche releases or domestication progression until remedied. This Chapter interfaces with Document 11 (sanctions and ethics during incidents), Document 12 (security architecture and IAM), and Chapter 4 of this Manual (Exit and Wind-Down Procedures).

3.14 Records, Survivals, and Learning. Incident logs, exercise reports, corrective action registers, approvals, and communications records are archived per retention rules. Survivals include confidentiality, data-protection duties, IP in runbooks and playbooks, and audit rights. GSIA Holding AB issues periodic anonymised lessons-learned circulars to update standards, training, and accreditation content.

Chapter 4 — Exit and Wind-Down Procedures

4.1 Purpose and Triggers. This Chapter establishes binding procedures for an orderly, controlled exit or wind-down of a programme or Hosted Ownership portfolio, preserving value, continuity of essential services, evidentiary integrity, and public-interest objectives. Triggers include mandate expiry by term; completion and domestication to Member authorities; strategic termination by reasoned resolution; persistent funding shortfall; force majeure rendering continuation impracticable; material breach of fiduciary or legal obligations; sanctions constraints; or a Member's lawful sovereign decision invoking exit consistent with the Charter and governing instruments.

4.2 Governance and Separation of Functions. The GSIA SCE authorises exit by reasoned resolution specifying scope, grounds, timelines, and custodial outcomes. GSIA Holding AB maintains canonical exit playbooks, asset and liability classification standards, document escrow taxonomies, and knowledge-transfer templates, without operational control over the exit itself. GSIA AB and any Hosted Ownership SPV execute wind-down tasks under an authority matrix enforcing four-eyes control,

segregation of duties, and calibrated countersignature thresholds. External validators may be commissioned under Document 09 to assure propriety and completeness of exit actions.

4.3 Exit Planning and Timelines. An Exit Plan is drafted within fifteen business days of the trigger, approved by the SCE Committee, and published with lawful redaction. It specifies the inventory of assets and liabilities; outstanding contractual obligations; workforce measures; communications; data and evidence disposition; treasury closure and reconciliations; legal and regulatory filings; escrow and handover artifacts; insurance and hedging run-off; and dispute or claim management. The plan sets milestones and responsible owners, with interlocks to domestication gates where exit occurs through handover.

4.4 Asset and Liability Treatment. Assets are classified as project-titled, Member-titled, leased, or third-party; liabilities as contractual, statutory, or contingent. Under Hosted Ownership, project assets and cash remain within the ring-fenced perimeter with non-attachment and negative pledge intact. No private distribution is permitted beyond agreed service consideration. Disposal or transfer follows Implementation Agreements and Leasing Schedules, with priority given to transfer to the Member or designated public custodian. Inventory lists are reconciled to discrete ledgers and verified by independent assurance prior to finalisation.

4.5 Treasury Wind-Down. Discrete project bank accounts and sub-ledgers are reconciled to a zero-variance standard. Payment queues are triaged; essential obligations are honoured; non-essential or disputed obligations are suspended pending legal review. Escrow constructs are adjusted to secure pending claims and handover commitments. Hedging instruments are run off or closed out per Chapter 5. Signatory matrices are amended to prevent new risk taking except as necessary to wind-down. Final bank statements and reconciliations are archived and preserved for audit and publication with lawful redaction.

4.6 Contracts, Procurement, and Suppliers. Active contracts are reviewed for termination, assignment, or novation consistent with governing law and public-interest commitments. Critical suppliers receive notice and continuity instructions; backup providers are activated where required to maintain essential services during transition. Procurement actions in flight are paused unless a reasoned resolution authorises completion to prevent value loss or critical service interruption. Termination or variation letters are standardised and logged; disputes are channelled under the Legal Instruments Compendium without prejudicing exit.

4.7 Workforce and Knowledge Transfer. Staff transitions follow lawful employment practices and duty-of-care standards. Knowledge transfer is mandatory: runbooks, procedures, configuration baselines, keys, and registers are escrowed and delivered to the designated custodian. For domestication exits, Member personnel assume lead-role status prior to handover to ensure continuity. Access rights are de-provisioned according to a controlled schedule, with privileged access revoked last under break-glass oversight to complete restore or archival tasks.

4.8 Data, Evidence, and IP. Data and evidence repositories are inventoried, hashed, and archived; chain-of-custody logs are preserved. Controllers and processors implement DPIAs where exit modifies processing bases or locations. Personal data is localised or transferred under lawful mechanisms; retention and deletion follow statutory and Charter requirements. IP stewardship remains with GSIA Holding AB; operational copies and licensed materials are transferred under non-exclusive, royalty-free licences where required for public custody, consistent with publication doctrine and security needs.

4.9 Continuity During Exit. Essential services—treasury minimal operations, MEL reporting required for closure, grievance redress channels, and security monitoring—remain active under a reduced operating model until handover or termination is achieved. Continuity RTO/RPO targets from Chapter 3 remain applicable; any deviations require reasoned resolution and public notice with lawful redaction.

4.10 Domestication and Reversion Mechanics. Where exit occurs by domestication, the gates are reaffirmed: shadowing completion; dual-key operations; lead-role assumption; system handover with escrowed documentation and keys; legal localisation of instruments; and readiness certification. Under Hosted Ownership, the reversion covenant is executed: title transfers to the Member or designated public custodian; registers are updated; escrow conditions are satisfied; and survivals (audit rights, records, warranties, and liabilities as stipulated) persist post-transfer.

4.11 Publication, Transparency, and Appeals. The Exit Plan, milestone reports, reconciled inventories, and final closure memorandum are published with lawful redaction. Deferrals are reasoned, time-limited, and recorded. Stakeholders may request reconsideration on factual accuracy; appeals on material exit decisions lie to the Appeals Board under Document 09 Chapter 4. A consolidated "Exit Docket" records decisions, redactions, deferrals, and outcomes.

4.12 Insurance, Claims, and Disputes. Insurance notifications and run-off elections are made promptly; claims are pursued to conclusion or assigned to the successor custodian. Disputes are managed under contractual mechanisms without delaying essential wind-down actions. Settlements are reasoned, documented, and published with lawful redaction.

4.13 Records, Survivals, and Audit. Exit records—plans, approvals, reconciliations, inventories, contracts, communications, assurance reports—are archived per the longer of Charter, statutory, or covenant periods. Survivals include confidentiality, data-protection obligations, audit and access rights, negative pledge and non-attachment until closure, and IP stewardship. Independent validation of exit completeness may be commissioned and published.

Chapter 5 — Insurance and Hedging Instruments

5.1 Purpose and Guardrails. This Chapter codifies the disciplined use of insurance and hedging instruments to transfer or mitigate insurable and market risks without introducing speculative exposure or value leakage. The objective is resilience and continuity—never profit seeking. Instruments are employed only where proportionate, cost-effective, and aligned to public-interest outcomes.

5.2 Governance and Separation of Functions. The GSIA SCE approves risk transfer policy, eligible instrument classes, limits, and counterparties. GSIA Holding AB maintains canonical coverage matrices, hedging policy templates, actuarial and market risk models, and broker due-diligence standards. GSIA AB executes placements and hedges under authority matrices that enforce four-eyes control, segregation of front/middle/back office functions, and calibrated countersignature thresholds. Hosted Ownership SPVs mirror these controls within ring-fenced perimeters and sovereign constraints.

5.3 Insurance Programme Architecture. Insurance is structured in layers and modules tailored to programme risk profiles: property and equipment; business interruption linked to continuity targets; general and professional liability; cyber and data-breach; crime and fidelity; directors and officers where applicable; and political risk (including expropriation, currency inconvertibility, and transfer restrictions) where insurable and cost-effective. Deductibles and limits are set by reasoned analysis of

risk appetite, retention capacity, and continuity objectives. Aggregation clauses, exclusions, territorial and jurisdictional limits, and notification duties are documented and reviewed before binding.

5.4 Political Risk Insurance and Sovereign Constraints. Where permitted and prudent, political risk coverage is procured to mitigate transfer and convertibility risk, expropriation, and arbitrary contract frustration. In jurisdictions restricting foreign insurance or imposing localisation, structures may include onshore primary layers with reinsurance cessions to rated markets, provided sovereignty and compliance are respected while preserving claims certainty and auditability.

5.5 Broker and Insurer Due Diligence. Brokers and insurers are onboarded under the counterparty standards in Chapter 2: licensure, credit rating and solvency, sanctions screening, governance and conduct record, claims-handling capability, and acceptance of GSIA audit and publication clauses with lawful redaction. Concentration limits apply by insurer and group; security is periodically reassessed. Misconduct, downgrade below tolerance, or sanctions events trigger enhanced monitoring or replacement.

5.6 Placement, Documentation, and Claims. Placements are executed under standardised binding authorities and cover notes; policies are reviewed for accuracy, warranties, and conditions precedent. Claims protocols define notification timelines, evidence standards, adjuster appointment, mitigation duties, and interim funding options. Claims files maintain chain-of-custody for evidence, are logged immutably, and are published in summary with lawful redaction. Recoveries are credited to the project perimeter; no private distribution is permitted.

5.7 Hedging Policy and Limits. Hedging instruments are limited to deliverable forwards, non-deliverable forwards where necessary, and plain-vanilla options to cap adverse moves. Complex, path-dependent, or leveraged structures are prohibited. Hedge volumes shall not exceed documented net exposures; tenor aligns to obligation timing; early termination requires reasoned approval. Effectiveness testing is conducted and recorded; ineffectiveness beyond tolerance triggers investigation and, if persistent, model recalibration or policy revision.

5.8 Accounting, Valuation, and Disclosure. Insurance costs and hedge fair values are recorded in discrete ledgers at the project level. Valuation methods are documented; sensitivity to market inputs is disclosed internally to the SCE Committee and relevant Member authorities. Public disclosures summarise coverage and hedging posture with lawful redaction of sensitive counterparties or identifiers. Publication deferrals for market sensitivity are time-limited and recorded.

5.9 Interfaces with Treasury and Continuity. Insurance and hedging strategies are integrated with liquidity buffers, counterparty limits, and continuity planning. Business interruption parameters align with RTO/RPO targets in Chapter 3. Political risk insurance complements, but does not replace, escrow, step-in rights, and contractual mitigants. Hedging is coordinated with forecast cash flows to avoid over-hedging or liquidity strain at settlements.

5.10 Data-Protection and Security. Where insurance or hedging operations involve personal data or sensitive system logs (e.g., cyber claims), controller/processor allocations are reaffirmed; DPAs are in place with brokers, adjusters, and TPAs; DPIAs are conducted for high-risk processing or cross-border transfers. Evidence repositories are encrypted in transit and at rest; IAM enforces least-privilege; access logs are immutable and audited.

5.11 Hosted Ownership Safeguards. Insurance proceeds and hedge cash flows related to Hosted Ownership projects are credited exclusively to the ring-fenced perimeter's bank accounts and ledgers.

Non-attachment and negative pledge remain in force. Proceeds utilised for restoration or remediation are documented and published with lawful redaction; residual funds follow Leasing Schedules and Implementation Agreements. No private distribution is permissible.

5.12 Domestication Alignment. As domestication progresses, Members participate in coverage selection, broker engagement, and hedge approvals at dual-key stage; assume placement leadership at lead-role; and receive full documentation and assignments at handover. Legal localisation adjusts policy wording and governing law to national requirements without diluting coverage certainty or audit and publication survivals. Readiness certification requires demonstrated capability to manage coverage, claims, and hedges per this Chapter.

5.13 KRIs, Stress Testing, and Escalation. KRIs include uninsured or under-insured exposures, coverage gaps due to exclusions or territorial limits, premium affordability breaches, counterparty downgrade events, repeated hedge ineffectiveness, and settlement liquidity strain. Stress testing includes simulated claims scenarios and market shocks affecting hedge settlements. Breaches and adverse results escalate under Document 17's risk taxonomy; corrective actions are tracked to closure and may trigger policy redesign or increased buffers.

5.14 Records, Survivals, and Publication. Placement files, policies, endorsements, claims dossiers, hedge documentation, valuations, and approvals are archived for the longer of Charter, statutory, or covenant periods. Survivals include confidentiality, data-protection obligations, audit and access rights, IP in models and templates, and publication registers. Summaries of insurance posture and hedging utilisation are published periodically with lawful redaction; deferrals are reasoned, time-limited, and sunset-reviewed.