RWA.immo

CONFIDENTIAL

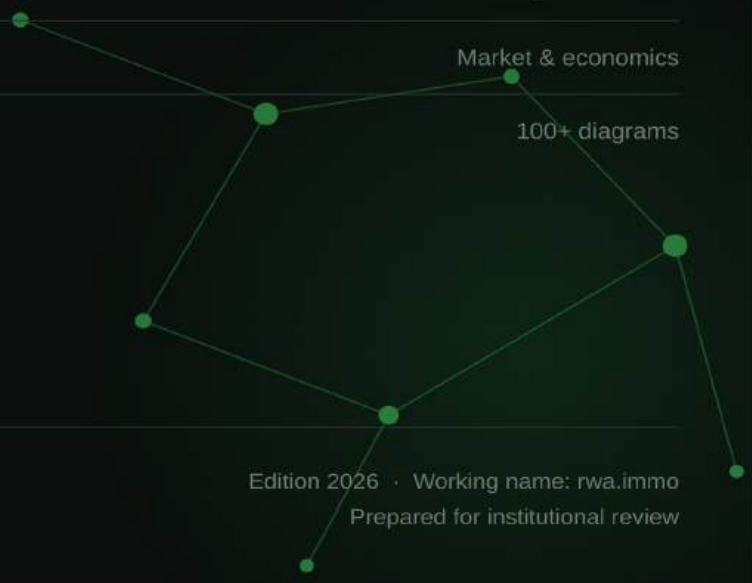
INSTITUTIONAL DOCUMENTATION PACKAGE

Institutional Digital Real Estate Capital Markets Infrastructure

A seven-volume institutional architecture & documentation package — from legal foundation and system architecture to markets, financial intelligence, security, commercial model and a consolidated atlas.

THE SEVEN VOLUMES

I	**Executive & Regulatory**	Legal foundation
II	**Technical Architecture**	System & contracts
III	**Marketplace & Trading**	Venue & settlement
IV	**Financial Intelligence**	Valuation, NAV & risk
V	**Security & Operations**	Custody & resilience
VI	**Business & Financial Model**	Market & economics
VII	**Architecture Atlas**	100+ diagrams



Reza Ebrahimi · Founder

Edition 2026 · Working name: rwa.immo
Prepared for institutional review

Table of Contents

VOLUME I — EXECUTIVE & REGULATORY....21
Institutional Digital Real Estate Capital Markets Infrastructure....21
Multi-Volume Documentation Package — Volume I of VII....21
TITLE PAGE & DOCUMENT CONTROL....21
HOW TO READ THIS VOLUME (Control File — seed)....22
DETAILED TABLE OF CONTENTS....22
LIST OF FIGURES....23
LIST OF TABLES....24
EXECUTIVE SUMMARY....24
CHAPTER 1 — TOKEN CLASSIFICATION (LEAD ANALYSIS)....26
1.1 Why classification comes first....26
1.2 The Swiss FINMA token taxonomy (substance over form)....26
1.3 Classification of the platform's instruments....27
1.4 Liechtenstein FMA substance-over-form alignment....29
1.5 EEA activity: MiCA / MiFID II carve-out, ART/EMT, DORA....30
1.6 The settlement asset as a distinct classification problem....31
1.7 Classification summary matrix....32
CHAPTER 2 — STRATEGIC VISION, OPERATING MODEL & GOVERNANCE....34
2.1 Strategic vision and market context....34
2.2 The platform as a domain map....34
2.3 Dual-mode operating model....35
2.4 Governance, organisation and the responsibility map (RACI)....35
2.5 On-chain vs. off-chain governance....36
CHAPTER 3 — DUAL-MODE FUNDING & CAPITAL FORMATION (LEGAL ARCHITECTURE)....37

3.1 Model A — Asset-Backed Issuance....37
3.2 Model B — Forward-Funding / Development Finance....38
3.3 Special-purpose vehicle (SPV) structures....39
3.4 On-chain subscription, capital-call and escrow mechanics....39
3.5 Investor eligibility and accreditation....40
CHAPTER 4 — SWISS REGULATORY FOUNDATION....41
4.1 DLT Act and CO Art. 973d–973i mapping....41
4.2 FinSA prospectus regime and key information document....43
4.3 FinfraG / DLT Trading Facility licensing....45
4.4 AMLA / AMLO-FINMA anti-money-laundering regime....46
4.5 Collective Investment Schemes Act (CISA) boundary analysis....48
4.6 Bankruptcy remoteness and client-asset segregation....50
VOLUME I — PART 2 (Chapters 5–11 and tail)....51
CHAPTER 5 — SECONDARY JURISDICTION: UNITED ARAB EMIRATES (DUBAI / VARA)....51
5.1 The UAE regulatory architecture (who regulates what)....51
5.2 Token classification under VARA — ARVA....51
5.3 Licensing, capital, disclosure and segregation....52
5.4 AML/CFT and sanctions (UAE)....53
CHAPTER 6 — ADDITIONAL JURISDICTIONS: LIECHTENSTEIN, SINGAPORE, HONG KONG....53
6.1 Liechtenstein (TVTG, SPG/Due Diligence Act)....53
6.2 Singapore (MAS — SFA, PS Act, FSM Act)....54
6.3 Hong Kong (SFC — SFO, AMLO; HKMA — Stablecoins Ordinance)....56
6.4 Jurisdiction comparison matrix....57
CHAPTER 7 — CROSS-BORDER AML/CFT, SANCTIONS, CRS/FATCA....60

7.1 A single control framework, multiple legal bases....60
7.2 Sanctions....60
7.3 Tax-information exchange — CRS and FATCA....61
CHAPTER 8 — TAX, ACCOUNTING & REGULATORY-REPORTING AUTOMATION 61
8.1 Scope and posture....61
8.2 Principal tax touchpoints....61
8.3 Tax structuring memorandum — outline (flowchart)....62
8.4 Accounting and NAV....63
CHAPTER 9 — DATA PROTECTION & PRIVACY....64
9.1 Applicable regimes....64
9.2 The blockchain-specific tension....64
9.3 Governance....64
CHAPTER 10 — VENDOR & OUTSOURCING RISK MANAGEMENT....65
10.1 Why this is a board-level matter....65
10.2 The vendor-risk lifecycle....65
10.3 Key controls....65
CHAPTER 11 — COMPETITIVE LANDSCAPE, INDUSTRY THREATS & LIMITATIONS 65
11.1 Competitive landscape (categories and benchmarks)....65
11.2 Industry threats and limitations register....66
11.3 Honest limitations....67
INTERIM COMPLIANCE & COMPLETENESS AUDIT — VOLUME I....68
FUTURE JURISDICTION COMPATIBILITY NOTES....69
GLOSSARY....70
APPENDIX A — LEGAL SOURCE REGISTER & VERBATIM-TEXT POINTERS....73
APPENDIX B — LEGAL-EVENT → ON-CHAIN-STATE MAPPING (Table 4)....74

APPENDIX C — RACI MATRIX (Table 5) 75
APPENDIX D — CITATION REGISTER (Table 8) 78
APPENDIX E — CROSS-REFERENCE INDEX 80
DIAGRAM INVENTORY (Volume I) 80
END OF VOLUME I (interim draft) 81
VOLUME II — TECHNICAL ARCHITECTURE 82
Institutional Digital Real Estate Capital Markets Infrastructure 82
Multi-Volume Documentation Package — Volume II of VII 82
TITLE PAGE & DOCUMENT CONTROL 82
HOW TO READ THIS VOLUME (CONTROL FILE) 83
DETAILED TABLE OF CONTENTS 84
LIST OF FIGURES 84
LIST OF TABLES 86
EXECUTIVE SUMMARY 88
CHAPTER 1 — ARCHITECTURE PRINCIPLES & THE C4 MODEL 89
1.1 The governing principle: compliance by construction 89
1.2 Principles and the mechanisms that implement them 90
1.3 C4 system and container views 90
1.4 The on-chain / off-chain split 91
CHAPTER 2 — CHAIN LAYER & NETWORK TOPOLOGY 92
2.1 Requirements on the chain layer 92
2.2 Deployment options and trade-offs 92
2.3 Network topology and interoperability 94
CHAPTER 3 — SMART-CONTRACT ARCHITECTURE 95
3.1 The ERC-3643 / T-REX suite 95
3.2 The compliant transfer 97

3.3 Dual-mode funding contracts....98
3.4 Upgradeability and storage safety....99
CHAPTER 4 — IDENTITY, COMPLIANCE & ELIGIBILITY ENFORCEMENT....100
4.1 Why identity is part of the protocol....100
4.2 Claim issuance and verification....101
4.3 Mapping compliance modules to Volume I legal rules....101
CHAPTER 5 — ORACLE & DATA LAYER....102
5.1 The data gap....102
5.2 Oracle services and their uses....102
5.3 Oracle risk and mitigations....103
CHAPTER 6 — OFF-CHAIN PLATFORM: MICROSERVICES ARCHITECTURE....104
6.1 Why microservices, and the boundaries....104
6.2 Microservice catalogue....104
6.3 End-to-end subscription....105
CHAPTER 7 — CUSTODY & KEY MANAGEMENT (ARCHITECTURAL)....106
7.1 What must be protected....106
7.2 Custody models and key architecture....106
7.3 Architectural requirements (summary)....107
CHAPTER 8 — CRYPTOGRAPHY: ZERO-KNOWLEDGE PROOFS & POST-QUANTUM READINESS....107
8.1 Two cryptographic agendas....107
8.2 Zero-knowledge and confidential compute (privacy)....107
8.3 Post-quantum readiness (longevity)....108
CHAPTER 9 — FIAT, BANKING & SETTLEMENT INTEGRATION....110
9.1 The cash leg and delivery-versus-payment....110
9.2 Banking rails, messaging and reconciliation....111

CHAPTER 10 — SECURITY ARCHITECTURE & DEVSECOPS....112
10.1 Threat model and defence in depth....112
10.2 Secure SDLC and pipeline gates....112
10.3 Runtime security and operations....112
CHAPTER 11 — OBSERVABILITY, RESILIENCE & SCALABILITY....113
11.1 Observability and SRE....113
11.2 Resilience and finality handling....113
11.3 Scalability....113
CHAPTER 12 — TECHNOLOGY STACK, STANDARDS REGISTER & LIMITATIONS 114
12.1 Stack and versions (summary)....114
12.2 What is settled vs. what is an option....114
12.3 Technical threats & limitations register (honest assessment)....115
12.4 Honest limitations....116
INTERIM COMPLIANCE & COMPLETENESS AUDIT — VOLUME II....116
FUTURE JURISDICTION & TECHNOLOGY COMPATIBILITY NOTES....117
GLOSSARY (TECHNICAL)....117
APPENDIX A — STANDARDS & VERSIONS REGISTER....119
APPENDIX B — CONTRACT INTERFACE INVENTORY (INDICATIVE)....120
APPENDIX C — SERVICE CATALOGUE (OFF-CHAIN)....121
APPENDIX D — CITATION REGISTER (TABLE — VOLUME II)....121
APPENDIX E — CROSS-REFERENCE INDEX....122
DIAGRAM INVENTORY (Volume II)....123
END OF VOLUME II (interim draft)....124
VOLUME III — MARKETPLACE & TRADING....124
Institutional Digital Real Estate Capital Markets Infrastructure....124

Multi-Volume Documentation Package — Volume III of VII....124
TITLE PAGE & DOCUMENT CONTROL....124
HOW TO READ THIS VOLUME (CONTROL FILE)....125
DETAILED TABLE OF CONTENTS....126
LIST OF FIGURES....127
LIST OF TABLES....128
EXECUTIVE SUMMARY....128
CHAPTER 1 — MARKET STRUCTURE & DESIGN PRINCIPLES....130
1.1 What “marketplace” means for a permissioned security....130
1.2 The asset lifecycle....130
1.3 Participants and the venue....130
1.4 Design principles....131
CHAPTER 2 — REGULATED VENUE STRATEGY (MULTI-JURISDICTION)....132
2.1 Why venue choice is a first-order decision....132
2.2 The venue regimes compared....132
2.3 Operate vs list, and the multi-jurisdiction map....134
2.4 The US watch item....135
CHAPTER 3 — TRADING MODELS: ORDER BOOK, RFQ, AMM....135
3.1 Matching the model to the asset....135
3.2 The three models compared....136
3.3 Off-chain matching, on-chain settlement....136
CHAPTER 4 — ORDER LIFECYCLE & MATCHING....137
4.1 Order types....137
4.2 The order lifecycle with pre-trade compliance....137
4.3 Matching-engine architecture....138
CHAPTER 5 — SETTLEMENT & CLEARING....139

5.1 The settlement question....139
5.2 Atomic delivery-versus-payment....140
5.3 Finality and failed-trade handling....141
CHAPTER 6 — LIQUIDITY....142
6.1 The honest problem....142
6.2 Sources of liquidity and how they are provided....142
6.3 Liquidity, redemption and the product design....143
CHAPTER 7 — MARKET INTEGRITY & SURVEILLANCE....143
7.1 Why integrity controls apply....143
7.2 Behaviours and controls....143
7.3 Surveillance architecture and reporting....144
CHAPTER 8 — INVESTOR PROTECTION & CONDUCT AT THE POINT OF TRADE 146
8.1 Conduct does not stop at onboarding....146
8.2 Point-of-trade conduct flow....146
8.3 Conduct obligations by regime....148
CHAPTER 9 — SECONDARY-MARKET COMPLIANCE ENFORCEMENT....148
9.1 The same enforcement, now at trade time....148
9.2 Corporate actions and the transfer-agent function....150
9.3 Cross-jurisdiction enforcement....150
CHAPTER 10 — FEES, MARKET DATA & CONNECTIVITY....150
10.1 Fee model (architectural)....150
10.2 Market data....150
10.3 Connectivity and onboarding....150
CHAPTER 11 — COMPETITIVE LANDSCAPE & BENCHMARKS....153
11.1 Benchmarks, not targets....153

11.2 What the benchmarks teach....154
CHAPTER 12 — LIMITATIONS & THREATS REGISTER....154
12.1 Honest assessment....154
12.2 Honest limitations....156
INTERIM COMPLIANCE & COMPLETENESS AUDIT — VOLUME III....156
FUTURE JURISDICTION & TECHNOLOGY COMPATIBILITY NOTES....158
GLOSSARY....159
APPENDIX A — VENUE & REGULATORY REGISTER....160
APPENDIX B — ORDER-TYPE & MESSAGE CATALOGUE (INDICATIVE)....161
APPENDIX C — SURVEILLANCE SCENARIO LIBRARY (INDICATIVE)....161
APPENDIX D — CITATION REGISTER (TABLE — VOLUME III)....162
APPENDIX E — CROSS-REFERENCE INDEX....162
DIAGRAM INVENTORY (Volume III)....163
END OF VOLUME III (interim draft)....164
VOLUME IV — FINANCIAL INTELLIGENCE....164
Institutional Digital Real Estate Capital Markets Infrastructure....164
Multi-Volume Documentation Package — Volume IV of VII....164
TITLE PAGE & DOCUMENT CONTROL....164
HOW TO READ THIS VOLUME (CONTROL FILE)....165
DETAILED TABLE OF CONTENTS....166
LIST OF FIGURES....167
LIST OF TABLES....167
EXECUTIVE SUMMARY....168
CHAPTER 1 — PRINCIPLES & THE INTELLIGENCE ARCHITECTURE....169
1.1 What “financial intelligence” means here....169
1.2 The intelligence is a pipeline, not a black box....170

1.3 The architecture.....170
1.4 Principles and mechanisms.....172
CHAPTER 2 — VALUATION FOUNDATIONS & STANDARDS.....172
2.1 Why standards come first.....172
2.2 Bases of value and the three approaches.....173
2.3 Applicability to the platform’s assets.....175
CHAPTER 3 — NAV COMPUTATION & THE ORACLE PIPELINE.....175
3.1 From valuation to NAV to the chain.....175
3.2 The NAV pipeline.....175
3.3 Frequency, basis and controls.....176
CHAPTER 4 — DISCOUNTED-CASH-FLOW & INCOME MODELLING.....176
4.1 The role of DCF.....176
4.2 Model structure and inputs.....176
4.3 Sensitivity and the limits of a point estimate.....178
CHAPTER 5 — RISK MODELLING & MONTE CARLO SIMULATION.....179
5.1 From point estimates to distributions.....179
5.2 The simulation flow.....180
5.3 Risk metrics and stress testing.....182
CHAPTER 6 — AUTOMATED VALUATION & MACHINE-LEARNING MODELS.....183
6.1 Where ML helps — and where it does not.....183
6.2 The ML pipeline.....184
6.3 Accuracy, data and honest limits.....184
CHAPTER 7 — EXPLAINABILITY & MODEL CARDS.....184
7.1 Why explainability is non-negotiable.....184
7.2 Techniques.....184
7.3 Model cards.....185

CHAPTER 8 — MODEL GOVERNANCE & MODEL-RISK MANAGEMENT.....186
8.1 Models are a managed risk.....186
8.2 The model lifecycle.....186
8.3 Controls.....187
CHAPTER 9 — AI REGULATORY ALIGNMENT.....188
9.1 Three frameworks, one programme.....188
9.2 Mapping the platform’s AI uses to the EU AI Act.....189
9.3 Why conservative classification.....190
CHAPTER 10 — LARGE-LANGUAGE-MODEL USAGE POLICY.....190
10.1 Where LLMs are used — and the bright line.....190
10.2 Risks and controls.....190
10.3 The LLM control flow.....191
10.4 Prohibited and disclosed uses.....193
CHAPTER 11 — DATA ARCHITECTURE FOR INTELLIGENCE.....193
11.1 Data quality is the foundation (IVS 104).....193
11.2 The architecture.....193
11.3 Lineage, reproducibility and privacy.....195
CHAPTER 12 — LIMITATIONS & THREATS REGISTER.....195
12.1 Honest assessment.....195
12.2 Honest limitations.....196
INTERIM COMPLIANCE & COMPLETENESS AUDIT — VOLUME IV.....196
FUTURE JURISDICTION & TECHNOLOGY COMPATIBILITY NOTES.....198
GLOSSARY.....198
APPENDIX A — STANDARDS & FRAMEWORKS REGISTER.....199
APPENDIX B — MODEL INVENTORY TEMPLATE (INDICATIVE).....200
APPENDIX C — EXAMPLE MODEL CARD (SKELETON).....201

APPENDIX D — CITATION REGISTER (TABLE — VOLUME IV)....201
APPENDIX E — CROSS-REFERENCE INDEX....202
DIAGRAM INVENTORY (Volume IV)....202
END OF VOLUME IV (interim draft)....203
VOLUME V — SECURITY & OPERATIONS....204
Institutional Digital Real Estate Capital Markets Infrastructure....204
Multi-Volume Documentation Package — Volume V of VII....204
TITLE PAGE & DOCUMENT CONTROL....204
HOW TO READ THIS VOLUME (CONTROL FILE)....205
DETAILED TABLE OF CONTENTS....206
LIST OF FIGURES....207
LIST OF TABLES....207
EXECUTIVE SUMMARY....208
CHAPTER 1 — PRINCIPLES & THE SECURITY-OPERATIONS MODEL....210
1.1 Security is a programme, not a property....210
1.2 The operating model: three lines and a SOC....210
1.3 The layered model....210
1.4 Principles and mechanisms....210
CHAPTER 2 — CUSTODY ARCHITECTURE (DEPTH)....211
2.1 What custody must achieve....211
2.2 Segregation models under FINMA Guidance 01/2026....211
2.3 Custody and key-control architecture....212
2.4 Responsibility does not transfer....213
CHAPTER 3 — KEY MANAGEMENT & KEY CEREMONIES....214
3.1 The keys and what they protect....214
3.2 The key-management toolkit....214

3.3 Key ceremonies....214
3.4 The key lifecycle and recovery....215
CHAPTER 4 — POST-QUANTUM MIGRATION PLAN....215
4.1 The threat and the deadline....215
4.2 The standards and where they apply....216
4.3 The phased migration roadmap....217
4.4 Governance of the migration....219
CHAPTER 5 — DEVSECOPS (DEPTH)....219
5.1 Security is built, not inspected in....219
5.2 The secure SDLC....219
5.3 The control set....219
CHAPTER 6 — SMART-CONTRACT SECURITY OPERATIONS....220
6.1 Operating immutable code safely....220
6.2 Monitoring, circuit breakers and governed upgrades....220
6.3 Incident playbooks and a bug bounty....222
CHAPTER 7 — THREAT DETECTION, SOC & INCIDENT RESPONSE....222
7.1 Detect and respond, because prevention is never perfect....222
7.2 The incident-response lifecycle....222
7.3 SOC and detection architecture....222
7.4 Incident classification and reporting....224
CHAPTER 8 — OPERATIONAL RESILIENCE & DORA....224
8.1 Resilience is now a legal obligation....224
8.2 The five pillars mapped....225
8.3 Pillar-by-pillar....225
8.4 Concentration risk and Critical ICT Third-Party Providers....226

CHAPTER 9 — BUSINESS CONTINUITY, DISASTER RECOVERY & RESILIENCE TESTING....227
9.1 Withstand, respond, recover....227
9.2 BC/DR architecture....227
9.3 Resilience testing....227
CHAPTER 10 — DEV-PHASE FUND-RUN & STRESS TESTING....228
10.1 Why simulate a run before real money is at stake....228
10.2 The fund-run scenario....228
10.3 What is tested....230
CHAPTER 11 — VENDOR & THIRD-PARTY RISK....230
11.1 The platform is only as resilient as its dependencies....230
11.2 Concentration and the CTPP dimension....231
11.3 Vendor categories and controls....233
CHAPTER 12 — LIMITATIONS & THREATS REGISTER....233
12.1 Honest assessment....233
12.2 Honest limitations....234
INTERIM COMPLIANCE & COMPLETENESS AUDIT — VOLUME V....235
FUTURE JURISDICTION & TECHNOLOGY COMPATIBILITY NOTES....236
GLOSSARY....237
APPENDIX A — STANDARDS, FRAMEWORKS & VERSIONS REGISTER....238
APPENDIX B — KEY-CEREMONY CHECKLIST (INDICATIVE)....239
APPENDIX C — INCIDENT SEVERITY & REPORTING MATRIX (INDICATIVE)....240
APPENDIX D — CITATION REGISTER (TABLE — VOLUME V)....240
APPENDIX E — CROSS-REFERENCE INDEX....240
DIAGRAM INVENTORY (Volume V)....241
END OF VOLUME V (interim draft)....242

VOLUME VI — BUSINESS & FINANCIAL MODEL....242
Institutional Digital Real Estate Capital Markets Infrastructure....242
Multi-Volume Documentation Package — Volume VI of VII....242
TITLE PAGE & DOCUMENT CONTROL....242
HOW TO READ THIS VOLUME (CONTROL FILE)....243
DETAILED TABLE OF CONTENTS....244
LIST OF FIGURES....245
LIST OF TABLES....245
EXECUTIVE SUMMARY....246
CHAPTER 1 — PRINCIPLES & THE BUSINESS-MODEL FRAME....247
1.1 What this volume is — and is not....247
1.2 The value the platform captures — and the value it must first create....247
1.3 The business-model frame....247
1.4 Principles and mechanisms....248
CHAPTER 2 — MARKET OPPORTUNITY (TAM / SAM / SOM)....248
2.1 A market defined by a gap....248
2.2 The ceiling: external forecasts (attributed, with variance)....249
2.3 From TAM to SOM....250
2.4 The floor: forecast versus reality....252
CHAPTER 3 — VALUE PROPOSITION & COMPETITIVE POSITION....253
3.1 Problems solved, and for whom....253
3.2 Value by participant....253
3.3 Competitive position and honest threats....255
CHAPTER 4 — REVENUE MODEL & TOKENOMICS....255
4.1 Diversified, mostly usage-based....255
4.2 Revenue streams....255

4.3 Alignment and honesty in pricing....256
4.4 Tokenomics: a platform token is an option, not an assumption....256
CHAPTER 5 — UNIT ECONOMICS....258
5.1 The unit is an issuance (and the assets it carries)....258
5.2 Illustrative unit economics....258
5.3 What has to be true....259
CHAPTER 6 — FINANCIAL MODEL & SCENARIOS....259
6.1 A driver-based model, not a point forecast....259
6.2 Drivers and scenarios....259
6.3 Reading the scenarios honestly....260
CHAPTER 7 — COST & CAPACITY PLANNING....261
7.1 A cost base dominated by trust....261
7.2 Build versus run....261
7.3 Capacity....263
CHAPTER 8 — FUNDING & CAPITAL REQUIREMENTS....263
8.1 Two distinct capital needs....263
8.2 Funding stages and options....264
8.3 Runway discipline....264
CHAPTER 9 — ROADMAP & PHASING....264
9.1 Gated, jurisdiction-sequenced growth....264
9.2 The phases....264
9.3 Dependencies and sequencing risk....265
CHAPTER 10 — KEY RISKS TO THE BUSINESS MODEL....265
10.1 The risks that decide the outcome....265
10.2 The one to watch....266
CHAPTER 11 — KPIs & MODEL GOVERNANCE....266

11.1 Measure what matters.....266
11.2 The KPI tree.....267
11.3 Governing the model.....267
CHAPTER 12 — LIMITATIONS & THREATS REGISTER.....267
12.1 Honest assessment.....267
12.2 Honest limitations.....268
INTERIM COMPLIANCE & COMPLETENESS AUDIT — VOLUME VI.....268
FUTURE JURISDICTION & TECHNOLOGY COMPATIBILITY NOTES.....269
GLOSSARY.....270
APPENDIX A — MARKET DATA & SOURCES REGISTER.....270
APPENDIX B — ILLUSTRATIVE ASSUMPTION SET (TEMPLATE).....271
APPENDIX C — KPI DEFINITIONS (INDICATIVE).....272
APPENDIX D — CITATION REGISTER (TABLE — VOLUME VI).....272
APPENDIX E — CROSS-REFERENCE INDEX.....273
DIAGRAM INVENTORY (Volume VI).....273
END OF VOLUME VI (interim draft).....274
VOLUME VII — ARCHITECTURE ATLAS.....274
Institutional Digital Real Estate Capital Markets Infrastructure.....274
Multi-Volume Documentation Package — Volume VII of VII.....274
TITLE PAGE & DOCUMENT CONTROL.....275
HOW TO READ THIS ATLAS (CONTROL FILE).....275
DETAILED TABLE OF CONTENTS.....276
LIST OF FIGURES (VOLUME VII).....276
EXECUTIVE SUMMARY.....277
CHAPTER 1 — THE C4 MODEL (CONTEXT → CONTAINER → COMPONENT).....278
1.1 Level 1 — System context.....278

1.2 Level 2 — Container view....278
1.3 Level 3 — Component: on-chain compliance & token suite....279
1.4 Level 3 — Component: off-chain services & oracle....279
CHAPTER 2 — CONTRACT & DATA MODELS (CODE · ENTITY-RELATIONSHIP · DOMAIN)....280
2.1 Code — the ERC-3643 contract model....280
2.2 Entity-relationship — the platform data model....281
2.3 Domain class model — platform services....281
CHAPTER 3 — LIFECYCLE, STATE & INTERACTIONS....282
3.1 The ledger-based security lifecycle....282
3.2 Primary issuance & compliant subscription....284
3.3 Secondary trade with atomic DvP....284
3.4 NAV update & proof-of-reserve gating....285
CHAPTER 4 — CROSS-CUTTING CONSOLIDATED VIEWS....285
4.1 End-to-end reference architecture....285
4.2 Security & key architecture (consolidated)....286
4.3 Governance & assurance (consolidated)....286
4.4 Trust boundaries & data classification....287
CHAPTER 5 — MASTER DIAGRAM INDEX (VOLUMES I–VI)....287
5.1 Volume I — Executive & Regulatory (15 figures)....288
5.2 Volume II — Technical Architecture (17 figures)....288
5.3 Volume III — Marketplace & Trading (15 figures)....289
5.4 Volume IV — Financial Intelligence (13 figures)....290
5.5 Volume V — Security & Operations (14 figures)....290
5.6 Volume VI — Business & Financial Model (12 figures)....291
5.7 Coverage summary....291

INTERIM NOTE & HANDOVER TO THE CROSS-VOLUME AUDIT.....292

GLOSSARY (POINTER).....292

APPENDIX A — NOTATION LEGEND.....292

APPENDIX B — CROSS-VOLUME FIGURE MAP (ATLAS → SOURCES).....293

DIAGRAM INVENTORY (Volume VII).....294

END OF VOLUME VII (interim draft) — END OF THE SEVEN-VOLUME PACKAGE (drafts).....295

VOLUME I — EXECUTIVE & REGULATORY

Institutional Digital Real Estate Capital Markets Infrastructure

Multi-Volume Documentation Package — Volume I of VII

TITLE PAGE & DOCUMENT CONTROL

Field	Detail
Document	Volume I — Executive & Regulatory
Package	Institutional Digital Real Estate Capital Markets Infrastructure (7 volumes)
Status	Working draft for internal review and counsel sign-off — **not for regulatory submission or investor reliance in this form**
Version	I-0.1 (interim; full cross-volume Compliance & Completeness Audit pending completion of Volume VII)
Date of documentation	30 June 2026
Classification	Confidential — Draft
Jurisdictional priority	Switzerland (primary) → United Arab Emirates / Dubai (secondary) → Liechtenstein, Singapore, Hong Kong (supported), with EEA/MiCA analysis for cross-border activity

Authoring team (internal, fictional roles — see §2.4 for the responsibility map). This volume is authored by the platform's internal working group: the Chief Legal & Regulatory Officer (lead), Securities & Capital Markets Counsel, Tax Counsel, Data-Protection Counsel, Head of Financial Crime / MLRO, Chief Risk Officer (model & operational risk), Chief Product Officer, Lead Solution Architect, and the Head of Vendor & Outsourcing Risk. No part of this document is authored by, or on behalf of, any named external firm; published work by professional-services firms, market infrastructures, and standards bodies is referenced only as benchmark and is cited.

> **Authorship and reliance caveat (read first).** This documentation is an AI-assisted drafting and due-diligence aid prepared to institutional standards of rigour. Legal-article numbers, standards references, and statutory wording cited here have been checked against official or primary sources at the date of documentation and are footnoted to those sources. Nevertheless, this is a draft: **it must be reviewed and signed off by qualified counsel admitted in each relevant jurisdiction — Swiss securities, tax, and regulatory counsel first — before any regulatory submission, capital raise, or investor reliance.** Where the precise wording of a provision could not be independently

retrieved, the requirement is stated in general terms and the gap is flagged; no citation has been fabricated. Statutory texts reproduced or pointed to in the appendices are official-source materials (statutes are not subject to copyright); all other source material is paraphrased.

HOW TO READ THIS VOLUME (Control File — seed)

This is the first of seven self-contained volumes. Because the package is produced one volume per turn, a **Control File** (condensed master glossary, cross-reference index, and verified-citation register) is reproduced at the top of every volume **after** this one. Volume I **establishes** that Control File:

- **Controlled vocabulary.** One canonical term per concept. Where the market uses synonyms, the canonical term is used throughout and the synonym is mapped as *deprecated* in the Glossary (see Glossary, end of volume). Example: the canonical term is **“ledger-based security”** (the official English rendering of *Registerwertrecht*); the synonyms “DLT security”, “uncertificated register security (URS)”, and “tokenised security” are noted but not used interchangeably where precision matters.
- **Cross-reference anchors.** Internal references use the form `[Vol. I §4.1]`. Forward references to material that will appear in later volumes are listed in the Cross-Reference Index (Appendix E) and **must be resolved before final delivery**; none is left as a vague summary.
- **Citation register.** Every external source relied on is listed in the Citation Register (Appendix D) with a verification note. A source that could not be confirmed is not cited.

Formatting convention: **design options** (choices among alternatives, or proposals not yet established fact) are explicitly labelled *“Design option”* with their trade-offs. Established legal or technical facts are stated plainly and cited.

DETAILED TABLE OF CONTENTS

Front matter — Title page & document control · How to read this volume · List of figures · List of tables · Executive summary

Body - **Chapter 1 — Token Classification (lead analysis)** - 1.1 Why classification comes first - 1.2 The Swiss FINMA token taxonomy (substance over form) - 1.3 Classification of the platform’s instruments - 1.4 Liechtenstein FMA substance-over-form alignment - 1.5 EEA activity: MiCA / MiFID II carve-out, ART/EMT, DORA - 1.6 The settlement asset as a distinct classification problem - 1.7 Classification summary matrix - **Chapter 2 — Strategic Vision, Operating Model & Governance** - 2.1 Strategic vision and market context - 2.2 The platform as a domain map - 2.3 Dual-mode

operating model - 2.4 Governance, organisation and the responsibility map (RACI) - 2.5 On-chain vs. off-chain governance - **Chapter 3 — Dual-Mode Funding & Capital Formation (legal architecture)** - 3.1 Model A — Asset-Backed Issuance - 3.2 Model B — Forward-Funding / Development Finance - 3.3 Special-purpose vehicle (SPV) structures - 3.4 On-chain subscription, capital-call and escrow mechanics - 3.5 Investor eligibility and accreditation - **Chapter 4 — Swiss Regulatory Foundation** - 4.1 DLT Act and CO Art. 973d–973i mapping - 4.2 FinSA prospectus regime and key information document - 4.3 FinfraG / DLT Trading Facility licensing - 4.4 AMLA / AMLO-FINMA anti-money-laundering regime - 4.5 Collective Investment Schemes Act (CISA) boundary analysis - 4.6 Bankruptcy remoteness and client-asset segregation - **Chapter 5 — Secondary Jurisdiction: United Arab Emirates (VARA)** *(Part 2)* - **Chapter 6 — Additional Jurisdictions: Liechtenstein, Singapore, Hong Kong** *(Part 2)* - **Chapter 7 — Cross-Border AML/CFT, Sanctions, CRS/FATCA** *(Part 2)* - **Chapter 8 — Tax, Accounting & Regulatory-Reporting Automation** *(Part 2)* - **Chapter 9 — Data Protection & Privacy** *(Part 2)* - **Chapter 10 — Vendor & Outsourcing Risk Management** *(Part 2)* - **Chapter 11 — Competitive Landscape, Industry Threats & Limitations** *(Part 2)*

Tail — Interim Compliance & Completeness Audit (Volume I) · Future Jurisdiction Compatibility Notes · Glossary · Appendices A–E · Diagram Inventory

---

LIST OF FIGURES

Figure	Title	Section
1	Platform domain map	2.2
2	Dual-mode operating model	2.3
3	Governance and three-lines-of-defence	2.4
4	Indicative organisation chart	2.4
5	Asset-backed issuance — SPV and rights structure	3.1
6	Forward-funding — SPV, escrow and drawdown structure	3.2
7	Token-classification decision tree	1.3
8	Ledger-based security lifecycle (CO 973d–973i) — state machine	4.1
9	Forward-funding milestone-drawdown sequence	3.4
10	On-chain subscription and capital-call sequence	3.4
11	AML/CFT onboarding and	4.4

Figure	Title	Section
	monitoring flow	
12	Collective-investment-scheme boundary decision tree	4.5
13	Regulatory-pathway roadmap (Switzerland-first) — Gantt	4.3

(Figures 14+ appear in Part 2 and later volumes; see Diagram Inventory.)

LIST OF TABLES

Table	Title	Section
1	Token classification across regimes	1.7
2	CO Art. 973d–973i — article-by-article mapping	4.1
3	FinSA prospectus duty and exemptions	4.2
4	Legal-event → on-chain-state mapping (both models)	Appendix B
5	RACI matrix (governance)	Appendix C
6	Jurisdiction comparison matrix	Ch. 6 (Part 2)
7	Industry threats and limitations register	Ch. 11 (Part 2)
8	Citation register	Appendix D

EXECUTIVE SUMMARY

What this is. The platform is an institutional-grade infrastructure for raising and trading capital against real estate using ledger-based securities. It is deliberately **not** a decentralised-finance (DeFi) protocol, a startup minimum-viable product, or a retail crypto venue. It is a permissioned, hybrid distributed system operated under recognised financial-market law, targeting family offices, accredited and qualified investors, private-wealth and asset managers, banks, and institutions.

Two origination models, one infrastructure. The platform supports two distinct ways of forming capital, regulated and engineered separately but sharing common rails:

1. **Asset-Backed Issuance (Model A).** An existing, income-producing property (or portfolio) is legally wrapped in a special-purpose vehicle, independently valued, and fractionalised into tokens that confer rights to existing rental income and capital appreciation. The classification, valuation and disclosure are anchored in a present, verifiable asset.

2. **Forward-Funding / Development Finance (Model B).** A sponsor proposes a plan (land acquisition, construction, refurbishment) and raises capital before or during asset creation. Tokens represent a claim on a *future* asset and its income, governed by drawdown schedules, milestone-based escrow releases, and completion-risk management. Model B carries materially higher disclosure, completion-risk and collective-investment-scheme considerations than Model A.

Regulatory spine (Switzerland first). The instruments are structured as **ledger-based securities** under Swiss Code of Obligations (CO) Art. 973d–973i, introduced by the 2021 DLT Act.[1] Under the FINMA token taxonomy they are **asset tokens**, hence **securities**.[2] Public offers engage the **FinSA** prospectus regime (with defined exemptions for professional-client and limited offerings).[3] A multilateral secondary venue engages the **DLT Trading Facility** licence introduced into the Financial Market Infrastructure Act (FinfraG/FMIA).[4] Anti-money-laundering duties arise under the **AMLA**; the **CISA** collective-investment boundary must be actively managed, especially for Model B and for any pooled/managed structure.

Why this is hard, stated honestly. Three structural risks dominate Volume I and recur throughout the package: (i) the **collective-investment-scheme boundary** — a pooled, third-party-managed vehicle can inadvertently become a regulated fund (see [Vol. I §4.5]); (ii) the **physical–digital enforceability gap** — a token's on-chain transfer must map to enforceable off-chain rights and, ideally, to the land register and SPV cap table (see [Vol. I §3.3] and Volume II's oracle/registry architecture); and (iii) **completion risk** in Model B — investors fund an asset that does not yet exist, requiring escrow, milestone verification and stress scenarios (see [Vol. I §3.4] and Volume V's development-phase run scenarios).

What the reader should do with this volume. Treat Chapters 1, 3 and 4 as the load-bearing legal analysis; Chapter 2 as the operating and governance frame; Chapters 5–7

---

[1] Swiss Code of Obligations, Art. 973d–973i (ledger-based securities / *Registerwertrechte*), introduced by the DLT Act, in force 1 Feb 2021. Official text: Fedlex SR 220, https://www.fedlex.admin.ch/eli/cc/27/317_321_377/en (verify verbatim wording at compile).

[2] FINMA, "Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)", 16 Feb 2018 — payment/utility/asset token taxonomy; asset tokens treated as securities. https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

[3] Financial Services Act (FinSA / FIDLEG), SR 950.1 — Art. 35 (prospectus duty), Art. 36 (exemptions), Art. 40–51 (content/review), Art. 58–66 (KID). Official text: Fedlex, https://www.fedlex.admin.ch/eli/cc/2019/758/en

[4] Financial Market Infrastructure Act (FinfraG/FMIA) — DLT Trading Facility, Art. 73a et seq., introduced by the DLT Act. (Verify article range and verbatim text at compile.)

(Part 2) as the multi-jurisdiction extension; and Chapters 8–11 (Part 2) as the tax, data-protection, vendor-risk and competitive context. Every regulated design choice is paired with its rationale and trade-offs, and every cited provision is registered in Appendix D.

CHAPTER 1 — TOKEN CLASSIFICATION (LEAD ANALYSIS)

1.1 Why classification comes first

Everything downstream — whether a prospectus is owed, which licence the venue needs, whether anti-money-laundering rules bite, how the asset is taxed, and which investors may participate — turns on **what the token legally is**. Classification is therefore the first analytical step, not a labelling exercise performed after the product is built. The governing principle across all five jurisdictions in scope is **substance over form**: the regulator looks through the "token" wrapper to the economic function and the rights conferred.[56]

1.2 The Swiss FINMA token taxonomy (substance over form)

FINMA's ICO Guidelines (16 February 2018) set out a taxonomy that remains the Swiss reference point. FINMA assesses the **economic function** and **transferability** of a token and recognises three categories, with hybrids possible:[78]

- **Payment tokens** (synonymous with cryptocurrencies): intended as a means of payment or value transfer, with no claim on an issuer. They are **not** treated as securities, but their issuance/transfer can trigger anti-money-laundering rules.

---

[5] FINMA, "Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)", 16 Feb 2018 — payment/utility/asset token taxonomy; asset tokens treated as securities. https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

[6] ESMA, "Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments" (2025) — substance-over-form; MiFID II Art. 4(1)(15).

[7] FINMA, "Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)", 16 Feb 2018 — payment/utility/asset token taxonomy; asset tokens treated as securities. https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

[8] FINMA, "Developments in FinTech" dossier (token definitions; asset tokens analogous to equities/bonds/derivatives).

- **Utility tokens**: confer digital access to an application or service. They are **not** securities **if** their sole purpose is access **and** they are usable at issuance; a utility token with an investment function is treated cumulatively.
- **Asset tokens**: represent assets — a debt or equity claim on the issuer, a share in future earnings or capital flows, or the digital representation of a physical underlying. In economic terms they are analogous to equities, bonds or derivatives. **FINMA treats asset tokens as securities.**[9]

Hybrids attract **cumulative** requirements (e.g., a token that is both utility and payment is subject to both regimes).

1.3 Classification of the platform's instruments

Both Model A and Model B tokens confer rights to income and/or capital appreciation derived from real estate held (or to be created) within an SPV. They are standardised, fractionalised, and intended to be transferable among eligible investors. On the FINMA test:

- **Economic function** — investment: entitlement to income (rent / development profit) and capital return. This is the defining feature of an **asset token**.
- **Transferability / standardisation** — designed for mass-standardised holding and (eligible) transfer.

Conclusion: the platform's funding instruments are **asset tokens and therefore securities** under Swiss law, and — because they are structured by registration agreement on a qualifying ledger — they are **ledger-based securities** under CO Art. 973d–973i (see [Vol. I §4.1]).[10][11] This conclusion is robust for both models; Model B differs not in *category* but in the *nature of the underlying claim* (a future asset) and hence in disclosure and risk treatment.

---

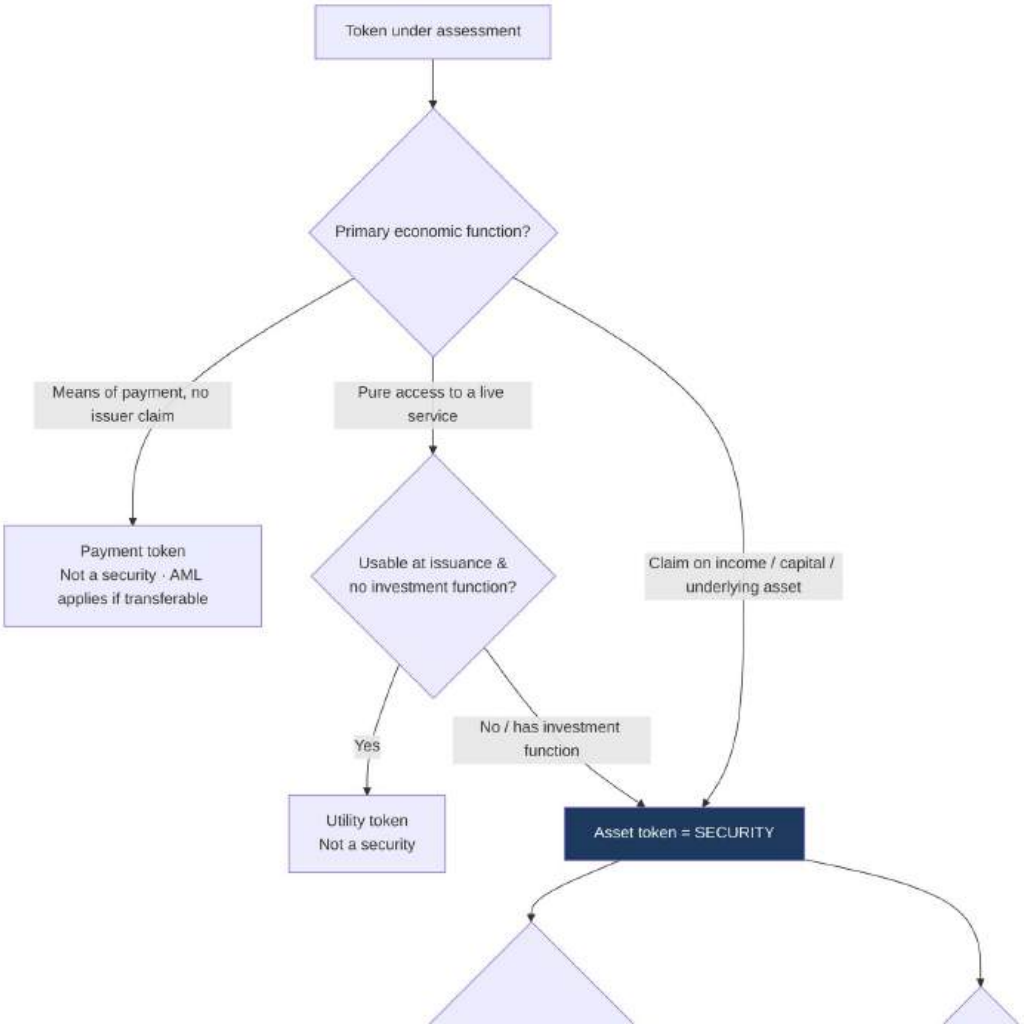
[9] FINMA, "Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)", 16 Feb 2018 — payment/utility/asset token taxonomy; asset tokens treated as securities. https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

[10] Swiss Code of Obligations, Art. 973d–973i (ledger-based securities / *Registerwertrechte*), introduced by the DLT Act, in force 1 Feb 2021. Official text: Fedlex SR 220, https://www.fedlex.admin.ch/eli/cc/27/317_321_377/en (verify verbatim wording at compile).

[11] FINMA, "Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)", 16 Feb 2018 — payment/utility/asset token taxonomy; asset tokens treated as securities. https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

Design option — instrument form within the asset-token class. The token may represent (a) **equity** in the property SPV (participation, dividend/appreciation rights), (b) **debt** (a bond-like claim with fixed/variable coupon), or (c) a **participation/profit-participation right**. Trade-offs: equity maximises upside alignment but raises corporate-law and CISA-boundary questions; debt is simpler to price and ring-fence but caps upside and engages bond-prospectus content; profit-participation rights are flexible but less familiar to some institutional allocators. The choice is made per issuance and documented in the offering terms; it materially affects tax treatment (see [Vol. I §8]) and the CISA analysis (see [Vol. I §4.5]).

Figure 7 — Token-classification decision tree. *Reads top to bottom; the platform's funding tokens follow the right-hand "asset token / security" path.*



1.4 Liechtenstein FMA substance-over-form alignment

Liechtenstein's **Token and TT Service Provider Act (TVTG)**, in force 1 January 2020, uses the **Token Container Model**: a token is a neutral "container" that can hold *any* right — money-like value, securities, rights to real estate, or other absolute/relative rights.[12][13] The legal character of the token follows the right it contains. Where the contained right is an investment claim equivalent to a security, Liechtenstein financial-market law (and, via the EEA, EU law — see §1.5) applies; the TVTG itself is **not** part of financial-market law, and TT service providers are not, by that fact alone, financial intermediaries.[14] The practical effect is the same substance-over-form result as Switzerland: a real-estate income/appreciation claim in a token is treated as a security/financial instrument.

[12] Liechtenstein Token and TT Service Provider Act (TVTG), in force 1 Jan 2020 — Token Container Model; Art. 2(1) service-provider roles incl. Physical Validator. tokenizestartup.com guide.

1.5 EEA activity: MiCA / MiFID II carve-out, ART/EMT, DORA

For any activity within the European Economic Area (relevant directly to Liechtenstein and to cross-border solicitation of EEA investors), the **Markets in Crypto-Assets Regulation (MiCAR, Reg (EU) 2023/1114)** matters only at its boundary. **MiCAR Art. 2(4)(a) excludes crypto-assets that qualify as financial instruments under MiFID II** (Directive 2014/65/EU, Art. 4(1)(15)).[15][16] Because the platform's tokens are securities/financial instruments, they fall **outside** MiCAR and remain under the MiFID II / Prospectus Regulation / national-securities-law stack. There is therefore **no blanket MiCA exclusion to assert** — the analysis is positive: *these are MiFID instruments, so MiCAR does not apply to them.*

Two MiCAR-adjacent points still bind:

- **Settlement asset (ART/EMT).** If the platform uses or issues a stablecoin as on-chain settlement, that instrument may be an **e-money token (EMT)** or **asset-referenced token (ART)** under MiCAR Titles III–IV (in application since 30 June 2024), which is a *different* classification problem from the funding token (see §1.6).[17]
- **DORA.** Any in-scope EU financial entity — and crypto-asset service providers — fall under the **Digital Operational Resilience Act (DORA, Reg (EU) 2022/2554)**, applicable since 17 January 2025, covering ICT risk management, incident reporting, resilience testing and third-party (ICT) oversight.[18] DORA

---

[13] Liechtenstein FMA, "Token and TT Service Provider Act (TVTG)" — TVTG not part of financial-market law; FATF-aligned supervision.

[14] Liechtenstein FMA, "Token and TT Service Provider Act (TVTG)" — TVTG not part of financial-market law; FATF-aligned supervision.

[15] Markets in Crypto-Assets Regulation (MiCAR), Reg (EU) 2023/1114 — Art. 2(4)(a) financial-instrument carve-out; Titles III–IV (ART/EMT) in application 30 June 2024; remainder 30 Dec 2024. Official consolidated text, Official Journal (EUR-Lex): https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng

[16] ESMA, "Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments" (2025) — substance-over-form; MiFID II Art. 4(1)(15).

[17] Markets in Crypto-Assets Regulation (MiCAR), Reg (EU) 2023/1114 — Art. 2(4)(a) financial-instrument carve-out; Titles III–IV (ART/EMT) in application 30 June 2024; remainder 30 Dec 2024. Official consolidated text, Official Journal (EUR-Lex): https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng

[18] Digital Operational Resilience Act (DORA), Reg (EU) 2022/2554, applicable 17 Jan 2025; applies to CASPs and EU financial entities. Official text, Official Journal (EUR-Lex): https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

obligations are picked up in Volume V (security & operations) and Volume II (architecture).

Time-sensitive note. MiCAR's transitional ("grandfathering") regime for crypto-asset service providers runs to **1 July 2026** (subject to shorter national windows).[19] As the date of documentation is 30 June 2026, any EEA-facing CASP activity must confirm its authorisation status immediately with the relevant national competent authority; this window is effectively closing and must be verified by counsel.

1.6 The settlement asset as a distinct classification problem

On-chain settlement requires a value leg. The options and their classification consequences:

Settlement leg	Likely classification	Key considerations
Tokenised bank deposit (claim on a regulated bank)	Bank deposit / book money; not a stablecoin	Strongest legal footing; depends on a willing regulated bank; intraday liquidity and cut-off times
Regulated EUR/CHF stablecoin	EMT/ART under MiCAR (EEA); e-money/payment-token analysis (CH)	Redemption risk, reserve quality, issuer authorisation; MiCAR Titles III–IV if EEA
Off-chain fiat (SEPA Instant /	Outside token classification	No on-chain atomicity; reconciliation

[19] MiCAR CASP transitional regime to 1 July 2026 (subject to shorter national windows). Dechert.

Settlement leg	Likely classification	Key considerations
SWIFT)		and settlement-finality timing gaps

Design option — settlement asset. The platform should select per-corridor and justify the choice against liquidity, redemption risk, legal finality and operational complexity. The full technical and risk treatment (delivery-versus-payment, Fireblocks/MPC custody, SEPA Instant / SWIFT gpi integration) is in Volume II; the trading-venue settlement design is in Volume III. *No "we will use a stablecoin" statement is made without naming the instrument, its issuer authorisation, and its redemption mechanics at the point of selection.*

1.7 Classification summary matrix

Table 1 — Token classification across regimes.

Jurisdiction / regime	Governing test	Result for the platform's funding token	Result for a settlement stablecoin
Switzerland — FINMA taxonomy	Economic function + transferability (substance over form)[20]	**Asset token = security**; ledger-based security (CO 973d–973i)	Payment-token / e-money analysis; AML in scope
Switzerland — civil law	CO 973d–973i registration agreement on qualifying ledger[21]	**Ledger-based security**	Generally not a ledger-based security
Liechtenstein — TVTG	Token Container Model; right contained governs[22]	Security/financial-instrument right in a container	Token containing a payment/e-money right
EEA — MiCAR/MiFID II	Art. 2(4)(a) financial-instrument carve-out[23][24]	**Outside MiCAR** → MiFID II / Prospectus Regulation	**EMT/ART under MiCAR** Titles III–IV

[20] FINMA, "Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)", 16 Feb 2018 — payment/utility/asset token taxonomy; asset tokens treated as securities. https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

[21] Swiss Code of Obligations, Art. 973d–973i (ledger-based securities / *Registerwertrechte*), introduced by the DLT Act, in force 1 Feb 2021. Official text: Fedlex SR 220, https://www.fedlex.admin.ch/eli/cc/27/317_321_377/en (verify verbatim wording at compile).

[22] Liechtenstein Token and TT Service Provider Act (TVTG), in force 1 Jan 2020 — Token Container Model; Art. 2(1) service-provider roles incl. Physical Validator. tokenizestartup.com guide.

[23] Markets in Crypto-Assets Regulation (MiCAR), Reg (EU) 2023/1114 — Art. 2(4)(a) financial-instrument carve-out; Titles III–IV (ART/EMT) in application 30 June 2024; remainder 30 Dec 2024. Official consolidated text, Official Journal (EUR-Lex):

Jurisdiction / regime	Governing test	Result for the platform's funding token	Result for a settlement stablecoin
UAE — VARA	Virtual-asset issuance rulebook; ARVA = asset-referenced VA[25][26]	**ARVA**, Category 1 issuance	FRVA (fiat-referenced) / payment-token rules
Singapore — MAS	"Same activity, same risk, same regulatory outcome"; SFA CMP[27][28]	**Capital-markets product** (tokenised security)	Digital payment token (PS Act)
Hong Kong — SFC	SFO "securities"; tokenised security = security + tokenisation overlay[29][30]	**Tokenised security** (SFO applies)	Stablecoin under Stablecoins Ordinance (HKMA)

Reading: the funding token is consistently a security/financial instrument across all five jurisdictions; the settlement stablecoin is a separate, payment-side classification. The two must never be conflated in the offering documents.

---

https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng

[24] ESMA, "Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments" (2025) — substance-over-form; MiFID II Art. 4(1)(15).

[25] VARA / Dubai real-estate tokenisation — ARVA classification; Category 1 issuance; DLD/Prypco sandbox. Summary.

[26] Linklaters, "Virtual Assets regulation in Dubai: VARA issues updates to its Rulebooks" — Rulebooks v2.0 effective 19 June 2025; ARVA/FRVA; client-asset segregation in insolvency; Sponsored VASP.

[27] Bird & Bird, "MAS issues revised Guide on Tokenisation of Capital Markets Products" (Dec 2025) — "same activity, same risk, same regulatory outcome"; tokenised CMPs under SFA/FAA.

[28] Lexology, "At a glance: cryptoassets for investment and financing in Singapore" — CMP definition (SFA s 2); STOs as offers of CMPs; accredited/institutional exemptions.

[29] Charltons, "Hong Kong SFC Expands VATPs' Permitted Products and Services" (Nov 2025) — tokenised securities as a subset of digital securities; SFO; AMLO s 53ZRA; Stablecoins Ordinance.

[30] Davis Polk, "Hong Kong permits virtual asset exchanges to access global liquidity…" (3 Nov 2025 circulars) — VATP regime in force 1 June 2023; tokenised-securities track-record relief.

CHAPTER 2 — STRATEGIC VISION, OPERATING MODEL & GOVERNANCE

2.1 Strategic vision and market context

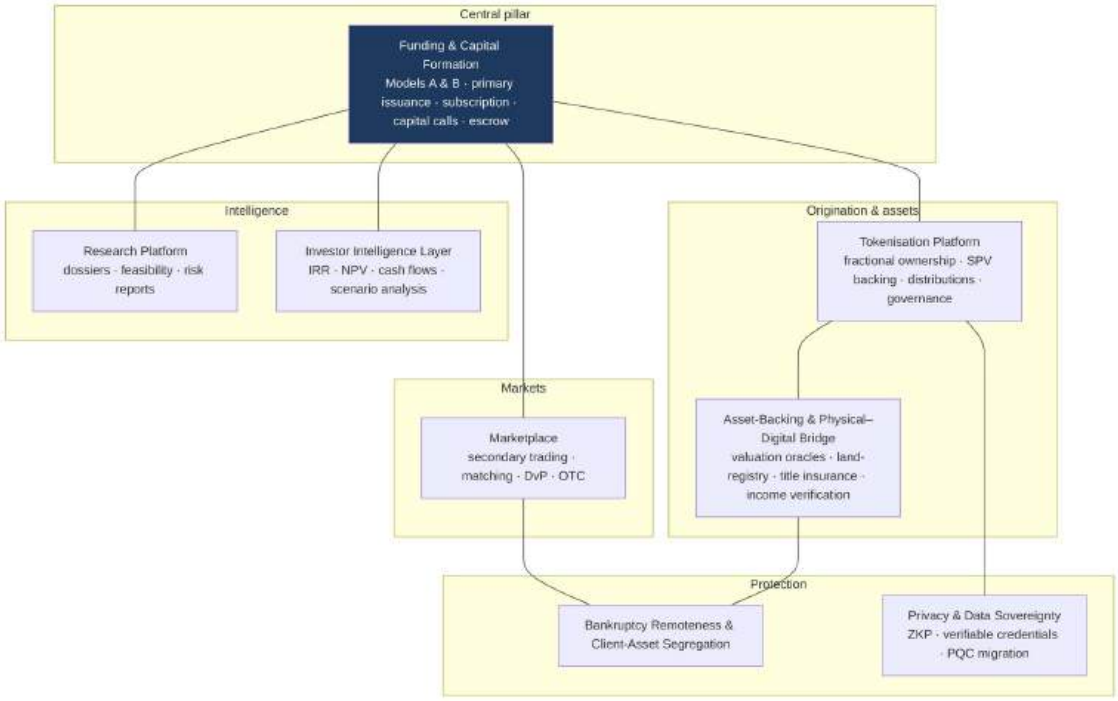
The platform's thesis is that real estate — a large, illiquid, operationally intensive asset class — can be made **fractionally ownable, transferable among eligible investors, and operationally transparent** by representing legally enforceable claims as ledger-based securities, **without** abandoning the investor protections of recognised financial-market law. The differentiator versus first-generation tokenisation efforts is institutional discipline: a regulated venue, bankruptcy-remote structuring, independent valuation, a verifiable physical–digital bridge, and dual-mode capital formation (existing assets *and* development finance) on shared rails.

Market context and benchmarks (tokenised real-world assets, regulated digital-asset venues, and tokenised funds) are surveyed in Chapter 11 (Part 2); concrete public reference points — e.g., Dubai Land Department's tokenised-property pilot under the VARA/CBUAE sandbox[31] — show the direction of travel without being relied upon as the platform's own claims.

2.2 The platform as a domain map

Figure 1 — Platform domain map. *Funding & Capital Formation is the central pillar; the other domains support origination, trading, intelligence, the physical–digital bridge, and protection.*

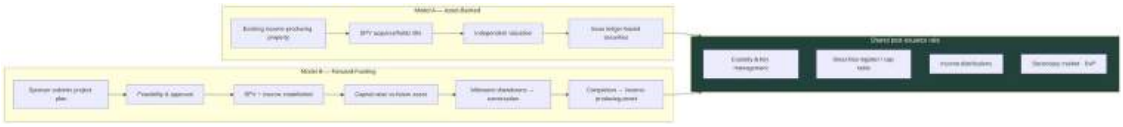
[31] VARA / Dubai real-estate tokenisation — ARVA classification; Category 1 issuance; DLD/Prypco sandbox. Summary.



Caption: Each domain maps to later volumes — Tokenisation/architecture and the physical–digital bridge to Volume II; Marketplace to Volume III; Research and Investor Intelligence to Volume IV; protection (custody, segregation, privacy, PQC) to Volume V.

2.3 Dual-mode operating model

Figure 2 — Dual-mode operating model. *Both models converge on the same post-issuance rails (custody, register, distributions, secondary market).*



Caption: Model B inserts feasibility, escrow, drawdown and completion-conversion stages ahead of the shared rails; Model A reaches them directly because the asset already exists.

2.4 Governance, organisation and the responsibility map (RACI)

Governance follows a **three-lines-of-defence** model with a clear separation between commercial origination and control functions.

Figure 3 — Governance and three lines of defence.

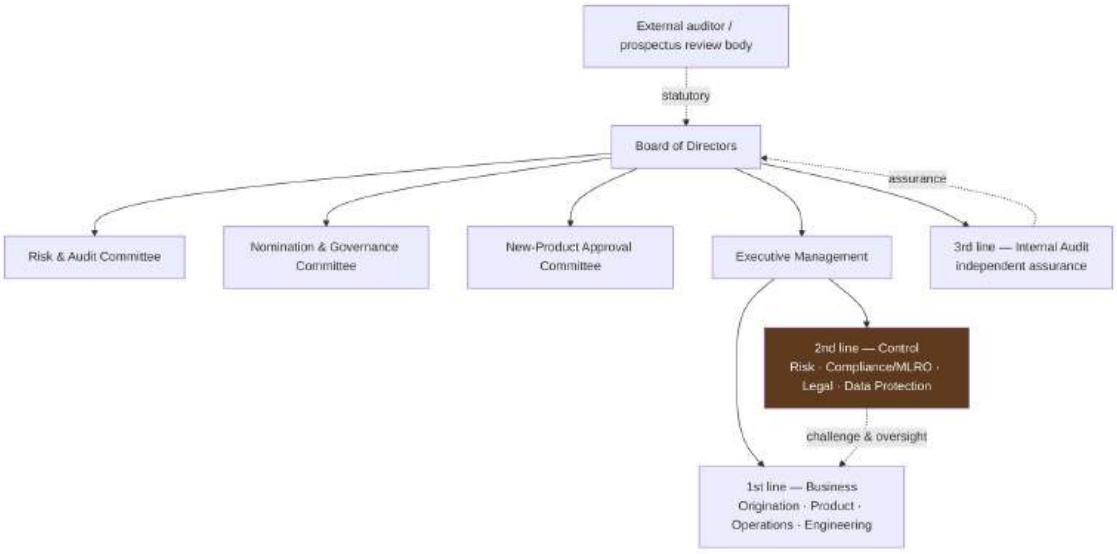


Diagram 04

Figure 4 — Indicative organisation chart.

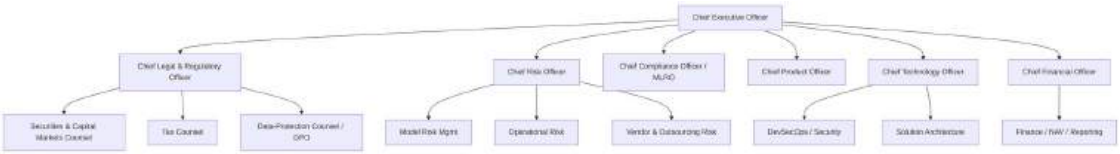


Diagram 05

The full **RACI matrix** (issuance approval, prospectus sign-off, AML onboarding, valuation, drawdown release, incident response, etc.) is in **Appendix C, Table 5**. Compliance workflows (onboarding, suitability, ongoing monitoring) are summarised in [Vol. I §4.4] and detailed operationally in Volume V.

2.5 On-chain vs. off-chain governance

A deliberate split is maintained:

- **Off-chain (legally controlling):** board and committee decisions, SPV corporate governance, prospectus approval, valuation sign-off, and the **registration agreement** that constitutively links each token to its right (CO 973f) (see [Vol. I §4.1]). The off-chain legal layer prevails in any conflict.
- **On-chain (executional):** issuance, transfer-restriction enforcement (eligibility/whitelisting), distributions, and capital-call/escrow logic, implemented under the ERC-3643 (T-REX) permissioned-token standard with UUPS-upgradeable contracts (architecture and upgrade-governance controls in Volume II).

Design option — upgrade governance. Upgradeable contracts (UUPS) create a tension between the need to fix/extend code and the immutability investors may expect. Trade-off resolution: time-locked, multi-signature upgrade authority with mandatory disclosure to holders, and an explicit statement in the offering terms that the registration agreement (not the code) governs the right. Detailed in Volume II and Volume V.

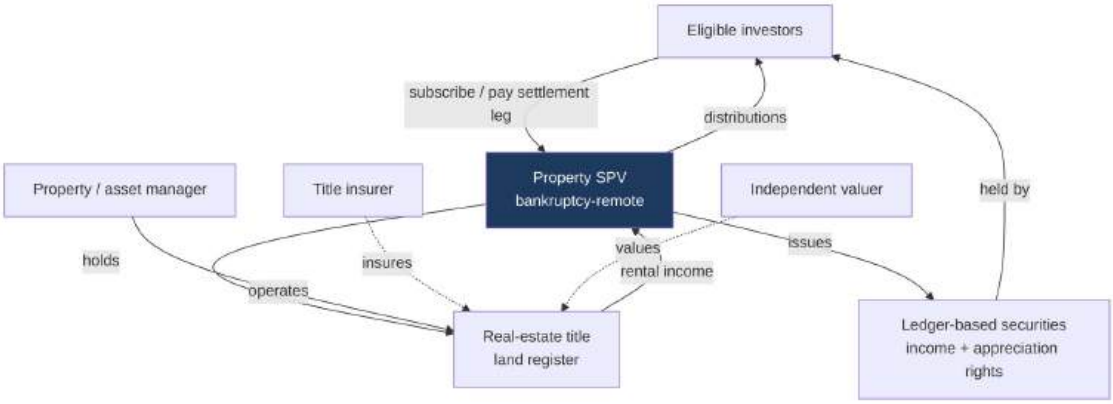
CHAPTER 3 — DUAL-MODE FUNDING & CAPITAL FORMATION (LEGAL ARCHITECTURE)

The Funding & Capital Formation pillar is where the platform's regulatory identity is most acute, because it is where **money is raised from investors**. Both models are described below with their legal anchors; the clause-by-clause legal-event → on-chain-state mapping for each is in **Appendix B, Table 4**.

3.1 Model A — Asset-Backed Issuance

Structure. An SPV acquires or already holds title to an existing income-producing property; the property is independently valued; the SPV issues ledger-based securities representing equity, debt, or participation rights (see [Vol. I §1.3]) entitling holders to existing rental income and capital appreciation.

Figure 5 — Asset-backed issuance: SPV and rights structure.



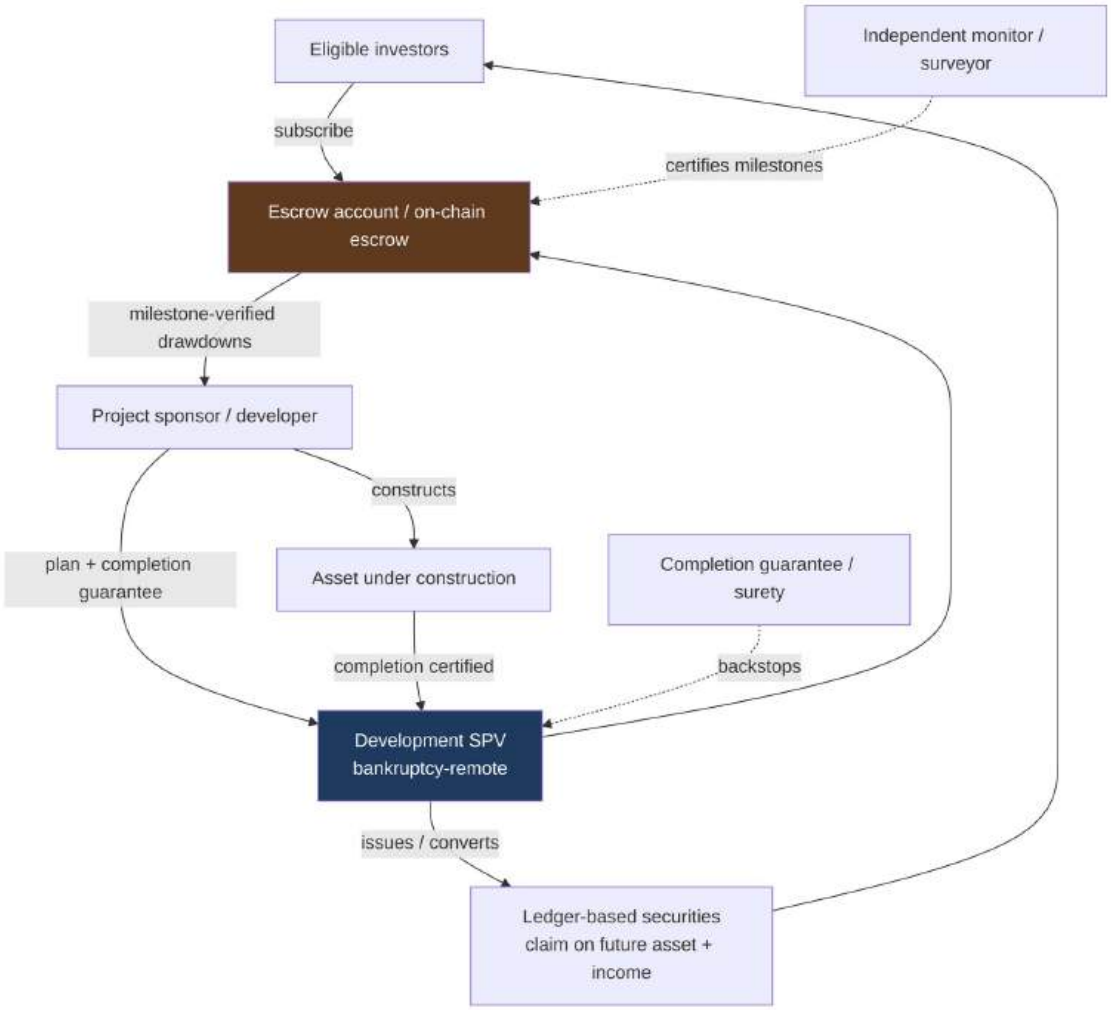
Caption: Income flows from the asset through the SPV to holders; title is verified against the land register and (design option) protected by title insurance. Valuation and the physical–digital bridge are detailed in Volume II and Volume IV.

Key legal points. (i) The SPV must genuinely own the asset and be bankruptcy-remote (see [Vol. I §4.6]); (ii) a public offer engages the FinSA prospectus regime unless an exemption applies (see [Vol. I §4.2]); (iii) the CISA boundary must be checked — a single-asset SPV with passive holders can resemble a fund (see [Vol. I §4.5]).

3.2 Model B — Forward-Funding / Development Finance

Structure. A sponsor proposes a development; after feasibility and approval, an SPV and an **escrow** are established; capital is raised against the *future* asset; funds are released to the sponsor in **milestone-based drawdowns**; on completion the asset becomes income-producing and converts to the Model-A steady state.

Figure 6 — Forward-funding: SPV, escrow and drawdown structure.



Caption: Escrow + independent milestone certification + completion guarantee are the completion-risk controls unique to Model B. Development-phase "fund run" stress scenarios are in Volume V.

Key legal points (incremental to Model A). (i) **Forward-looking statements** in the prospectus (construction timelines, projected yields) require careful disclosure and risk

warnings under FinSA;[32] (ii) **completion risk** must be disclosed and mitigated (escrow, milestones, guarantees); (iii) the **CISA boundary is more pressing** — pooled capital deployed by a sponsor toward a project can look like a collective investment scheme unless structured and disclosed appropriately (see [Vol. I §4.5]); (iv) **capital-call and drawdown mechanics** must be legally and technically enforceable (see §3.4).

3.3 Special-purpose vehicle (SPV) structures

The SPV is the legal container that (a) owns the asset, (b) issues the securities, and (c) achieves bankruptcy remoteness and client-asset segregation. **Design options** for the SPV jurisdiction and form:

- **Swiss SPV** (e.g., AG/SA or a contractual structure) — closest to the CO 973d–973i issuance and Swiss insolvency protections (see [Vol. I §4.6]); preferred for the primary, Switzerland-first design.
- **Liechtenstein SPV / Protected Cell Company (PCC)** — the PCC allows multiple ring-fenced cells under one legal entity, useful for portfolios and multi-tranche issuance; EEA-connected.[33]
- **UAE structure** — required where the asset and offering are Dubai-based and within VARA's perimeter (see Chapter 5, Part 2).

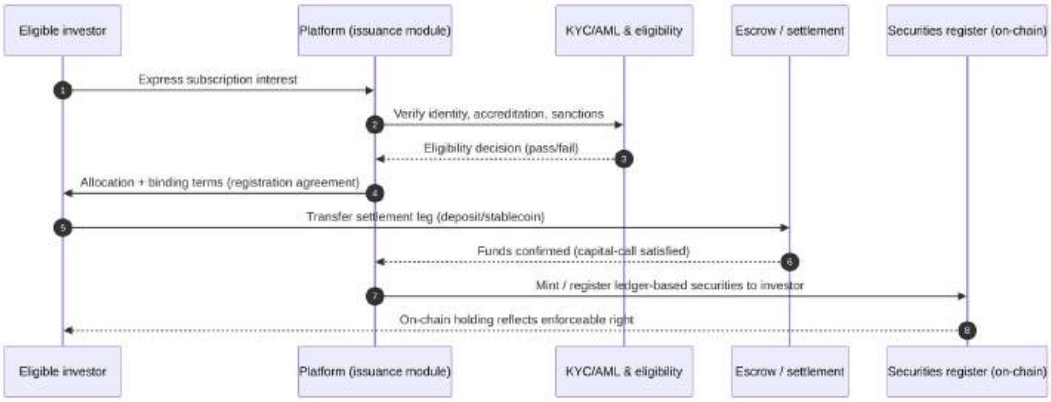
Trade-offs span insolvency protection, tax (see [Vol. I §8]), investor familiarity, and the enforceability of the physical–digital link. **A legal diagram for each SPV structure is provided per issuance**; Figures 5 and 6 above are the canonical Model-A and Model-B templates, and the per-jurisdiction variants appear in Chapter 5–6 (Part 2) and Volume VII (Architecture Atlas).

3.4 On-chain subscription, capital-call and escrow mechanics

Figure 10 — On-chain subscription and capital-call sequence.

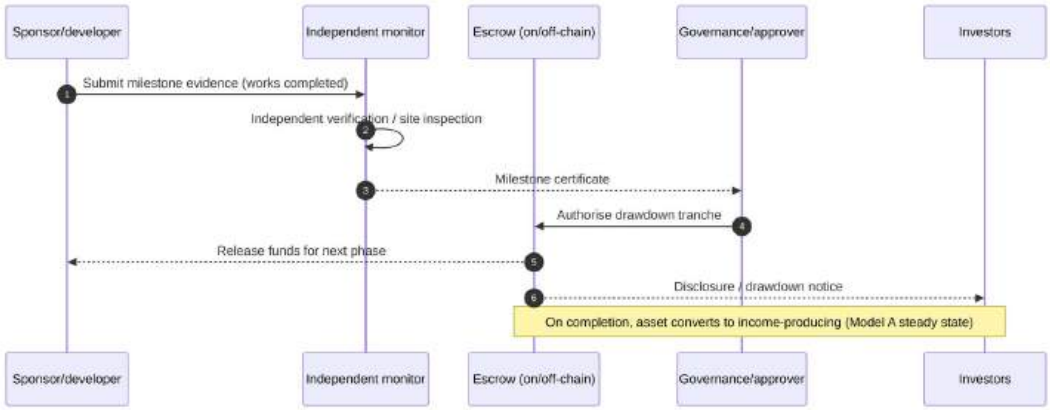
[32] Financial Services Act (FinSA / FIDLEG), SR 950.1 — Art. 35 (prospectus duty), Art. 36 (exemptions), Art. 40–51 (content/review), Art. 58–66 (KID). Official text: Fedlex, https://www.fedlex.admin.ch/eli/cc/2019/758/en

[33] European Blockchain Association, "Tokenizing Real-Assets in Liechtenstein" — Protected Cell Company for segregated multi-asset tokenisation.



Caption: Eligibility precedes allocation; settlement precedes registration. The registration agreement (off-chain, controlling) is referenced at allocation; the on-chain mint reflects — but does not replace — the legal right (CO 973f).

Figure 9 — Forward-funding milestone-drawdown sequence (Model B).



Caption: No drawdown without independent certification and governance authorisation — the core completion-risk control. Smart-contract escrow logic is specified in Volume II; stress scenarios in Volume V.

3.5 Investor eligibility and accreditation

Participation is restricted to **eligible investors** (family offices, accredited/qualified investors, professional clients, institutions). Eligibility is enforced both **off-chain** (onboarding, suitability) and **on-chain** (the ERC-3643 identity registry / whitelisting gates transfers to eligible addresses only). The precise eligibility set is jurisdiction-specific: Swiss FinSA “professional/institutional clients” (see [Vol. I §4.2]), UAE VARA professional-investor categories, Singapore “accredited/institutional investors” (see Chapter 6, Part 2), and Hong Kong “professional investors”. Restricting to professional/qualified investors is also the principal route to **prospectus exemption** (see [Vol. I §4.2]) and to managing the **CISA** and retail-protection rules.

CHAPTER 4 — SWISS REGULATORY FOUNDATION

Switzerland is the primary jurisdiction. This chapter maps the platform to the controlling Swiss statutes. **Every provision cited here is registered in Appendix D; the official-source text or pointer for each is in Appendix A.**

4.1 DLT Act and CO Art. 973d–973i mapping

The **Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology** ("DLT Act") amended several statutes; its core private-law innovation, the **ledger-based security (*Registerwertrecht*)**, was inserted into the Code of Obligations at **Art. 973d–973i** and took effect **1 February 2021**.[34][35] A ledger-based security is a right that, by agreement between the parties (the **registration agreement**), is recorded in a securities ledger and can be **asserted and transferred only via that ledger**; no written deed of assignment is required.[36][37]

The securities ledger must meet the requirements of **CO Art. 973d(2)**:[38][39] 1. **Power of disposal** — creditors (not the debtor) have power of disposal over their rights through technical means; 2. **Integrity** — protected against unauthorised modification by appropriate technical and organisational measures (e.g., joint administration by several

[34] Swiss Code of Obligations, Art. 973d–973i (ledger-based securities / *Registerwertrechte*), introduced by the DLT Act, in force 1 Feb 2021. Official text: Fedlex SR 220, https://www.fedlex.admin.ch/eli/cc/27/317_321_377/en (verify verbatim wording at compile).

[35] DLT Act overview — CO 973d et seq. effective 1 Feb 2021; insolvency-law amendments for segregation of crypto-based assets. CMS.

[36] Swiss Code of Obligations, Art. 973d–973i (ledger-based securities / *Registerwertrechte*), introduced by the DLT Act, in force 1 Feb 2021. Official text: Fedlex SR 220, https://www.fedlex.admin.ch/eli/cc/27/317_321_377/en (verify verbatim wording at compile).

[37] Pestalozzi Attorneys, "Ledger-based securities: introduction of DLT shares in Switzerland" — CO 973d(2) requirements; 973f transfer; 973g security interests. https://pestalozzilaw.com/en/insights/news/legal-insights/ledger-based-securities-introduction-dlt-shares-switzerland/

[38] Pestalozzi Attorneys, "Ledger-based securities: introduction of DLT shares in Switzerland" — CO 973d(2) requirements; 973f transfer; 973g security interests. https://pestalozzilaw.com/en/insights/news/legal-insights/ledger-based-securities-introduction-dlt-shares-switzerland/

[39] Lexology/CMS commentary on the Swiss DLT laws — Art. 973d(2) technical requirements; Art. 973i issuer disclosure and liability.

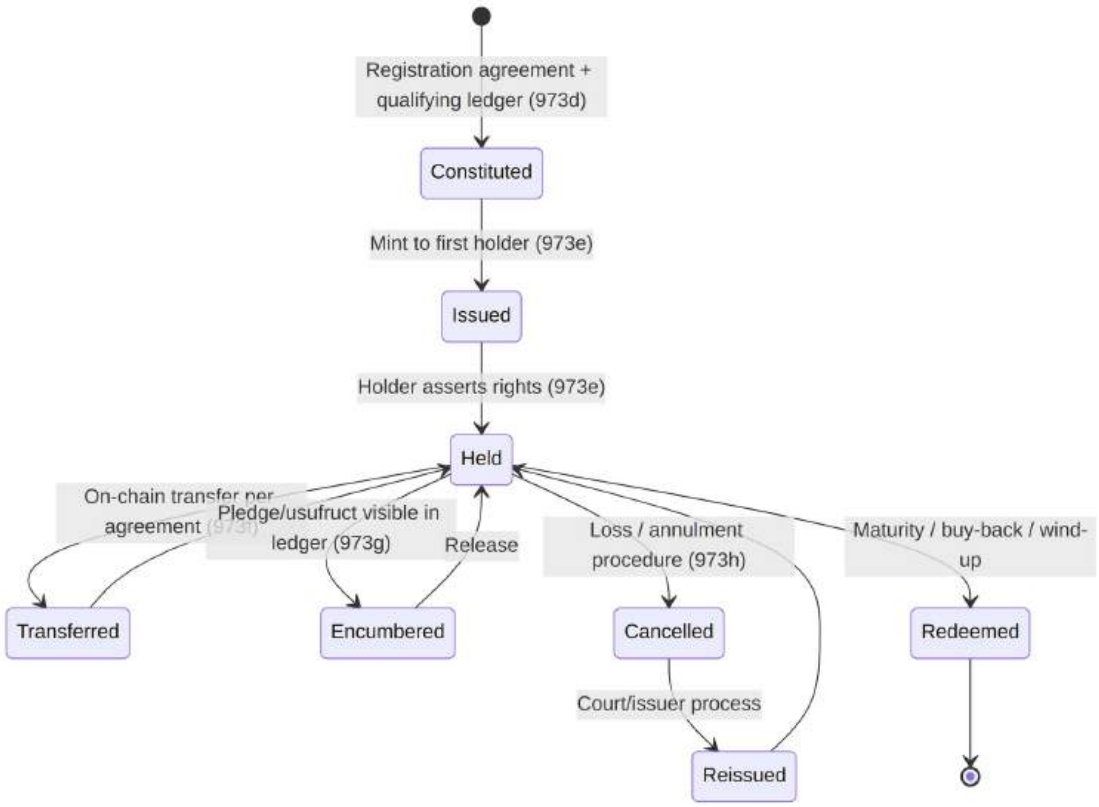
independent parties); 3. **Transparency of content** — the content of the rights, the functioning of the ledger, and the registration agreement are recorded in the ledger or in linked accompanying data; 4. **Public notice / verifiability** — creditors can access the relevant information and verify the integrity of the ledger independently of a third party.

Table 2 — CO Art. 973d–973i: article-by-article mapping to platform events.

Provision	What it governs	Platform mapping
Art. 973d	Definition; the four ledger requirements; debtor's duty to ensure the ledger operates per the registration agreement at all times	The chosen ledger (L2 rollup, then Avalanche — Volume II) must satisfy all four requirements; the platform documents how each is met
Art. 973e	Rights/defences; assertion of the right; protection of the obligor performing in good faith	Defines how holders assert income/redemption rights; obligor (SPV) performance rules
Art. 973f	**Transfer** of the ledger-based security per the registration agreement; no written assignment required; good-faith acquisition	On-chain transfer = legal transfer **because** the registration agreement so provides; eligibility gating sits here
Art. 973g	**Security interests** (e.g., pledge/usufruct) without transfer, if visible in the ledger	Enables tokens as collateral with on-ledger visibility
Art. 973h	**Cancellation / annulment** of a ledger-based security (e.g., on loss)	Lost-key / recovery and re-issuance procedures (Volume V) reference this
Art. 973i	**Issuer duty to inform** purchasers (features of the security, operating principles of the ledger, integrity measures) and **liability** for incorrect/misleading information	Disclosure content and issuer liability; aligns with FinSA prospectus completeness (Art. 51 FinSA)

Exact statutory wording: see Appendix A, with the official Fedlex source (SR 220). The mapping above is operative content, not a substitute for the verbatim text.

Figure 8 — Ledger-based security lifecycle (CO 973d–973i) — state machine.



4.2 FinSA prospectus regime and key information document

The **Financial Services Act (FinSA, SR 950.1)**, fully effective for prospectuses since 1 December 2020, imposes a **general duty to publish an approved prospectus** when securities are **publicly offered** in Switzerland or admitted to trading on a Swiss venue (**Art. 35 FinSA**).[40][41] Because the platform's tokens are securities, a public offer engages this duty **unless an exemption applies**.

Table 3 — FinSA prospectus duty and principal exemptions (Art. 36 FinSA).[42][43][44]

[40] Financial Services Act (FinSA / FIDLEG), SR 950.1 — Art. 35 (prospectus duty), Art. 36 (exemptions), Art. 40–51 (content/review), Art. 58–66 (KID). Official text: Fedlex, https://www.fedlex.admin.ch/eli/cc/2019/758/en

[41] VISCHER, "The Prospectus Requirement under the Financial Services Act" — Art. 35 duty (primary and secondary market).

[42] Financial Services Act (FinSA / FIDLEG), SR 950.1 — Art. 35 (prospectus duty), Art. 36 (exemptions), Art. 40–51 (content/review), Art. 58–66 (KID). Official text: Fedlex, https://www.fedlex.admin.ch/eli/cc/2019/758/en

Provision	Exemption (offer-type)	Relevance to the platform
Art. 35	*Duty*: public offer of securities / admission to trading	Baseline — applies to public token offers
Art. 36(1)(a)	Offer to **professional clients** only	Primary route for an institutional-only raise
Art. 36(1)(b)	Offer to **fewer than 500 investors**	Useful for tightly held issuances
Art. 36(1)(c)	Investors acquiring **≥ CHF 100,000** each	Sophistication proxy
Art. 36(1)(d)	**Minimum denomination ≥ CHF 100,000** per unit	Common for debt-form tokens
Art. 36(1)(e)	Total consideration **< CHF 8,000,000** over 12 months	Smaller raises (SME-scale)
Art. 36(5)	Federal Council may adjust the thresholds/numbers	Monitor for change

Additional points: a **Key Information Document (KID)** may be required for offers to retail clients (Art. 58–66 FinSA); prospectuses are reviewed by a FINMA-licensed **review body** (e.g., SIX Exchange Regulation; BX Swiss / Regservices); prospectus content/completeness is governed by Art. 40–51 FinSA and Annexes to the FinSO; and **wilful breach can attract criminal fines up to CHF 500,000**.[4546] For **Model B**, forward-looking statements (projected construction and yield) must be disclosed with appropriate assumptions and risk warnings and remain consistent, complete and understandable (Art. 51 FinSA).

Design option — exemption strategy. Restricting issuance to **professional clients** (Art. 36(1)(a)) is the cleanest route to avoid a full prospectus *and* to manage CISA/retail rules, at the cost of a smaller investor universe. A retail-facing offer requires a full reviewed prospectus and KID and materially higher cost and liability. The choice is documented per issuance.

[43] CapLaw, “Exemptions and Alleviations from the Duty to Publish a Prospectus under FinSA and FinSO” — Art. 36(1)(c)/(d)/(e) thresholds.

[44] IFLR, “Switzerland: New prospectus requirements in full effect” — review body; criminal fine up to CHF 500,000; FinSO Annex 1 content.

[45] IFLR, “Switzerland: New prospectus requirements in full effect” — review body; criminal fine up to CHF 500,000; FinSO Annex 1 content.

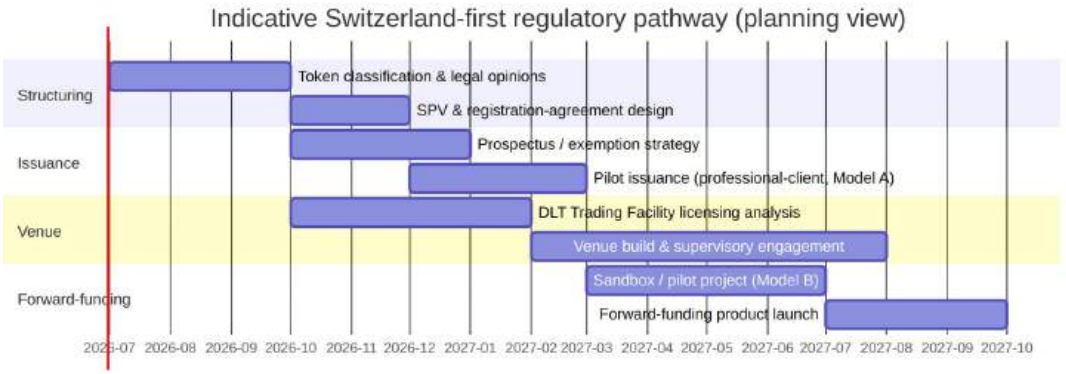
[46] Financial Services Act (FinSA / FIDLEG), SR 950.1 — Art. 35 (prospectus duty), Art. 36 (exemptions), Art. 40–51 (content/review), Art. 58–66 (KID). Official text: Fedlex, https://www.fedlex.admin.ch/eli/cc/2019/758/en

4.3 FinfraG / DLT Trading Facility licensing

The DLT Act introduced a bespoke financial-market-infrastructure category — the **DLT Trading Facility** — into the **Financial Market Infrastructure Act (FinfraG/FMIA)**, with the relevant provisions inserted at **Art. 73a et seq. FMIA**.[47][48] A DLT Trading Facility is a professionally operated venue for **multilateral trading of DLT securities** that, distinctively, may admit **natural persons and other non-supervised participants** directly (unlike a classic exchange/MTF), and may combine trading, central custody, clearing and settlement. The general FMIA licensing requirements apply, with the Federal Council empowered to set proportionate ("simplified") rules.[49]

Implication. Operating the platform's **secondary marketplace** as a multilateral venue for ledger-based securities points to a **DLT Trading Facility licence** (or operating within an existing licensed venue). If the venue's matching is non-discretionary and multilateral, the exchange/MTF analogy is closest; discretionary models implicate the organised-trading-facility analysis. The venue's operating design, order book, matching and DvP are specified in **Volume III**.

Figure 13 — Regulatory-pathway roadmap (Switzerland-first) — Gantt. *Indicative sequencing; durations are planning placeholders to be confirmed with counsel and FINMA, not commitments.*



Caption: Classification and legal opinions gate everything; Model A (existing asset) pilots before Model B (development finance); venue licensing runs in parallel. The business-model roadmap with milestones is in Volume VI.

---

[47] Financial Market Infrastructure Act (FinfraG/FMIA) — DLT Trading Facility, Art. 73a et seq., introduced by the DLT Act. (Verify article range and verbatim text at compile.)

[48] Loyens & Loeff, "Federal Council published a draft DLT-law" — FMIA new Art. 73a DLT trading facility; participants may include natural persons.

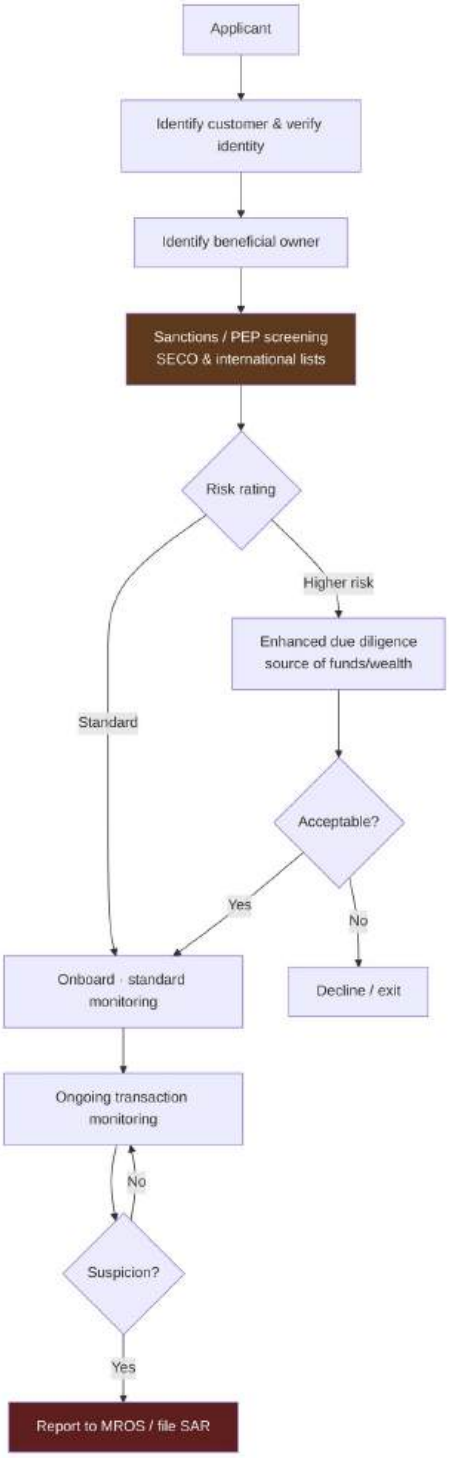
[49] Loyens & Loeff, "Federal Council published a draft DLT-law" — FMIA new Art. 73a DLT trading facility; participants may include natural persons.

4.4 AMLA / AMLO-FINMA anti-money-laundering regime

The **Anti-Money Laundering Act (AMLA, SR 955.0)** and **AMLO-FINMA** impose due-diligence and reporting duties on **financial intermediaries**. Whether and how they apply depends on the platform's activities: operating a venue, effecting transfers, providing custody, or exchanging tokens for fiat/other tokens are the kinds of activities that bring an operator within scope; per the FINMA ICO Guidelines, custody-wallet provision and token-for-fiat/token exchange fall under AMLA.[50] Core duties include **identification of the customer and beneficial owner, risk-based ongoing monitoring, special clarification of higher-risk relationships, reporting of suspicions, and either affiliation with a self-regulatory organisation (SRO) or direct prudential supervision** (the financial-intermediary supervisory route now runs through the supervisory-organisation framework).

Figure 11 — AML/CFT onboarding and monitoring flow.

[50] FINMA, "Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)", 16 Feb 2018 — payment/utility/asset token taxonomy; asset tokens treated as securities. https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/



Caption: Onboarding and monitoring are continuous, not one-off. Sanctions screening (SECO and international lists) and reporting to the Money Laundering Reporting Office Switzerland (MROS) are mandatory control points. Travel-rule and on-chain analytics integration are detailed in Volume V; cross-border AML/sanctions/CRS-FATCA are in Chapter 7 (Part 2).

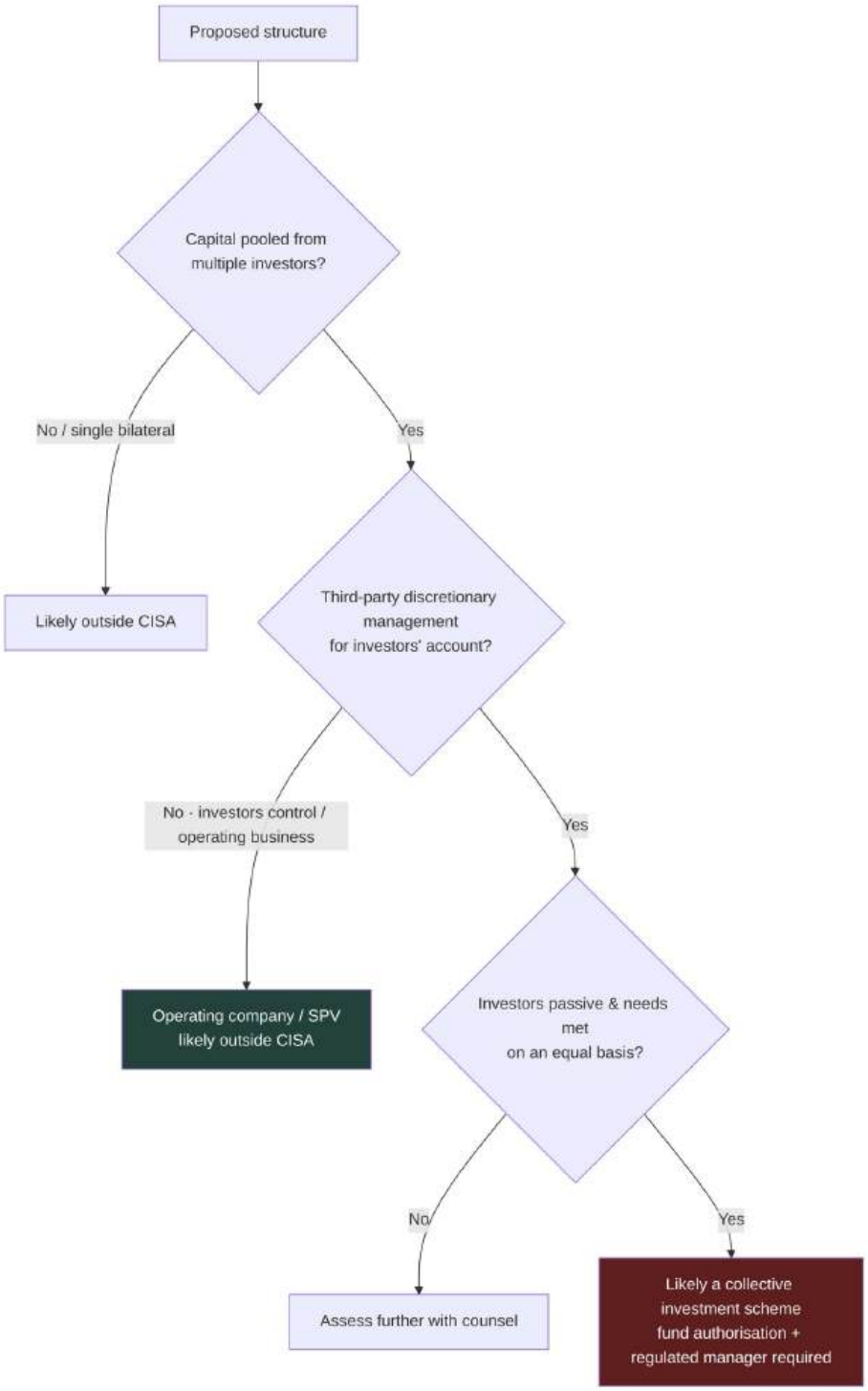
4.5 Collective Investment Schemes Act (CISA) boundary analysis

This is the **single most important boundary** for the platform. The **Collective Investment Schemes Act (CISA/KAG, SR 951.31)** regulates **collective investment schemes** — broadly, **assets raised from investors for the purpose of collective investment, managed by a third party for the investors' account**, where investors' needs are satisfied on an equal basis. If a structure is a CIS, it requires fund authorisation and a regulated management entity — a fundamentally different (and heavier) regime than issuing securities out of an operating SPV.

The distinction the platform must hold:

- **Outside CISA** — an **operating company / single-asset SPV** conducting a genuine real-estate business (owning, operating, developing a specific property), where token holders hold a security in *that* enterprise. Operating/commercial companies are not collective investment schemes.
- **Risk of falling inside CISA** — where the platform **pools** capital from many investors across **multiple assets** with **discretionary third-party management** and investors are **passive**, the structure can resemble a fund. **Model B is especially exposed**, because pooled capital deployed by a sponsor across a development looks economically like collective investment.

Figure 12 — Collective-investment-scheme boundary decision tree.



*Caption: This is a structuring and disclosure decision to be confirmed by Swiss counsel for **each** issuance. The platform's default design keeps issuances on the "operating company / SPV" side; any multi-asset, discretionary, passive-investor product must be assessed for CISA and may need to be offered as an authorised fund.*

Counsel flag. The CISA characterisation is fact-specific and outcome-determinative. No issuance should proceed without a written Swiss-counsel opinion on its CISA status, and the same boundary must be re-checked under each foreign regime (e.g., Singapore's "collective investment scheme" within the SFA, see Chapter 6, Part 2).

4.6 Bankruptcy remoteness and client-asset segregation

Two protections must hold so that investors are insulated from the insolvency of the platform operator, the custodian, and (to the extent structured) the sponsor:

1. **SPV ring-fencing.** The asset sits in a bankruptcy-remote SPV whose sole purpose is to hold the property and issue the securities, with restrictions on additional liabilities and on voluntary insolvency. The Liechtenstein **Protected Cell Company** is a design option for multi-cell segregation (see [Vol. I §3.3]).[51]
2. **Segregation of crypto-based custody assets.** The DLT Act amended Swiss insolvency law to provide for the **segregation of crypto-based assets held in custody from the custodian's bankruptcy estate**, so that such assets can be claimed by clients rather than falling to general creditors, provided they are held available for the client.[52] *The precise provisions (amendments to the Banking Act and to the Debt Enforcement and Bankruptcy Act) are identified in Appendix A; the exact article references are to be confirmed verbatim by counsel at compile — they are not reproduced from memory here.*

The operational custody design (multi-party computation / hardware security modules, key ceremonies, recovery) that gives effect to segregation is in **Volume V**.

[Volume I continues in Part 2 with Chapters 5–11, the Interim Compliance & Completeness Audit, Future Jurisdiction Compatibility Notes, Glossary, Appendices A–E, and the Diagram Inventory.]

---

[51] European Blockchain Association, "Tokenizing Real-Assets in Liechtenstein" — Protected Cell Company for segregated multi-asset tokenisation.

[52] DLT Act overview — CO 973d et seq. effective 1 Feb 2021; insolvency-law amendments for segregation of crypto-based assets. CMS.

VOLUME I — PART 2 (Chapters 5–11 and tail)

CHAPTER 5 — SECONDARY JURISDICTION: UNITED ARAB EMIRATES (DUBAI / VARA)

5.1 The UAE regulatory architecture (who regulates what)

The UAE has a layered framework. At federal level, **Cabinet Resolution No. 111 of 2022** regulates virtual assets and grants the **Securities and Commodities Authority (SCA)** broad supervisory powers. In the Emirate of Dubai, **Law No. 4 of 2022** established the **Virtual Assets Regulatory Authority (VARA)**, which licenses and supervises virtual-asset activity across Dubai's mainland and free zones **excluding the DIFC** (where the DFSA applies).[53][54] A real-estate-token platform operating from Dubai mainland is therefore primarily within **VARA's** perimeter, coordinating with the **Central Bank of the UAE (CBUAE)** on any payment/stablecoin leg and with the **Dubai Land Department (DLD)** / **RERA** on the property layer.

5.2 Token classification under VARA — ARVA

VARA's **Virtual Asset Issuance Rulebook (Version 2.0, effective 19 June 2025)** introduced explicit treatment of **real-world-asset (RWA) tokens**. A token backed by a real asset — expressly including **real estate** — is an **Asset-Referenced Virtual Asset (ARVA)**.[55][56] "RWA" is defined broadly to capture interests in financial instruments and tangible/intangible assets, so a property-backed token sits squarely within **Category 1 issuance**.[57] (A fiat-pegged settlement token would instead be a **Fiat-Referenced**

[53] UAE Government portal, "Regulation of digital properties" — Dubai Law No. 4 of 2022; federal Cabinet Resolution No. 111 of 2022 (SCA powers); VARA perimeter excludes DIFC.

[54] Linklaters, "Virtual Assets regulation in Dubai: VARA issues updates to its Rulebooks" — Rulebooks v2.0 effective 19 June 2025; ARVA/FRVA; client-asset segregation in insolvency; Sponsored VASP.

[55] VARA / Dubai real-estate tokenisation — ARVA classification; Category 1 issuance; DLD/Prypco sandbox. Summary.

[56] Linklaters, "Virtual Assets regulation in Dubai: VARA issues updates to its Rulebooks" — Rulebooks v2.0 effective 19 June 2025; ARVA/FRVA; client-asset segregation in insolvency; Sponsored VASP.

[57] Linklaters, "Virtual Assets regulation in Dubai: VARA issues updates to its Rulebooks" — Rulebooks v2.0 effective 19 June 2025; ARVA/FRVA; client-asset segregation in insolvency; Sponsored VASP.

Virtual Asset (FRVA) and engage CBUAE payment-token oversight — the same funding-vs-settlement split as [Vol. I §1.6].)

5.3 Licensing, capital, disclosure and segregation

Key obligations for an ARVA issuer/platform in Dubai:[585960]

- **Category 1 Virtual Asset Issuance licence** — required before any public offer/launch; issuing without authorisation is prohibited.
- **Whitepaper + risk-disclosure statement** — describing the token's link to the real asset, the legal structure, and investor protections.
- **Capital** — paid-up capital of at least **AED 1.5 million** or **2% of reserve assets**, whichever is applicable, maintained continuously, plus **monthly independent audits** of collateral.
- **Ongoing supervision** — periodic reporting, marketing restrictions (heightened for retail), and best-execution/disclosure rules where distribution runs through VARA-licensed brokers/exchanges.
- **Client-asset segregation** — Version 2.0 clarifies that client money and client virtual assets held by a VASP are **not owned by the VASP and do not form part of its insolvency estate**; separate client wallets must be labelled as such.[61]
- **Sponsored VASP** — a new concept allowing an entity to operate under a VARA-regulated sponsor, subject to control and marketing-compliance conditions.[62]
- **Secondary trading** — once authorised, ARVAs may be listed/distributed on Dubai-regulated exchanges and broker-dealers.

---

[58] VARA / Dubai real-estate tokenisation — ARVA classification; Category 1 issuance; DLD/Prypco sandbox. Summary.

[59] Linklaters, "Virtual Assets regulation in Dubai: VARA issues updates to its Rulebooks" — Rulebooks v2.0 effective 19 June 2025; ARVA/FRVA; client-asset segregation in insolvency; Sponsored VASP.

[60] Aston VIP, "VARA rulebook updates 2025" (and Cryptoverse Lawyers) — Category 1 ARVA issuance capital AED 1.5m or 2% of reserves; whitepaper + risk disclosure; monthly audits. (confirm exact figure for the platform's activity mix with counsel)

[61] Linklaters, "Virtual Assets regulation in Dubai: VARA issues updates to its Rulebooks" — Rulebooks v2.0 effective 19 June 2025; ARVA/FRVA; client-asset segregation in insolvency; Sponsored VASP.

[62] Linklaters, "Virtual Assets regulation in Dubai: VARA issues updates to its Rulebooks" — Rulebooks v2.0 effective 19 June 2025; ARVA/FRVA; client-asset segregation in insolvency; Sponsored VASP.

Real-estate-specific track record. Dubai has moved from pilot to framework: the DLD's tokenised-property initiative (with VARA, CBUAE and a licensed digital bank handling AED payments) is the public reference point for title-deed-backed fractional tokens.[63] The platform should treat this as a benchmark, not as its own claim, and should obtain RERA/DLD alignment for the property layer in addition to VARA authorisation for the token layer.

5.4 AML/CFT and sanctions (UAE)

VASPs in Dubai are subject to AML/CFT controls aligned with **FATF** standards, including customer due diligence, the travel rule, sanctions screening, and suspicious-transaction reporting, layered over federal AML law and SCA coordination.[64][65] Cross-border AML/sanctions/tax-reporting interactions are consolidated in Chapter 7.

CHAPTER 6 — ADDITIONAL JURISDICTIONS: LIECHTENSTEIN, SINGAPORE, HONG KONG

6.1 Liechtenstein (TVTG, SPG/Due Diligence Act)

As established in [Vol. I §1.4], the **TVTG** (in force 1 Jan 2020) applies the **Token Container Model**: the token's legal character follows the right it contains.[66] For a real-estate income/appreciation claim, that is a security/financial-instrument analysis under Liechtenstein financial-market law and, via the **EEA**, EU law (MiFID II / Prospectus

[63] VARA / Dubai real-estate tokenisation — ARVA classification; Category 1 issuance; DLD/Prypco sandbox. Summary.

[64] UAE Government portal, "Regulation of digital properties" — Dubai Law No. 4 of 2022; federal Cabinet Resolution No. 111 of 2022 (SCA powers); VARA perimeter excludes DIFC.

[65] Linklaters, "Virtual Assets regulation in Dubai: VARA issues updates to its Rulebooks" — Rulebooks v2.0 effective 19 June 2025; ARVA/FRVA; client-asset segregation in insolvency; Sponsored VASP.

[66] Liechtenstein Token and TT Service Provider Act (TVTG), in force 1 Jan 2020 — Token Container Model; Art. 2(1) service-provider roles incl. Physical Validator. tokenizestartup.com guide.

Regulation — with a **EUR 8 million** 12-month prospectus exemption available).[6768] Service-provider roles register with the **FMA** (Art. 23 TVTG); **AML/CFT** is governed by the **Due Diligence Act (SPG)**, reflecting FATF recommendations.[69] The **Physical Validator** role (Art. 2(1)) is purpose-built for the platform's physical–digital bridge: a registered validator is responsible for ensuring the off-chain asset exists and matches its on-chain representation.[70] The **Protected Cell Company** supports ring-fenced multi-asset issuance (see [Vol. I §3.3] and §4.6).[71]

6.2 Singapore (MAS — SFA, PS Act, FSM Act)

MAS applies **technology neutrality** and **"same activity, same risk, same regulatory outcome"**: tokenising a capital-markets product (CMP) does not change its substance.[72] A tokenised property-investment security is a **CMP** (the SFA defines CMPs to include securities, collective-investment-scheme units, and derivatives), regulated under the **Securities and Futures Act 2001 (SFA)** and **Financial Advisers Act 2001 (FAA)** like its non-tokenised equivalent.[7374] Consequences:

---

[67] Liechtenstein Token and TT Service Provider Act (TVTG), in force 1 Jan 2020 — Token Container Model; Art. 2(1) service-provider roles incl. Physical Validator. tokenizestartup.com guide.

[68] Liechtenstein FMA, "Token and TT Service Provider Act (TVTG)" — TVTG not part of financial-market law; FATF-aligned supervision.

[69] Liechtenstein FMA, "Token and TT Service Provider Act (TVTG)" — TVTG not part of financial-market law; FATF-aligned supervision.

[70] Liechtenstein Token and TT Service Provider Act (TVTG), in force 1 Jan 2020 — Token Container Model; Art. 2(1) service-provider roles incl. Physical Validator. tokenizestartup.com guide.

[71] European Blockchain Association, "Tokenizing Real-Assets in Liechtenstein" — Protected Cell Company for segregated multi-asset tokenisation.

[72] Bird & Bird, "MAS issues revised Guide on Tokenisation of Capital Markets Products" (Dec 2025) — "same activity, same risk, same regulatory outcome"; tokenised CMPs under SFA/FAA.

[73] Bird & Bird, "MAS issues revised Guide on Tokenisation of Capital Markets Products" (Dec 2025) — "same activity, same risk, same regulatory outcome"; tokenised CMPs under SFA/FAA.

[74] Lexology, "At a glance: cryptoassets for investment and financing in Singapore" — CMP definition (SFA s 2); STOs as offers of CMPs; accredited/institutional exemptions.

- **Offers/issuances** of tokenised CMPs may trigger **prospectus requirements under the SFA unless exemptions apply** (e.g., offers solely to **accredited or institutional investors**).[75]
- **Intermediaries** dealing/advising in tokenised CMPs may need a **capital-markets-services licence** or financial-adviser licence; requirements can apply **extra-territorially** where activity reaches persons in Singapore.[76]
- **Collective-investment-scheme** analysis mirrors the Swiss concern: if the structure is a CIS, fund/licensing rules apply; a real-estate fractionalisation amounting to a CIS is treated accordingly.[77]
- A **digital-payment-token** settlement leg falls under the **Payment Services Act 2019** and **MAS Notice PSN02** (AML/CFT; travel rule, with information requirements for transfers — last revised 30 June 2025).[78] Separately, the **DTSP regime** under the **Financial Services and Markets Act 2022** (in effect 30 June 2025) governs providers serving only overseas clients and is deliberately hard to license.[79]

[75] Lexology, “At a glance: cryptoassets for investment and financing in Singapore” — CMP definition (SFA s 2); STOs as offers of CMPs; accredited/institutional exemptions.

[76] Bird & Bird, “MAS issues revised Guide on Tokenisation of Capital Markets Products” (Dec 2025) — “same activity, same risk, same regulatory outcome”; tokenised CMPs under SFA/FAA.

[77] Lexology, “At a glance: cryptoassets for investment and financing in Singapore” — CMP definition (SFA s 2); STOs as offers of CMPs; accredited/institutional exemptions.

[78] MAS, “Guidelines to Notice PSN02 on AML/CFT — Digital Payment Token Service” (revised 30 June 2025); travel-rule information requirements. https://www.mas.gov.sg/regulation/guidelines/guidelines-to-notice-psn02-on-aml-and-cft—dpt

[79] MAS, “MAS Clarifies Regulatory Regime for Digital Token Service Providers” (6 June 2025) — DTSP licensing under the FSM Act 2022 from 30 June 2025. https://www.mas.gov.sg/news/media-releases/2025/mas-clarifies-regulatory-regime-for-digital-token-service-providers

6.3 Hong Kong (SFC — SFO, AMLO; HKMA — Stablecoins Ordinance)

Hong Kong runs a **dual regime**:[80][81][82]

- **Tokenised securities / security tokens** are **"securities" under the Securities and Futures Ordinance (SFO, Cap. 571)**; the SFC treats a tokenised security as the underlying security **plus** a tokenisation overlay, per its Circular on Intermediaries Engaging in Tokenised Securities-related Activities (2 Nov 2023) and related guidance.[83] A platform handling even one security token typically needs **Type 1 (dealing in securities)** and **Type 7 (automated trading services)** licences.[84]
- **Non-security virtual assets** are licensed under the **Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO, Cap. 615) VATP regime, in force 1 June 2023** ("virtual asset" defined in **s. 53ZRA AMLO**).[85][86]
- **Stablecoins** fall under the **Stablecoins Ordinance (Cap. 656)**, with the **HKMA** licensing fiat-referenced stablecoin issuers.[87]
- The SFC's **ASPIRe Roadmap** (Feb 2025) and its **3 November 2025 circulars** expanded VATP products/services (distribution of tokenised securities; custody)

---

[80] Charltons, "Hong Kong SFC Expands VATPs' Permitted Products and Services" (Nov 2025) — tokenised securities as a subset of digital securities; SFO; AMLO s 53ZRA; Stablecoins Ordinance.

[81] Davis Polk, "Hong Kong permits virtual asset exchanges to access global liquidity…" (3 Nov 2025 circulars) — VATP regime in force 1 June 2023; tokenised-securities track-record relief.

[82] Stephenson Harwood / Hacken — HK dual licensing (SFO Type 1+7 for security tokens; AMLO VATP); VA dealing/custody consultation conclusions (24 Dec 2025), LegCo bill expected 2026.

[83] Charltons, "Hong Kong SFC Expands VATPs' Permitted Products and Services" (Nov 2025) — tokenised securities as a subset of digital securities; SFO; AMLO s 53ZRA; Stablecoins Ordinance.

[84] Stephenson Harwood / Hacken — HK dual licensing (SFO Type 1+7 for security tokens; AMLO VATP); VA dealing/custody consultation conclusions (24 Dec 2025), LegCo bill expected 2026.

[85] Charltons, "Hong Kong SFC Expands VATPs' Permitted Products and Services" (Nov 2025) — tokenised securities as a subset of digital securities; SFO; AMLO s 53ZRA; Stablecoins Ordinance.

[86] Davis Polk, "Hong Kong permits virtual asset exchanges to access global liquidity…" (3 Nov 2025 circulars) — VATP regime in force 1 June 2023; tokenised-securities track-record relief.

and permitted shared global liquidity with affiliated overseas platforms; the **12-month track-record requirement does not apply to tokenised securities**.[88] New **VA dealing and custody** licensing regimes were consulted on (conclusions 24 Dec 2025), with a bill expected in the Legislative Council in 2026.[89]

6.4 Jurisdiction comparison matrix

Table 6 — Jurisdiction comparison (funding token = security/financial instrument in all five).

Dimension	Switzerland	UAE / Dubai (VARA)	Liechtenstein	Singapore (MAS)	Hong Kong (SFC)
Funding-token class	Asset token → ledger-based	ARVA, Category 1 issuance[91]	Security right in a token	Capital-markets product (SFA)[93]	Tokenised security (SFO)[94]

[87] Charltons, “Hong Kong SFC Expands VATPs’ Permitted Products and Services” (Nov 2025) — tokenised securities as a subset of digital securities; SFO; AMLO s 53ZRA; Stablecoins Ordinance.

[88] Davis Polk, “Hong Kong permits virtual asset exchanges to access global liquidity…” (3 Nov 2025 circulars) — VATP regime in force 1 June 2023; tokenised-securities track-record relief.

[89] Stephenson Harwood / Hacken — HK dual licensing (SFO Type 1+7 for security tokens; AMLO VATP); VA dealing/custody consultation conclusions (24 Dec 2025), LegCo bill expected 2026.

[91] Linklaters, “Virtual Assets regulation in Dubai: VARA issues updates to its Rulebooks” — Rulebooks v2.0 effective 19 June 2025; ARVA/FRVA; client-asset segregation in insolvency; Sponsored VASP.

[93] Bird & Bird, “MAS issues revised Guide on Tokenisation of Capital Markets Products” (Dec 2025) — “same activity, same risk, same regulatory outcome”; tokenised CMPs under SFA/FAA.

[94] Charltons, “Hong Kong SFC Expands VATPs’ Permitted Products and Services” (Nov 2025) — tokenised securities as a subset of digital securities; SFO; AMLO s 53ZRA; Stablecoins Ordinance.

Dimension	Switzerland	UAE / Dubai (VARA)	Liechtenstein	Singapore (MAS)	Hong Kong (SFC)
	security (CO 973d–973i)[90]		container (TVTG)[92]		
Primary statute(s)	CO; FinSA; FinfraG; AMLA; CISA	Law No. 4/2022; Cabinet Res. 111/2022; VARA Rulebooks v2.0	TVTG; SPG; EEA/MiFID II	SFA 2001; FAA 2001; PS Act 2019; FSM Act 2022	SFO (Cap. 571); AMLO (Cap. 615); Stablecoins Ord. (Cap. 656)
Prospectus / disclosure	FinSA Art. 35–36 (exemptions)[95]	Whitepaper + risk disclosure[96]	EEA Prospectus Reg (EUR 8m exemption)[97]	SFA prospectus (accredited/institutional exemptions)[98]	SFO offer rules + tokenisation overlay[99]
Secondary venue	DLT Trading Facility (FMIA Art. 73a et seq.)[100]	VARA exchange / broker-dealer[101]	EU-regulated MTF for security tokens[102]	Approved venue / RMO (SFA)	VATP (Type 1+7); ATS[103]

[90] Swiss Code of Obligations, Art. 973d–973i (ledger-based securities / *Registerwertrechte*), introduced by the DLT Act, in force 1 Feb 2021. Official text: Fedlex SR 220, https://www.fedlex.admin.ch/eli/cc/27/317_321_377/en (verify verbatim wording at compile).

[92] Liechtenstein Token and TT Service Provider Act (TVTG), in force 1 Jan 2020 — Token Container Model; Art. 2(1) service-provider roles incl. Physical Validator. tokenizestartup.com guide.

[95] Financial Services Act (FinSA / FIDLEG), SR 950.1 — Art. 35 (prospectus duty), Art. 36 (exemptions), Art. 40–51 (content/review), Art. 58–66 (KID). Official text: Fedlex, https://www.fedlex.admin.ch/eli/cc/2019/758/en

[96] VARA / Dubai real-estate tokenisation — ARVA classification; Category 1 issuance; DLD/Prypco sandbox. Summary.

[97] Liechtenstein Token and TT Service Provider Act (TVTG), in force 1 Jan 2020 — Token Container Model; Art. 2(1) service-provider roles incl. Physical Validator. tokenizestartup.com guide.

[98] Lexology, “At a glance: cryptoassets for investment and financing in Singapore” — CMP definition (SFA s 2); STOs as offers of CMPs; accredited/institutional exemptions.

[99] Charltons, “Hong Kong SFC Expands VATPs’ Permitted Products and Services” (Nov 2025) — tokenised securities as a subset of digital securities; SFO; AMLO s 53ZRA; Stablecoins Ordinance.

[100] Financial Market Infrastructure Act (FinfraG/FMIA) — DLT Trading Facility, Art. 73a et seq., introduced by the DLT Act. (Verify article range and verbatim text at compile.)

Dimension	Switzerland	UAE / Dubai (VARA)	Liechtenstein	Singapore (MAS)	Hong Kong (SFC)
AML/CFT	AMLA / AMLO-FINMA[104]	FATF-aligned VASP rules[105]	SPG (Due Diligence Act)[106]	PSN02 / FSM Act[107]	AMLO[108]
Client-asset segregation	DLT-Act insolvency segregation[109]	Client assets outside VASP estate[110]	PCC ring-fencing[111]	CMS client-money rules	SFC custody standards[112]

Reading: the classification result is consistent; the licensing and disclosure machinery differs. A single multi-jurisdiction issuance requires parallel counsel opinions and may require separate offering documents per jurisdiction.

---

[101] Linklaters, “Virtual Assets regulation in Dubai: VARA issues updates to its Rulebooks” — Rulebooks v2.0 effective 19 June 2025; ARVA/FRVA; client-asset segregation in insolvency; Sponsored VASP.

[102] Liechtenstein Token and TT Service Provider Act (TVTG), in force 1 Jan 2020 — Token Container Model; Art. 2(1) service-provider roles incl. Physical Validator. tokenizestartup.com guide.

[103] Stephenson Harwood / Hacken — HK dual licensing (SFO Type 1+7 for security tokens; AMLO VATP); VA dealing/custody consultation conclusions (24 Dec 2025), LegCo bill expected 2026.

[104] FINMA, “Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)”, 16 Feb 2018 — payment/utility/asset token taxonomy; asset tokens treated as securities. https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

[105] Linklaters, “Virtual Assets regulation in Dubai: VARA issues updates to its Rulebooks” — Rulebooks v2.0 effective 19 June 2025; ARVA/FRVA; client-asset segregation in insolvency; Sponsored VASP.

[106] Liechtenstein FMA, “Token and TT Service Provider Act (TVTG)” — TVTG not part of financial-market law; FATF-aligned supervision.

[107] MAS, “Guidelines to Notice PSN02 on AML/CFT — Digital Payment Token Service” (revised 30 June 2025); travel-rule information requirements. https://www.mas.gov.sg/regulation/guidelines/guidelines-to-notice-psn02-on-aml-and-cft—dpt

[108] Charltons, “Hong Kong SFC Expands VATPs’ Permitted Products and Services” (Nov 2025) — tokenised securities as a subset of digital securities; SFO; AMLO s 53ZRA; Stablecoins Ordinance.

[109] DLT Act overview — CO 973d et seq. effective 1 Feb 2021; insolvency-law amendments for segregation of crypto-based assets. CMS.

CHAPTER 7 — CROSS-BORDER AML/CFT, SANCTIONS, CRS/FATCA

7.1 A single control framework, multiple legal bases

Rather than a per-jurisdiction patchwork, the platform operates **one risk-based financial-crime control framework** calibrated to the **highest applicable standard** and mapped to each legal basis: AMLA/AMLO-FINMA (CH), VARA/FATF (UAE), SPG (LI), PS Act/PSN02 (SG), AMLO (HK). All are **FATF-aligned**, which makes a common control set feasible: customer and beneficial-owner identification, sanctions/PEP screening, risk rating, enhanced due diligence, ongoing monitoring, the **travel rule**, and suspicious-activity reporting (to MROS in Switzerland; to the relevant FIU elsewhere).[113][114][115] On-chain analytics and travel-rule tooling are specified in Volume V.

7.2 Sanctions

Sanctions screening covers **SECO** (Switzerland), **UN**, and other applicable lists (e.g., EU/OFAC where relevant to counterparties or currencies). Sanctions controls apply at

---

[110] Linklaters, “Virtual Assets regulation in Dubai: VARA issues updates to its Rulebooks” — Rulebooks v2.0 effective 19 June 2025; ARVA/FRVA; client-asset segregation in insolvency; Sponsored VASP.

[111] European Blockchain Association, “Tokenizing Real-Assets in Liechtenstein” — Protected Cell Company for segregated multi-asset tokenisation.

[112] Davis Polk, “Hong Kong permits virtual asset exchanges to access global liquidity…” (3 Nov 2025 circulars) — VATP regime in force 1 June 2023; tokenised-securities track-record relief.

[113] FINMA, “Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)”, 16 Feb 2018 — payment/utility/asset token taxonomy; asset tokens treated as securities. https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

[114] Linklaters, “Virtual Assets regulation in Dubai: VARA issues updates to its Rulebooks” — Rulebooks v2.0 effective 19 June 2025; ARVA/FRVA; client-asset segregation in insolvency; Sponsored VASP.

[115] MAS, “Guidelines to Notice PSN02 on AML/CFT — Digital Payment Token Service” (revised 30 June 2025); travel-rule information requirements. https://www.mas.gov.sg/regulation/guidelines/guidelines-to-notice-psn02-on-aml-and-cft—dpt

onboarding and continuously, including wallet-level screening; positive matches trigger freezing and reporting obligations (see Figure 11, [Vol. I §4.4]). Sanctioned-jurisdiction and high-risk-jurisdiction controls are enforced through eligibility gating.

7.3 Tax-information exchange — CRS and FATCA

- **CRS (Common Reporting Standard).** Where the issuing/holding vehicle or the platform is a **reporting financial institution**, account-holder information must be identified and reported to the relevant tax authority for automatic exchange. The platform's vehicles must each be classified for CRS (FI vs. NFE) — a per-structure determination.
- **FATCA.** US-person identification and reporting (or applicable IGA treatment) must be built into onboarding where US persons could participate; many institutional issuances exclude US persons entirely to simplify this.

Counsel flag. CRS/FATCA classification of each SPV/issuer and of the platform operator is fact-specific and must be confirmed by tax counsel (see [Vol. I §8]); misclassification carries reporting and penalty risk. Crypto-asset reporting frameworks (e.g., the OECD CARF and EU DAC8 extensions) are an emerging overlay flagged in the Future Jurisdiction Compatibility Notes.

CHAPTER 8 — TAX, ACCOUNTING & REGULATORY-REPORTING AUTOMATION

8.1 Scope and posture

This chapter frames the tax/accounting/reporting **architecture**; it is **not** tax advice and every position must be confirmed by qualified tax counsel per structure and per jurisdiction. The platform's design goal is **automation with an auditable trail**: withholding-tax computation, net-asset-value (NAV) determination, investor tax reporting, and regulatory reporting are generated from the same golden source (the securities register + asset/income data).

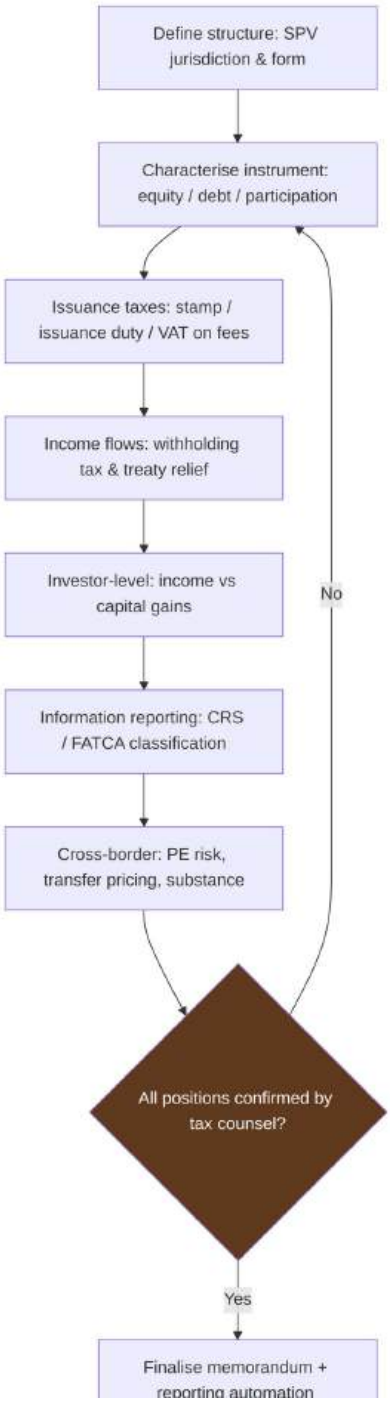
8.2 Principal tax touchpoints

- **At issuance** — stamp/issuance duties (jurisdiction-specific), VAT treatment of platform fees, and the characterisation of the instrument (equity/debt/participation — see [Vol. I §1.3]) which drives downstream treatment.
- **On income** — **withholding tax** on distributions (notably Swiss withholding tax on certain income), treaty relief, and the mechanics of computing/withholding at distribution.
- **On transfer** — securities-transfer-tax considerations on the secondary market (venue-dependent).

- **At investor level** — income vs. capital-gains characterisation, reportable under CRS/FATCA (see [Vol. I §7.3]).

8.3 Tax structuring memorandum — outline (flowchart)

Figure 14 — Tax structuring memorandum: decision flow. *The memorandum itself is produced per structure; this is its logical skeleton.*



8.4 Accounting and NAV

NAV is computed from independent valuation (Model A) or cost-plus-progress and residual-value methods (Model B) — the unified valuation methodology is in **Volume IV**. Accounting policies (fair value vs. cost, consolidation of SPVs, treatment of escrow) are

set per structure and audited. Regulatory reports (e.g., prospectus-related filings, AML/STR, supervisory returns, fund reporting if any CISA-scope product exists) are generated and version-controlled.

CHAPTER 9 — DATA PROTECTION & PRIVACY

9.1 Applicable regimes

Two regimes are primary: the Swiss **Federal Act on Data Protection (FADP/nFADP, SR 235.1)**, in force in its revised form since **1 September 2023**, and the EU **GDPR** where EEA data subjects are involved (directly relevant via Liechtenstein and cross-border investors).[116] Both require a lawful basis, purpose limitation, data minimisation, transparency, data-subject rights, breach notification, and controls on cross-border transfers.

9.2 The blockchain-specific tension

A core design problem: **GDPR/FADP rights (erasure, rectification) sit uneasily with ledger immutability.** The platform resolves this by a strict **on-chain/off-chain data split**:

- **On-chain:** only pseudonymous identifiers, cryptographic commitments, and the minimum needed to evidence the right and its transfer — **never** plaintext personal data.
- **Off-chain:** identity, KYC, and personal data held in controlled, erasable systems; on-chain references are designed so that off-chain deletion renders on-chain data non-attributable.
- **Privacy technology:** zero-knowledge proofs (ZKP), W3C **Verifiable Credentials** for reusable eligibility, and confidential computing reduce on-chain personal-data exposure; the **post-quantum cryptography (PQC)** migration path protects long-lived confidential data. These are specified in Volume II (architecture) and Volume V (security).

9.3 Governance

A **Data Protection Officer / Data-Protection Counsel** owns the data-protection programme; records of processing, data-protection impact assessments (DPIAs) for high-risk processing, and processor agreements (linking to vendor risk, Chapter 10) are maintained. Cross-border transfer mechanisms (adequacy, standard contractual clauses) are documented per data flow.

---

[116] Swiss Federal Act on Data Protection (FADP/nFADP), SR 235.1, revised version in force 1 Sept 2023. Official text: Fedlex (SR 235.1).

CHAPTER 10 — VENDOR & OUTSOURCING RISK MANAGEMENT

10.1 Why this is a board-level matter

The platform depends on critical third parties — cloud/hosting, custody technology (e.g., MPC/HSM providers), oracle and valuation-data providers, KYC/AML and sanctions-data vendors, banking/settlement partners, and audit/legal. Under financial-market outsourcing expectations (and, for EEA-facing activity, **DORA's ICT third-party rules** — see [Vol. I §1.5]),[117] the operator remains **fully responsible** for outsourced functions.

10.2 The vendor-risk lifecycle

Figure 15 — Vendor-risk management lifecycle.

Caption: Concentration risk (over-reliance on a single cloud or custody provider) and substitutability (can the function be moved?) are explicit assessment criteria, consistent with DORA's critical-ICT-third-party focus. Detailed control mapping is in Volume V.

10.3 Key controls

Right-to-audit and step-in rights; data-processing agreements (Chapter 9); defined exit and substitutability plans for critical providers; continuous monitoring of security posture and incidents; and a register of all critical/important outsourcing arrangements with their concentration profile.

CHAPTER 11 — COMPETITIVE LANDSCAPE, INDUSTRY THREATS & LIMITATIONS

11.1 Competitive landscape (categories and benchmarks)

The platform competes and interoperates across four categories. Named institutions are cited **only as published benchmarks**; the platform does not act for them, and

[117] Digital Operational Resilience Act (DORA), Reg (EU) 2022/2554, applicable 17 Jan 2025; applies to CASPs and EU financial entities. Official text, Official Journal (EUR-Lex): https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

quantified competitive facts are sourced in **Volume VI**.

- **Regulated digital-asset market infrastructures / digital CSDs** — venues issuing and settling tokenised securities under financial-market licences (e.g., SIX Digital Exchange in Switzerland) are the closest infrastructure benchmark for the DLT Trading Facility design (see [Vol. I §4.3]).
- **Tokenised-fund and tokenised-money-market platforms** — large asset managers' tokenised funds set institutional expectations for custody, transfer-agency and disclosure.
- **Real-world-asset (RWA) tokenisation platforms** — including real-estate-specific efforts; Dubai's DLD/VARA initiative is the leading public real-estate reference point.[118]
- **Traditional real-estate vehicles** — REITs and real-estate funds are the incumbent comparators on cost, liquidity and investor familiarity; the platform's claim is lower friction and finer fractionalisation **without** sacrificing investor protection.

11.2 Industry threats and limitations register

Table 7 — Threats and limitations (with mitigations and forward references).

#	Threat / limitation	Why it matters	Primary mitigation	Detailed in
1	**Smart-contract risk**	Code defects can cause loss or lock-up	Audited ERC-3643 contracts; formal verification; time-locked upgrades	Vol. II, Vol. V
2	**Oracle / valuation manipulation**	Tokenised value depends on off-chain truth	Multiple independent valuers/oracles; signed attestations; circuit breakers	Vol. II, Vol. IV
3	**Physical–digital enforcement gap**	On-chain transfer must bind off-chain title	Registration agreement (CO 973f); land-registry linkage; title insurance	[Vol. I §3.3], Vol. II
4	**Completion risk (Model B)**	Investors fund a non-existent asset	Escrow; milestone certification; completion guarantees; stress tests	[Vol. I §3.4], Vol. V
5	**CISA / fund reclassification**	Could force unplanned fund authorisation	Operating-SPV structuring; counsel opinion per issuance	[Vol. I §4.5]

[118] VARA / Dubai real-estate tokenisation — ARVA classification; Category 1 issuance; DLD/Prypco sandbox. Summary.

#	Threat / limitation	Why it matters	Primary mitigation	Detailed in
6	**Custody / key compromise**	Loss of keys = loss of assets	MPC/HSM; key ceremonies; segregation; recovery (CO 973h)	Vol. V
7	**Secondary-market illiquidity**	Thin order books undermine the value proposition	Eligible-investor market-making; OTC; realistic disclosure	Vol. III
8	**Settlement-asset redemption risk**	Stablecoin de-peg / redemption failure	Prefer tokenised deposits; vet issuer/reserves; DvP	[Vol. I §1.6], Vol. II
9	**Bridge risk (cross-chain)**	Bridges are a known attack surface	Defer bridging; bridge-risk analysis; limits	Vol. II
10	**Regulatory divergence & change**	Five+ regimes, all evolving	Substance-over-form portability; modular compliance; monitoring	Future Jurisdiction Notes
11	**Data-protection vs. immutability**	GDPR/FADP erasure vs. ledger permanence	On-chain/off-chain split; no plaintext PII on-chain; ZKP	[Vol. I §9]
12	**Quantum / cryptographic obsolescence**	Long-lived assets outlive today's crypto	PQC migration plan	Vol. V
13	**Model risk (analytics/AI)**	Mis-stated IRR/NPV/risk scores mislead	Model cards; SHAP; validation; LLM-usage policy	Vol. IV
14	**Concentration (vendor/chain)**	Single points of failure	Vendor-risk lifecycle; substitutability plans	[Vol. I §10], Vol. V
15	**AML / sanctions breach**	Legal, reputational, licence risk	FATF-aligned controls; screening; travel rule	[Vol. I §4.4, §7]

11.3 Honest limitations

Three limitations are inherent rather than solvable by engineering: (i) **liquidity cannot be manufactured** — fractionalisation widens access but does not guarantee a deep secondary market; (ii) **the law is unsettled and divergent** across jurisdictions and is changing (the MiCA transitional window, the HK dealing/custody bill, evolving VARA rulebooks); and (iii) **tokenisation does not remove real-estate risk** — vacancy, development, valuation and interest-rate risks persist and must be disclosed, not obscured by the technology.

INTERIM COMPLIANCE & COMPLETENESS AUDIT — VOLUME I

> **Status of this audit.** Per the package method, a **full cross-volume Compliance & Completeness Audit** (a single regulatory-auditor pass over all seven volumes, checking every citation, resolving every forward reference, and reconciling the Control File) is performed **after Volume VII is drafted** and is then inserted immediately before each volume's Future Jurisdiction Compatibility Notes. What follows is the **interim, volume-local** self-audit for Volume I.

A. Citations. Every legal/standards source relied on in this volume is listed in the Citation Register (Appendix D) and footnoted to an official or primary source where one was retrievable (Fedlex for Swiss statutes; FINMA, ESMA, MAS, VARA/FMA and the SFC for regulator materials). **No citation has been fabricated.** Where only secondary (law-firm/commentary) sources were available, they are paraphrased — not quoted at length — and labelled as commentary.

B. Verbatim statutory text. This interim draft provides **operative summaries** of cited provisions plus **official-source pointers** (Appendix A), rather than reproducing long statutory passages from memory. Verbatim text will be pasted from the linked official sources at the `.docx` compile step, after counsel review. This is a deliberate integrity choice consistent with the no-fabrication rule.

C. Known open / flagged items (carried to the final audit): 1. **CO Art. 973h** — exact wording of the cancellation/annulment procedure to be inserted verbatim (Fedlex SR 220). 2. **FinfraG/FMIA Art. 73a et seq.** — confirm the precise article range and verbatim text for the DLT Trading Facility, and the FMIA provisions' staged commencement date. 3. **Bankruptcy segregation** — confirm the exact Banking Act and Debt Enforcement and Bankruptcy Act (SchKG/DEBA) article numbers introduced/amended by the DLT Act for segregation of crypto-based custody assets ([Vol. I §4.6]). 4. **AMLA supervisory route** — confirm current naming/structure of the financial-intermediary supervision route (supervisory-organisation framework) and SRO affiliation specifics. 5. **VARA capital threshold** — confirm whether the AED 1.5m / 2%-of-reserves figure is the operative Category-1 ARVA issuance capital requirement for the platform's exact activity mix, or whether a higher figure applies to combined activities. 6. **MiCA transitional window** — verify, as at the offering date, the live status of any EEA-facing CASP activity given the 1 July 2026 cut-off. 7. **Cross-volume forward references** — all `[Vol. II–VII §…]` pointers (Appendix E) to be resolved when those volumes exist.

D. Method conformance. Design options are labelled with trade-offs (§§1.3, 1.6, 2.5, 3.3, 4.2). The controlling-vocabulary rule is applied (canonical “ledger-based security”; deprecated synonyms mapped in the Glossary). Mermaid figures each carry a caption and are listed in the Diagram Inventory.

FUTURE JURISDICTION COMPATIBILITY NOTES

The architecture and legal design are built to extend to further jurisdictions **without re-engineering the core**:

- **Portable classification logic.** Because every in-scope regime applies **substance over form**, the token-classification decision tree (Figure 7) is reusable: a new jurisdiction is added by mapping its “security/financial instrument” definition and its prospectus/licensing machinery onto the existing structure, not by re-deriving the instrument.
- **Modular SPV and eligibility layers.** The SPV layer ([Vol. I §3.3]) and the on-chain eligibility/whitelisting layer ([Vol. I §3.5]) are configurable per jurisdiction (investor categories, transfer restrictions, disclosure packs), so a new market is an additional configuration and offering document, not a new platform.
- **Settlement-asset abstraction.** The funding/settlement split ([Vol. I §1.6]) lets a new jurisdiction’s preferred settlement leg (local tokenised deposit, regulated stablecoin, or fiat rail) be slotted in without affecting the funding-token classification.

Watch items (to monitor and flag at each volume’s audit): 1. **United States** — an evolving federal/state framework for digital-asset securities; any US-person participation must be assessed separately (most institutional issuances currently exclude US persons). 2. **OECD CARF / EU DAC8** — crypto-asset tax-reporting frameworks that will extend CRS-style reporting to crypto-assets; build reporting hooks now ([Vol. I §7.3]). 3. **EU DLT Pilot Regime (Reg (EU) 2022/858)** — a sandbox for DLT market infrastructures that may offer an EEA route for tokenised-securities trading/settlement; assess as the platform’s EEA strategy matures. 4. **MiCA window (Reg (EU) 2023/1114)** — the CASP transitional regime to 1 July 2026 and ongoing ESMA guidance on the financial-instrument boundary. 5. **Evolving VARA and Hong Kong regimes** — VARA rulebook versioning and Hong Kong’s forthcoming VA dealing/custody legislation (LegCo 2026) will change specifics; re-verify before each Dubai/HK issuance.

GLOSSARY

*Full-form definitions of every abbreviation used in this volume. Canonical terms are marked **(canonical)**; deprecated synonyms are mapped at the end.*

Term	Definition
AML / AMLA	Anti-Money Laundering; the Swiss Anti-Money Laundering Act (SR 955.0), imposing due-diligence and reporting duties on financial intermediaries.
AMLO	(HK) Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615); also used for AML/CFT obligations generally.
AMLO-FINMA	FINMA Anti-Money Laundering Ordinance implementing AMLA for FINMA-supervised intermediaries.
ART	Asset-Referenced Token — a MiCAR crypto-asset referencing a basket/asset to stabilise value (distinct from an EMT).
ARVA	(UAE/VARA) Asset-Referenced Virtual Asset — a token backed by a real asset (incl. real estate); Category 1 issuance.
CARF	(OECD) Crypto-Asset Reporting Framework — emerging tax-reporting standard for crypto-assets.
CISA / KAG	Collective Investment Schemes Act (SR 951.31) — Swiss fund regulation; the boundary the platform must manage.
CMP	(SG) Capital Markets Product under the Securities and Futures Act 2001.
CO	Swiss Code of Obligations (SR 220); Art. 973d–973i govern ledger-based securities.
CRS	Common Reporting Standard — automatic exchange of financial-account information for tax purposes.
DAC8	EU Directive extending tax-reporting/administrative cooperation to crypto-assets.
DEBA / SchKG	(CH) Debt Enforcement and Bankruptcy Act — relevant to segregation of crypto-based custody assets.
DLD	(UAE) Dubai Land Department — the property-registration authority; runs the tokenised-property initiative.
DLT	Distributed Ledger Technology.
DLTR / DLT Pilot Regime	EU Regulation (EU) 2022/858 establishing a pilot regime for DLT market infrastructures.
DORA	Digital Operational Resilience Act, Reg (EU) 2022/2554 — ICT risk, incident reporting, resilience testing, third-

Term	Definition
	party oversight.
DPT	(SG) Digital Payment Token under the Payment Services Act 2019.
DvP	Delivery-versus-Payment — simultaneous exchange of asset and payment legs at settlement.
DFSA / DIFC	Dubai Financial Services Authority / Dubai International Financial Centre — a separate free-zone regulator/zone outside VARA's perimeter.
EMT	E-Money Token — a MiCAR crypto-asset referencing a single fiat currency.
ERC-3643 (T-REX)	Permissioned-token standard for compliant security tokens (identity/eligibility-gated transfers).
FADP / nFADP	(CH) Federal Act on Data Protection (SR 235.1), revised version in force 1 Sept 2023.
FAA	(SG) Financial Advisers Act 2001.
FATCA	(US) Foreign Account Tax Compliance Act — US-person tax reporting.
FATF	Financial Action Task Force — global AML/CFT standard-setter.
FINMA	Swiss Financial Market Supervisory Authority.
FinfraG / FMIA	(CH) Financial Market Infrastructure Act — includes the DLT Trading Facility licence (Art. 73a et seq.).
FinSA / FIDLEG	(CH) Financial Services Act (SR 950.1) — prospectus duty (Art. 35), exemptions (Art. 36), KID (Art. 58–66).
FinSO	(CH) Financial Services Ordinance implementing FinSA.
FRVA	(UAE/VARA) Fiat-Referenced Virtual Asset — a fiat-pegged token (settlement-side).
FSM Act	(SG) Financial Services and Markets Act 2022 — includes the DTSP regime.
GDPR	EU General Data Protection Regulation.
HKMA	Hong Kong Monetary Authority — licenses fiat-referenced stablecoin issuers.
IRR / NPV	Internal Rate of Return / Net Present Value — investor-return metrics (Volume IV).
KID	Key Information Document — concise retail disclosure under FinSA Art. 58–66.
KYC	Know Your Customer — identity verification at onboarding.
Ledger-based security (canonical)	The official English rendering of *Registerwertrecht* (CO

Term	Definition
	973d–973i): a right created by registration agreement on a qualifying ledger, asserted and transferred only via that ledger.
MAS	Monetary Authority of Singapore.
MiCAR / MiCA	Markets in Crypto-Assets Regulation, Reg (EU) 2023/1114; Art. 2(4)(a) excludes financial instruments.
MiFID II	Markets in Financial Instruments Directive 2014/65/EU — defines “financial instrument” (Art. 4(1)(15)).
MLRO	Money Laundering Reporting Officer.
MROS	Money Laundering Reporting Office Switzerland — the Swiss financial intelligence unit.
MTF / OTF	Multilateral / Organised Trading Facility — categories of trading venue.
NAV	Net Asset Value.
PCC	Protected Cell Company — a vehicle with ring-fenced cells (Liechtenstein); supports segregated multi-asset issuance.
PEP	Politically Exposed Person — a higher-risk AML category.
PQC	Post-Quantum Cryptography — migration to quantum-resistant algorithms.
PS Act / PSN02	(SG) Payment Services Act 2019 / MAS Notice PSN02 (AML/CFT for DPT services; travel rule).
RACI	Responsible, Accountable, Consulted, Informed — responsibility-assignment matrix (Appendix C).
RERA	(UAE) Real Estate Regulatory Agency (within DLD).
SCA	(UAE) Securities and Commodities Authority — federal regulator (Cabinet Resolution 111/2022).
SECO	(CH) State Secretariat for Economic Affairs — administers Swiss sanctions.
SFA	(SG) Securities and Futures Act 2001.
SFC	(HK) Securities and Futures Commission.
SFO	(HK) Securities and Futures Ordinance (Cap. 571).
SPG	(LI) Due Diligence Act — Liechtenstein AML/CFT law.
SPV	Special-Purpose Vehicle — bankruptcy-remote entity owning the asset and issuing the securities.
SRO	Self-Regulatory Organisation — an AMLA supervision/affiliation route.
STO	Security Token Offering.

Term	Definition
Stablecoins Ordinance	(HK) Cap. 656 — HKMA-administered regime for fiat-referenced stablecoins.
TVTG	(LI) Token and TT Service Provider Act (Blockchain Act), in force 1 Jan 2020; Token Container Model.
UUPS	Universal Upgradeable Proxy Standard (EIP-1822) — a smart-contract upgrade pattern.
VARA	(UAE) Virtual Assets Regulatory Authority (Dubai); Law No. 4 of 2022.
VASP	Virtual Asset Service Provider.
VATP	(HK) Virtual Asset Trading Platform — licensed under AMLO Chapter 5B (and SFO for security tokens).
ZKP	Zero-Knowledge Proof — cryptographic proof revealing validity without underlying data.

Deprecated-synonym mapping (use the canonical term):

Deprecated / market synonym	Canonical term
DLT security · uncertificated register security (URS) · “tokenised security” (when Swiss civil-law precision is needed)	**Ledger-based security**
Crypto token / coin (for the funding instrument)	**Asset token / security** (per FINMA)
“The fund” (for a single-asset operating SPV)	**Property SPV / issuer** (avoids implying CISA scope)
Stablecoin (generic)	**Settlement asset** (named per instrument: EMT/ART/tokenised deposit)

APPENDIX A — LEGAL SOURCE REGISTER & VERBATIM-TEXT POINTERS

Honest approach: this register gives the official source for each cited instrument and the status of verbatim text. Verbatim passages are inserted from these official sources at the `.docx` compile step; they are not reproduced from memory in this interim draft. Statutes are not subject to copyright. Hyperlinks appear only where an official primary source was verified live as of the date of documentation; secondary commentary is cited by author and title (no hyperlink) to prevent link rot.

#	Instrument / provision	Official source (pointer)	Verbatim-text status
A1	CO Art. 973d–973i (ledger-based securities)	Fedlex SR 220 — https://www.fedlex.admin.ch/eli/cc/27/317_321_377/en	Operative summary in §4.1; **insert verbatim 973d–973i at compile**; 973h wording flagged

#	Instrument / provision	Official source (pointer)	Verbatim-text status
A2	FinSA (SR 950.1), Art. 35–36, 40–51, 58–66	Fedlex — https://www.fedlex.admin.ch/eli/cc/2019/758/en	Operative summary in §4.2; insert Art. 35–36 verbatim at compile
A3	FinSO (SR 950.11)	Fedlex (SR 950.11)	Referenced (Annex 1 content); pointer only
A4	FinfraG/FMIA — DLT Trading Facility (Art. 73a et seq.)	Fedlex (FMIA, SR 958.1)	**Article range and verbatim text flagged** for confirmation at compile
A5	AMLA (SR 955.0); AMLO-FINMA	Fedlex (SR 955.0)	Operative summary in §4.4; pointer only
A6	CISA/KAG (SR 951.31)	Fedlex (SR 951.31)	Operative summary in §4.5; CIS definition to be cited verbatim at compile
A7	DLT-Act insolvency segregation (Banking Act; DEBA/SchKG)	Fedlex (Banking Act SR 952.0; DEBA SR 281.1)	**Exact article numbers flagged** ([Vol. I §4.6])
A8	FADP/nFADP (SR 235.1)	Fedlex (SR 235.1)	Operative summary in §9.1; pointer only
A9	VARA Law No. 4 of 2022; Cabinet Resolution 111/2022; Rulebooks v2.0	VARA; UAE Government portal	Operative summary in Ch. 5; rulebook clauses to be cited at compile
A10	TVTG (Liechtenstein Blockchain Act)	Liechtenstein FMA	Operative summary in §§1.4, 6.1; Art. 2(1)/23 to be cited at compile
A11	SFA 2001; FAA 2001; PS Act 2019; PSN02; FSM Act 2022	MAS	Operative summary in §6.2; PSN02 (rev. 30 Jun 2025) pointer
A12	SFO (Cap. 571); AMLO (Cap. 615); Stablecoins Ordinance (Cap. 656)	HK e-Legislation; SFC	Operative summary in §6.3; s. 53ZRA AMLO to be cited at compile
A13	MiCAR Reg (EU) 2023/1114; MiFID II 2014/65/EU; DORA Reg (EU) 2022/2554; DLTR Reg (EU) 2022/858	EUR-Lex (Reg 2023/1114; 2022/2554; 2022/858); ESMA	Operative summary in §1.5; Art. 2(4)(a) to be cited at compile

APPENDIX B — LEGAL-EVENT → ON-CHAIN-STATE MAPPING (Table 4)

Maps each legal event to its on-chain effect and CO anchor, for both models. The on-chain mechanism is specified in Volume II; this table is the legal–technical bridge.

Legal event	Model	On-chain state change	CO / legal anchor
Eligibility approved	A & B	Investor address added to identity registry / whitelist	Eligibility (FinSA client categories); no security state change
Subscription accepted	A & B	Allocation recorded; binding terms reference registration agreement	Registration agreement (CO 973d)
Settlement received	A & B	Capital-call satisfied; escrow credited	Contract / escrow terms
Issuance	A (now) / B (on completion)	**Mint** ledger-based security to holder	CO 973d–973e
Transfer (eligible↔eligible)	A & B	**Transfer** executed; eligibility-gated; ineligible transfers blocked	CO 973f (no written assignment)
Pledge / usufruct	A & B	**Encumbrance** flag visible in ledger	CO 973g
Income distribution	A (now) / B (post-completion)	Distribution event; withholding computed off-chain	CO 973e; tax (§8)
Milestone certified	B	Escrow **drawdown tranche** authorised and released	Escrow terms; §3.4
Completion / conversion	B	Claim converts to income-producing security (Model-A steady state)	Offering terms; §3.2
Loss / annulment	A & B	**Cancellation** + controlled re-issuance	CO 973h
Redemption / wind-up	A & B	**Burn** + final distribution	Offering terms; CO 973e

APPENDIX C — RACI MATRIX (Table 5)

R = Responsible, A = Accountable, C = Consulted, I = Informed. Roles per the org chart (Figure 4). "Review/Ext." = prospectus review body / external auditor as applicable.

Activity	Board	CLRO	Sec. Counsel	MLRO/ CCO	CRO	CPO	CTO/ Arch	CFO	Int. Audit	Review /Ext.
Token classification & legal opinion	A	R	R	C	C	I	C	I	I	C
SPV	A	R	R	I	C	I	C	C	I	C

Activity	Board	CLRO	Sec. Counsel	MLRO/ CCO	CRO	CPO	CTO/ Arch	CFO	Int. Audit	Review /Ext.
formation & registration agreement										
Prospectus / exemption decision & sign-off	A	R	R	C	C	I	I	C	I	R
KID preparation (retail)	I	A	R	C	C	C	I	C	I	C
Investor onboarding (KYC/AML)	I	C	I	A/R	C	I	C	I	I	I
Suitability / eligibility determination	I	C	C	A	C	R	C	I	I	I
New-product / issuance approval	A	C	C	C	C	R	C	C	I	I
Valuation sign-off	A	C	I	I	C	C	I	R	I	C
Drawdown / milestone release (Model B)	A	C	C	I	R	C	C	C	I	C (monitor)
Smart-contrac	I	C	I	I	C	C	A/R	I	I	I

Activity	Board	CLRO	Sec. Counsel	MLRO/ CCO	CRO	CPO	CTO/ Arch	CFO	Int. Audit	Review /Ext.
t deployment & upgrade										
Custody & key management	A	C	I	C	R	I	C	C	I	I
Distributions / withholding	I	C	C	I	C	I	C	A/R	I	I
Tax positions & CRS/FATCA reporting	A	C	C	C	C	I	I	R	I	C
Data protection / DPIA	I	A	C	C	C	C	R	I	I	I
Vendor onboarding (critical)	I	C	C	C	A	C	R	C	I	I
Incident response	A	C	I	C	R	I	R	I	C	I
Regulatory reporting / supervisory returns	A	R	C	C	C	I	I	C	I	C
Sanctions screening & MROS reporting	I	C	I	A/R	C	I	C	I	I	I

APPENDIX D — CITATION REGISTER (Table 8)

*Every external source relied on in Volume I, with a verification note. Official/primary sources are marked **P**; secondary/commentary sources (paraphrased only) are marked **S**.*

Ref	Source	Type	Used for	Verification note
co973	Fedlex SR 220 (CO)	P	Ledger-based securities Art. 973d–973i	Official text; verbatim to be inserted at compile
finma	FINMA ICO Guidelines (16 Feb 2018)	P	Token taxonomy; asset tokens = securities	Regulator primary source
finmadev	FINMA FinTech dossier	P	Token definitions	Regulator primary source
finsa	Fedlex SR 950.1 (FinSA)	P	Prospectus duty/exemptions/KID	Official text
fmia	FMIA / Loyens & Loeff analysis	P/S	DLT Trading Facility Art. 73a et seq.	Article range flagged for confirmation
esmafi	ESMA Guidelines (2025)	P	Crypto-asset = financial instrument	Regulator primary source
mica	MiCAR Reg (EU) 2023/1114 (EUR-Lex)	P	Art. 2(4)(a) carve-out; timeline	EUR-Lex official text
micatrans	Dechert	S	CASP transitional to 1 Jul 2026	Paraphrased
dora	DORA Reg (EU) 2022/2554 (EUR-Lex)	P	ICT resilience; applies 17 Jan 2025	EUR-Lex official text
cms	CMS	S	DLT Act effective dates; segregation	Paraphrased; statute pointer in Appendix A
pesta	Pestalozzi	S	CO 973d(2)/973f/973g detail	Paraphrased
lex	Lexology/CMS	S	973d(2) requirements; 973i liability	Paraphrased
loyens	Loyens & Loeff	S	FMIA Art. 73a; participant scope	Paraphrased
vischer	VISCHER	S	FinSA Art. 35 scope	Paraphrased
caplaw	CapLaw	S	Art. 36(1)(c)/(d)/(e) thresholds	Paraphrased

Ref	Source	Type	Used for	Verification note
iflr	IFLR	S	Review body; CHF 500k fine	Paraphrased
tvtg	TVTG guide	S	Token Container Model; Art. 2(1)/23	Paraphrased; FMA pointer (tvtgfma)
tvtgfma	Liechtenstein FMA	P	TVTG status; FATF alignment	Regulator primary source
tvtgpcc	European Blockchain Assoc.	S	Protected Cell Company	Paraphrased
vararwa	tokenizer.estate summary	S	ARVA; Category 1; DLD pilot	Paraphrased
varav2	Linklaters	S	Rulebooks v2.0 (19 Jun 2025); segregation; Sponsored VASP	Paraphrased
varacap	Aston VIP / Cryptoverse	S	AED 1.5m / 2% capital; monthly audits	Paraphrased; **confirm for exact activity mix**
uaegov	UAE Government portal	P	Law No. 4/2022; Cabinet Res. 111/2022; SCA	Government primary source
mastoken	Bird & Bird	S	Revised CMP tokenisation guide (Dec 2025)	Paraphrased
maslex	Lexology	S	CMP/STO definitions; exemptions	Paraphrased
psn02	MAS	P	PSN02 (rev. 30 Jun 2025); travel rule	Regulator primary source
dtsp	MAS media release (6 Jun 2025)	P	DTSP regime from 30 Jun 2025	Regulator primary source
hktok	Charltons	S	SFO; s. 53ZRA AMLO; Stablecoins Ord.	Paraphrased
hkexp	Davis Polk	S	3 Nov 2025 circulars; VATP from 1 Jun 2023	Paraphrased
hklic	Stephenson Harwood / Hacken	S	Type 1+7; dealing/custody bill 2026	Paraphrased
fadp	Swiss FADP (SR 235.1)	P	Data protection in force 1 Sept 2023	Official text pointer

APPENDIX E — CROSS-REFERENCE INDEX

Internal (resolved within this volume): §1.3 ↔ §4.1 (asset token → ledger-based security); §1.6 ↔ §4.6 (settlement asset / segregation); §3.4 ↔ Appendix B (events → on-chain state); §2.4 ↔ Appendix C (RACI); §4.5 ↔ §6.2 (CISA / SG CIS).

Forward references (to be resolved when later volumes are drafted):

Anchor used	Target volume	Topic
Vol. II	Volume II — Technical Architecture	Ledger choice, ERC-3643/UUPS, oracles, physical–digital bridge, settlement/DvP, ZKP/PQC
Vol. III	Volume III — Marketplace & Trading	DLT-venue design, order book, matching, OTC
Vol. IV	Volume IV — Financial Intelligence	Valuation methodology, IRR/NPV, Monte Carlo, model cards/SHAP, LLM policy
Vol. V	Volume V — Security & Operations	Custody (MPC/HSM), key ceremonies, recovery, PQC migration, development-phase stress runs, DORA controls
Vol. VI	Volume VI — Business & Financial Model	TAM/SAM/SOM, sourced competitive facts, tokenomics, roadmap
Vol. VII	Volume VII — Architecture Atlas	Consolidated diagrams (all-Mermaid)

All forward references above must be replaced with concrete section pointers before final delivery; none is left as a vague summary.

DIAGRAM INVENTORY (Volume I)

Fig.	Title	Mermaid type	Section
1	Platform domain map	flowchart	2.2
2	Dual-mode operating model	flowchart	2.3
3	Governance & three lines of defence	flowchart	2.4
4	Indicative organisation chart	graph	2.4
5	Asset-backed issuance — SPV & rights	flowchart	3.1

Fig.	Title	Mermaid type	Section
6	Forward-funding — SPV, escrow & drawdown	flowchart	3.2
7	Token-classification decision tree	flowchart	1.3
8	Ledger-based security lifecycle (CO 973d–973i)	stateDiagram	4.1
9	Forward-funding milestone-drawdown sequence	sequenceDiagram	3.4
10	On-chain subscription & capital-call sequence	sequenceDiagram	3.4
11	AML/CFT onboarding & monitoring flow	flowchart	4.4
12	Collective-investment-scheme boundary tree	flowchart	4.5
13	Regulatory-pathway roadmap (Gantt)	gantt	4.3
14	Tax structuring memorandum: decision flow	flowchart	8.3
15	Vendor-risk management lifecycle	flowchart	10.2

Diagram-type palette in this volume: flowchart, graph, stateDiagram, sequenceDiagram, gantt. Later volumes add C4/component, ER, and class/contract diagrams (Volume VII consolidates all).

END OF VOLUME I (interim draft)

Next: Volume II — Technical Architecture. Before final delivery of the package, all seven volumes undergo a single cross-volume Compliance & Completeness Audit; forward references are resolved; verbatim statutory text is inserted from the Appendix A sources; and the package is compiled to `.docx` on explicit request.

VOLUME II — TECHNICAL ARCHITECTURE

Institutional Digital Real Estate Capital Markets Infrastructure

Multi-Volume Documentation Package — Volume II of VII

TITLE PAGE & DOCUMENT CONTROL

Field	Detail
Document	Volume II — Technical Architecture
Package	Institutional Digital Real Estate Capital Markets Infrastructure (7 volumes)
Status	Working draft for internal review and engineering/security sign-off — **not a build specification or audit substitute in this form**
Version	II-0.1 (interim; full cross-volume Compliance & Completeness Audit pending completion of Volume VII)
Date of documentation	30 June 2026
Classification	Confidential — Draft
Companion volume	Volume I — Executive & Regulatory (legal architecture, token classification, jurisdictions)

Authorship and reliance caveat (read first). This volume is an AI-assisted engineering design document prepared to institutional standards of rigour. Technology names, standards identifiers, version numbers, and release dates cited here were checked against official or primary sources **as of 30 June 2026** and are footnoted to those sources. Nevertheless, this is a draft: **it must be reviewed and validated by qualified solution architects, smart-contract auditors, and security engineers before any implementation, procurement, or reliance.** This document references third-party software, protocols, and standards as design candidates and benchmarks only; it is not a recommendation, endorsement, or warranty of any third-party product, and it does not constitute legal, financial, or security advice. Where a design choice is open, it is presented as a labelled **option with trade-offs** rather than a settled decision.

On “latest releases.” Because the technology stack moves quickly, every load-bearing version claim in this volume (compiler, libraries, token standard, chain upgrade, cryptographic standards, oracle platform) was re-verified against the vendor or standards body on the date of documentation and recorded in **Appendix A — Standards & Versions Register**. Versions current at build time must be re-checked against that register before any code is written.

HOW TO READ THIS VOLUME (CONTROL FILE)

This is the condensed **Control File** reproduced atop every volume after Volume I. It carries (a) the canonical-term reminder, (b) the cross-volume reference map, and (c) the rule set this package follows. The full master glossary and citation register live in Volume I Appendices D–E and in this volume's Glossary and Appendix D.

Canonical terms (do not substitute synonyms). The instrument the platform issues is a **ledger-based security** (Swiss CO Art. 973d; see Vol. I §4.1) implemented on-chain as a **permissioned token** conforming to **ERC-3643 / T-REX**. "The platform" denotes the institutional infrastructure as a whole. "Model A" = asset-backed issuance; "Model B" = forward-funding / development finance (both defined in Vol. I Ch. 3). "On-chain" vs "off-chain" are used precisely: the register of title is on-chain; personal data and source documents are off-chain (see §1.4 and Vol. I §9).

Cross-volume reference map.

Volume	Scope	This volume relies on / feeds
I	Executive & Regulatory	Legal basis for every control here (token = security; eligibility; segregation; data-protection split)
II	**Technical Architecture (this volume)**	**Implements Vol. I controls in code and infrastructure**
III	Marketplace & Trading	Consumes the contract and settlement interfaces defined here (§3, §9)
IV	Financial Intelligence	Consumes the oracle/data layer (§5) and valuation/NAV feeds
V	Security & Operations	Deepens custody (§7), key ceremonies, PQC migration (§8), DevSecOps (§10)
VI	Business & Financial Model	Tokenomics and cost model reference the stack here (§12)
VII	Architecture Atlas	Consolidates every diagram in this volume

Rule set (unchanged from Vol. I). No fabricated facts or citations; version and standards claims verified against primary sources and registered in Appendix A; design options labelled with trade-offs; commentary paraphrased; hyperlinks given **only** to official sources verified live on the date of documentation, with all other sources cited by name/identifier to avoid link rot.

DETAILED TABLE OF CONTENTS

- Architecture Principles & the C4 Model
- Chain Layer & Network Topology
- Smart-Contract Architecture (ERC-3643 / T-REX, Upgradeability, Dual-Mode Funding)
- Identity, Compliance & Eligibility Enforcement
- Oracle & Data Layer
- Off-Chain Platform — Microservices Architecture
- Custody & Key Management (Architectural)
- Cryptography — Zero-Knowledge Proofs & Post-Quantum Readiness
- Fiat, Banking & Settlement Integration
- Security Architecture & DevSecOps
- Observability, Resilience & Scalability
- Technology Stack, Standards Register & Limitations

3. Interim Compliance & Completeness Audit (Volume II)
4. Future Jurisdiction & Technology Compatibility Notes
5. Glossary (technical)
6. Appendices A–E
7. Diagram Inventory

LIST OF FIGURES

Figure	Title	Section
1	System context (C4 Level 1)	1.3
2	Container view (C4 Level 2)	1.3
3	On-chain / off-chain split	1.4

Figure	Title	Section
4	Network topology — permissioned Avalanche L1 & interop	2.3
5	Chain-choice decision tree	2.2
6	ERC-3643 / T-REX contract suite (component view)	3.1
7	Compliant-transfer sequence	3.2
8	Dual-mode funding contracts (Model A / Model B)	3.3
9	Forward-funding escrow & milestone-drawdown sequence	3.3
10	UUPS upgrade flow with namespaced storage	3.4
11	Identity & claim-issuance flow (ONCHAINID)	4.2
12	Oracle & data-layer dataflow	5.2
13	Off-chain microservices	6.2

Figure	Title	Section
	container diagram	
14	End-to-end subscription sequence (off-chain ↔ on-chain)	6.3
15	Crypto-agility & PQC layering	8.3
16	Delivery-versus-payment (DvP) settlement sequence	9.2
17	CI/CD with security gates (DevSecOps)	10.2

LIST OF TABLES

Table	Title	Section
1	Architecture principles → mechanisms	1.2

Table	Title	Section
2	Chain-deployment options & trade-offs	2.2
3	ERC-3643 / T-REX contracts and roles	3.1
4	Compliance-module → Vol. I legal-rule mapping	4.3
5	Oracle services and their uses	5.2
6	Microservice catalogue	6.2
7	NIST PQC standards and platform application	8.2
8	Technology stack & versions (summary)	12.1

Table	Title	Section
9	Technical threats & limitations register	12.3

EXECUTIVE SUMMARY

This volume specifies how the legal architecture of Volume I is realised in software and infrastructure, under one governing principle: **compliance is enforced by construction, not by policy.** A transfer that Volume I says is unlawful must be one the smart contract **cannot execute**, not merely one an off-chain system flags after the fact.

The design rests on five decisions. **First**, the register of title is a permissioned token conforming to **ERC-3643 / T-REX** — the only Ethereum token standard for regulated securities that has reached "Final" status and is governed by an industry association[119][120] — with on-chain identity via **ONCHAINID**. This binds Volume I's eligibility rules (KYC/AML, accreditation, jurisdiction, holder caps, lock-ups) into the token itself. **Second**, the platform runs on a **permissioned, EVM-compatible chain**; the recommended option is a sovereign **Avalanche L1** (the model introduced by the Avalanche9000 "Etna" upgrade, which replaced subnets with sovereign L1s carrying their own validator set and compliance posture)[121], with interoperability to public liquidity via cross-chain messaging. **Third**, off-chain value (prices, FX, fund NAV, reserve attestations, bank events) reaches the chain only through a **decentralised oracle layer** with proof-of-reserve "secure mint" gating for the asset-backed model.[122] **Fourth**, the platform is **crypto-agile and post-quantum-aware** from day one: classical primitives today, but with a migration path to the **NIST PQC standards FIPS 203/204/205** finalised in 2024, plus the HQC backup KEM selected in 2025 and the FALCON-based FIPS 206 still in development.[123][124] **Fifth**, the off-chain platform is a set of **independently deployable microservices** behind an API gateway, event-driven, with

[119] ERC-3643 Association / T-REX materials — permissioned-token suite, ONCHAINID (ERC-734/735), Agent roles, recovery, modular compliance; standard semantics confirmed via the EIP registry. Paraphrased.

[120] EIP-3643, Ethereum EIP registry — "Final" status and standardised interfaces. Verified live 30 Jun 2026: https://eips.ethereum.org/EIPS/eip-3643

[121] Avalanche "Etna" upgrade (Avalanche9000) — sovereign L1 model (ACP-77), Validator Manager, sub-second Snowman finality, interchain messaging; activated on mainnet 16 Dec 2024. Verified live: https://www.avax.network/about/blog/etna-enhancing-the-sovereignty-of-avalanche-l1-networks

[122] Decentralised oracle platform documentation — proof-of-reserve / secure mint, NAV feeds, DvP and interoperability for tokenised assets; regulator-supervised pilot precedents. Paraphrased from provider primary documentation.

hard separation between the on-chain register and the off-chain personal-data and document stores (the immutability-vs-erasure split of Vol. I §9).

The remainder of the volume develops each layer with C4 views, contract-level component and sequence diagrams, a microservice catalogue, a custody and key-management architecture, a cryptography chapter covering zero-knowledge proofs and the post-quantum migration, the fiat/settlement integration including delivery-versus-payment, and a DevSecOps and resilience treatment. Every load-bearing version is registered in Appendix A. Open items and honest limitations are gathered in the Interim Audit and the §12.3 register; deeper custody, key-ceremony, and stress-test material is deferred to Volume V.

CHAPTER 1 — ARCHITECTURE PRINCIPLES & THE C4 MODEL

1.1 The governing principle: compliance by construction

Volume I established that the platform's instruments are securities (ledger-based securities under Swiss law; financial instruments under MiFID II; asset-referenced tokens or security tokens in other regimes). The central engineering consequence is that **the legal envelope must be expressed as executable constraints.** Where Volume I says a transfer is permitted only between eligible investors, the contract must verify eligibility atomically inside the transfer; where Volume I requires segregation, the architecture must keep client assets outside any operator insolvency estate; where Volume I requires a prospectus or disclosure, the issuance workflow must gate minting on that artifact's existence.

This is the defining difference between a compliant-by-construction system and a compliance wrapper: in the former, a non-compliant action is **architecturally impossible**; in the latter, it is merely detected. The ERC-3643 design enforces this at the token level — its `transfer` and `transferFrom` are conditional, executing only when both investor rules (via on-chain identity) and offering rules (via modular compliance) are satisfied.[125]

---

[123] NIST Post-Quantum Cryptography standardisation programme — FIPS 203/204/205; HQC selected 11 Mar 2025; FIPS 206 (FN-DSA) in development; migration timelines. Verified live: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

[124] NIST — release of the first three finalised PQC standards (FIPS 203/204/205), 13 Aug 2024. Verified live: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

1.2 Principles and the mechanisms that implement them

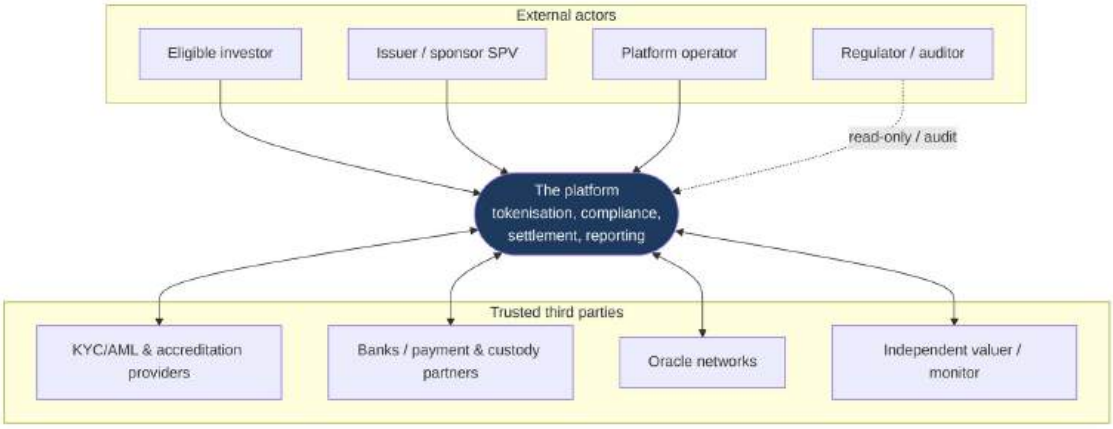
Principle	Mechanism in this architecture	Volume reference
Compliance by construction	ERC-3643 conditional transfers; modular compliance; on-chain identity	§3, §4
Substance-over-form portability	Compliance rules are data-driven modules, swappable per jurisdiction	Vol. I §1; §4.3
Segregation / bankruptcy remoteness	SPV-owned assets; client tokens self-custodied or in segregated custody; no operator commingling	Vol. I §4.6; §7
Defence in depth	Layered controls: chain, contract, oracle, service, key, network	§10
Crypto-agility	Abstracted cryptographic interfaces; hybrid classical+PQC migration path	§8
Least privilege & separation of duties	Agent roles, multisig, RBAC, segregated key custody	§3.1, §7, §10
On-chain/off-chain data split	Register on-chain; PII and documents off-chain with hashes anchored	§1.4; Vol. I §9
Verifiability & auditability	Event logs, deterministic state, oracle attestations, proof-of-reserve	§5, §10
Resilience & recoverability	HA/DR, deterministic finality handling, ERC-3643 recovery, key recovery	§7, §11

1.3 C4 system and container views

The architecture is described with the **C4 model** (Context, Container, Component, Code), which separates concern at increasing resolution. Figure 1 is the Level-1 context: who and what the system talks to. Figure 2 is the Level-2 container view: the major deployable units.

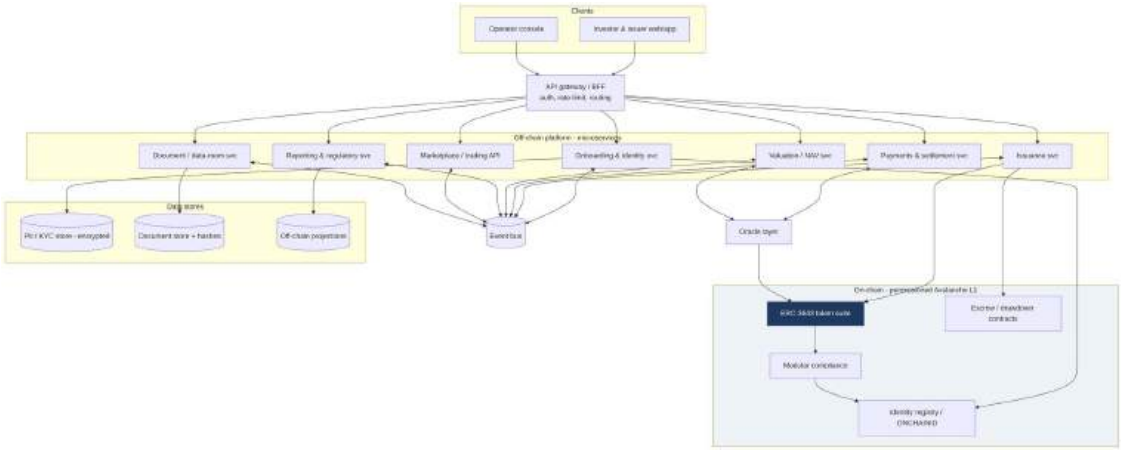
Figure 1 — System context (C4 Level 1).

[125] ERC-3643 Association / T-REX materials — permissioned-token suite, ONCHAINID (ERC-734/735), Agent roles, recovery, modular compliance; standard semantics confirmed via the EIP registry. Paraphrased.



The platform sits between eligible investors and issuers, mediated by trusted third parties for identity, money, data, and valuation. Regulators have read/audit access, not transactional access.

Figure 2 — Container view (C4 Level 2).



Clients reach a single gateway; off-chain microservices own workflow and personal data; the on-chain layer owns the register of title and compliance enforcement; the oracle layer is the only sanctioned bridge for off-chain truth.

1.4 The on-chain / off-chain split

Volume I §9 identified the core tension: a blockchain register is immutable, but data-protection law grants erasure rights. The architecture resolves this by **never placing personal data on-chain.** On-chain, an address is linked to an **ONCHAINID** identity contract that stores only *references and hashes* of signed claims (KYC passed, accreditation held, jurisdiction = X), not the underlying personal data.[126] The personal

[126] ERC-3643 Association / T-REX materials — permissioned-token suite, ONCHAINID (ERC-734/735), Agent roles, recovery, modular compliance; standard semantics confirmed via the EIP registry. Paraphrased.

data and source documents live off-chain in encrypted stores; erasure is performed off-chain, and the on-chain claim can be revoked. This preserves both the immutability of the register and the erasability of personal data.

Figure 3 — On-chain / off-chain split.

Only hashes and claim references cross the boundary onto the chain; the erasable personal data never does. Revoking an off-chain claim invalidates the on-chain eligibility without mutating the register.

CHAPTER 2 — CHAIN LAYER & NETWORK TOPOLOGY

2.1 Requirements on the chain layer

The chain must support: (a) EVM smart contracts (to run ERC-3643/T-REX); (b) permissioning or compliance-gating compatible with eligibility enforcement; (c) fast, deterministic finality (capital-markets settlement cannot tolerate long probabilistic finality or deep reorgs); (d) predictable, low fees; (e) interoperability with public liquidity and settlement assets; and (f) a governance and validator model an institution can defend to a regulator. These requirements drive the options in §2.2.

2.2 Deployment options and trade-offs

Option	Description	Pros	Cons / risks
A. Public L1 (e.g. Ethereum mainnet)	Deploy contracts on a public permissionless L1	Deepest liquidity, neutrality, security budget	High/volatile fees; ~13-min economic finality; no native permissioning; public mempool exposure
B. Public L2 rollup	Deploy on an Ethereum L2	Lower fees; inherits L1 security; EVM	Sequencer centralisation/observability; finality depends on L1; limited control of validator/compliance posture
C. Sovereign permissioned chain (recommended): Avalanche L1	A dedicated EVM (Subnet-EVM) L1 with its own validator set and rules	Custom validator/compliance; sub-second deterministic finality; low, stable fees; institutional precedent	Operator responsibility for validators; bootstrapping liquidity; interop via bridges/messaging

Option	Description	Pros	Cons / risks
D. Other enterprise/permissioned EVM	Consortium chain	Control, privacy	Smaller ecosystem/tooling; interop friction

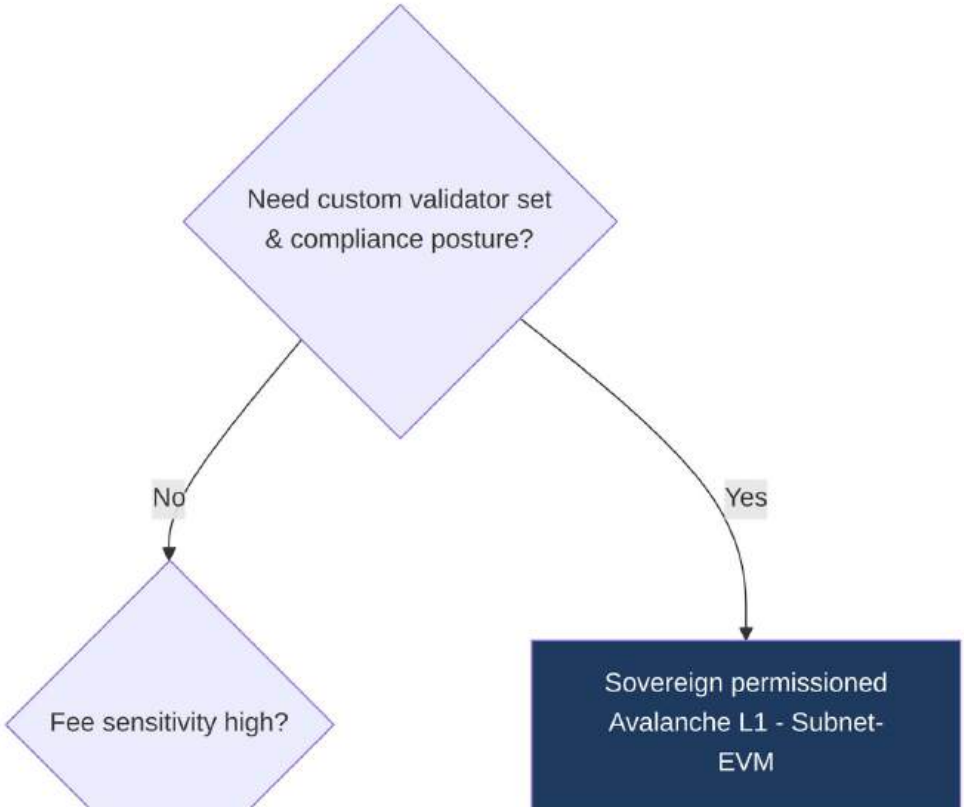
Recommendation and rationale (design option, not a settled decision). The recommended primary is **Option C — a sovereign, permissioned Avalanche L1**. Following the Avalanche9000 "Etna" upgrade (activated on mainnet 16 December 2024, implementing ACP-77), application-specific chains became **sovereign Layer-1s** with their own validator sets, custom gas tokens, governance, and compliance posture, decoupled from the Primary Network's staking requirement and instead paying a small continuous validator fee.[127][128] This directly satisfies requirements (b), (c), (d), and (f): an institution can run a compliance-gated L1 with a known validator set and sub-second deterministic finality (Snowman consensus), while retaining EVM tooling via Subnet-EVM and interoperating with public liquidity through cross-chain messaging (Avalanche Interchain Messaging / Teleporter) and a cross-chain interoperability protocol (§2.3).[129] The original programme concept of "an L2 rollup settling to a public L1" remains a viable Option B and is retained as a fallback; the sovereign-L1 path is preferred because eligibility-gating, validator governance, and finality are first-class rather than inherited. **This choice must be confirmed with counsel and the validator-operations plan in Volume V.**

Figure 5 — Chain-choice decision tree.

[127] Avalanche "Etna" upgrade (Avalanche9000) — sovereign L1 model (ACP-77), Validator Manager, sub-second Snowman finality, interchain messaging; activated on mainnet 16 Dec 2024. Verified live: https://www.avax.network/about/blog/etna-enhancing-the-sovereignty-of-avalanche-l1-networks

[128] Avalanche Community Proposal ACP-77 ("Reinventing Subnets"). Cited by identifier.

[129] Avalanche "Etna" upgrade (Avalanche9000) — sovereign L1 model (ACP-77), Validator Manager, sub-second Snowman finality, interchain messaging; activated on mainnet 16 Dec 2024. Verified live: https://www.avax.network/about/blog/etna-enhancing-the-sovereignty-of-avalanche-l1-networks



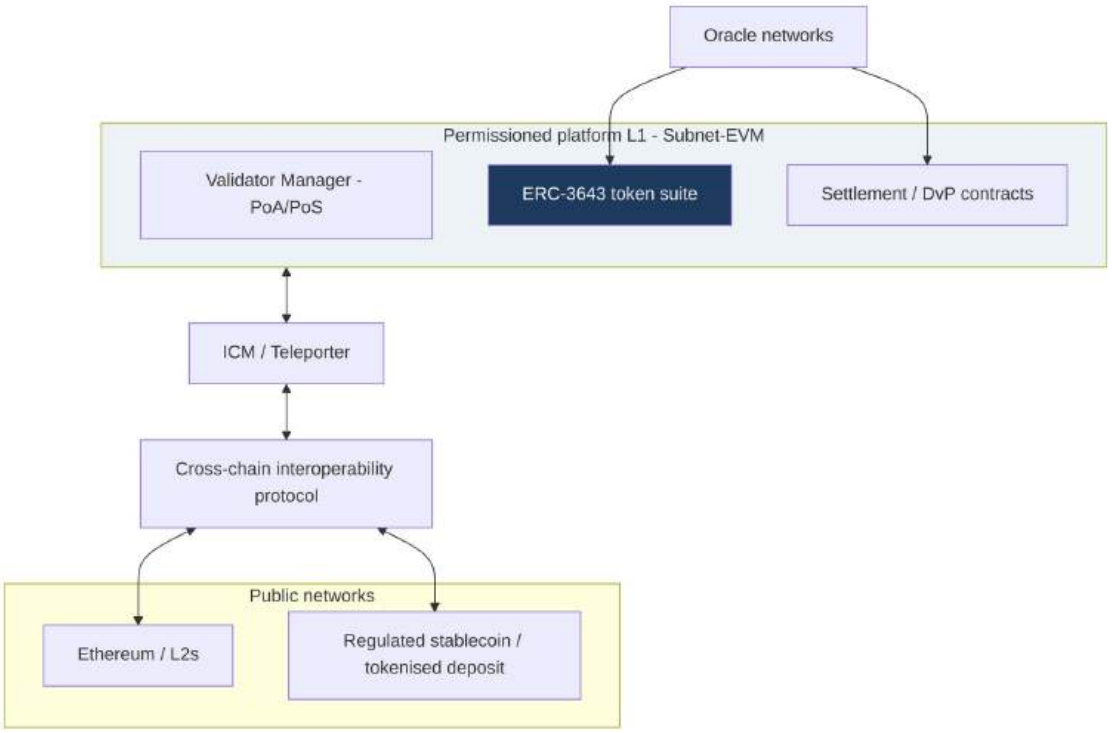
2.3 Network topology and interoperability

The platform L1 hosts the ERC-3643 suite and settlement contracts. It connects outward through two complementary mechanisms: native **Avalanche Interchain Messaging (ICM/Teleporter)** for chains in the Avalanche ecosystem, and a **cross-chain interoperability protocol (CCIP)** for reaching public networks and moving regulated value with compliance metadata attached.[130][131] A regulated settlement asset (a tokenised deposit or a fiat-backed stablecoin with proof-of-reserve) provides the cash leg for delivery-versus-payment (§9).

Figure 4 — Network topology: permissioned Avalanche L1 & interoperability.

[130] Avalanche “Etna” upgrade (Avalanche9000) — sovereign L1 model (ACP-77), Validator Manager, sub-second Snowman finality, interchain messaging; activated on mainnet 16 Dec 2024. Verified live: https://www.avax.network/about/blog/etna-enhancing-the-sovereignty-of-avalanche-l1-networks

[131] Cross-chain interoperability protocol documentation — cross-chain transfer of value and compliance metadata. Paraphrased.



The platform L1 keeps the register and settlement under its own validator and compliance governance, while messaging and interoperability protocols connect it to public liquidity and the cash settlement asset.

The **Validator Manager** contract (a pattern made available with the Etna upgrade) lets the L1 enforce proof-of-authority initially — a known, vetted validator set appropriate for a regulated venue — and migrate to proof-of-stake or a hybrid as the network matures, without changing the application layer.[132] Validator-operations detail (geographic distribution, HSM-protected signing keys, key ceremonies) is specified in Volume V.

CHAPTER 3 — SMART-CONTRACT ARCHITECTURE

3.1 The ERC-3643 / T-REX suite

The register of title is implemented with the **ERC-3643 (T-REX) permissioned-token standard**. ERC-3643 reached **"Final" status** as an Ethereum standard (the only securities-token standard to do so) and is maintained through the **ERC-3643**

[132] Avalanche "Etna" upgrade (Avalanche9000) — sovereign L1 model (ACP-77), Validator Manager, sub-second Snowman finality, interchain messaging; activated on mainnet 16 Dec 2024. Verified live: https://www.avax.network/about/blog/etna-enhancing-the-sovereignty-of-avalanche-l1-networks

Association; its open-source reference implementation, T-REX, has been used to tokenise a very large volume of real-world assets and has been independently audited.[133][134] It extends ERC-20 (so existing wallets and tooling interoperate) but overrides `transfer`/`transferFrom` to route every movement through identity and compliance checks. The suite is deliberately **modular** — responsibilities are split across contracts so that compliance rules and identity logic evolve without redeploying the token.

Contract	Responsibility	Key roles
Token (ERC-3643)	ERC-20-compatible security token; conditional transfers; mint/burn; pause; freeze; forced transfer; recovery	Agent, Owner
Identity Registry	Maps wallet → on-chain identity; checks verified status	Agent
Identity Registry Storage	Shared storage of identities (reusable across tokens)	Owner
Trusted Issuers Registry	Which claim issuers are trusted (e.g. KYC provider)	Owner

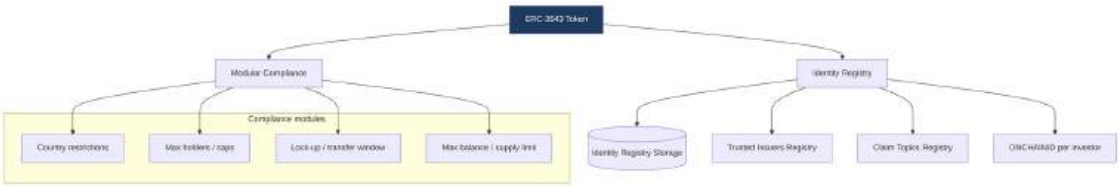
[133] ERC-3643 Association / T-REX materials — permissioned-token suite, ONCHAINID (ERC-734/735), Agent roles, recovery, modular compliance; standard semantics confirmed via the EIP registry. Paraphrased.

[134] EIP-3643, Ethereum EIP registry — “Final” status and standardised interfaces. Verified live 30 Jun 2026: https://eips.ethereum.org/EIPS/eip-3643

Contract	Responsibility	Key roles
Claim Topics Registry	Which claim topics are required (KYC, accreditation, jurisdiction)	Owner
Modular Compliance	Pluggable transfer rules (holder caps, country limits, lock-ups, max balances)	Owner
ONCHAINID	Per-investor identity contract; stores keys (ERC-734) and signed claims (ERC-735)	Identity owner, Claim issuers

Table 3 — ERC-3643 / T-REX contracts and roles. The **Agent** role performs sensitive lifecycle actions (mint, burn, freeze, forced transfer, recovery of a lost wallet); these powers are necessary for a regulated security (court orders, AML freezes, key loss) and are themselves guarded by multisig and separation-of-duties (§7, §10).

Figure 6 — ERC-3643 / T-REX contract suite (component view).

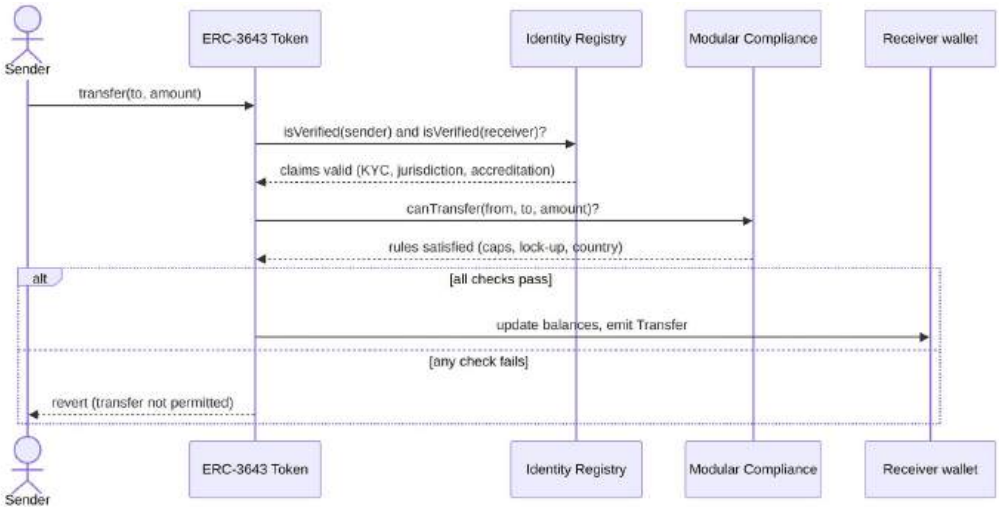


The token delegates "who may hold" to the Identity Registry (via ONCHAINID claims and trusted issuers) and "which transfers are allowed" to Modular Compliance (via swappable rule modules). Each maps directly to a Volume I legal rule (§4.3).

3.2 The compliant transfer

Every transfer is a multi-contract validation before any balance changes. If any check fails, the transfer **reverts** — it is rejected at the contract level, not reversed afterward.

Figure 7 — Compliant-transfer sequence.



Eligibility and offering rules are evaluated atomically inside the transfer; the only way a non-compliant transfer "happens" is that it does not.

3.3 Dual-mode funding contracts

Volume I defined two funding models. The contract architecture realises both on the same token base.

Model A — asset-backed issuance. The SPV owns an existing income-producing asset; tokens are issued against it. Minting is gated on **proof-of-reserve / proof-of-backing** so that supply cannot exceed the verified asset/collateral position (§5).[135] Distributions (rent, income) are computed off-chain and paid through the payments service, with on-chain events as the audit trail.

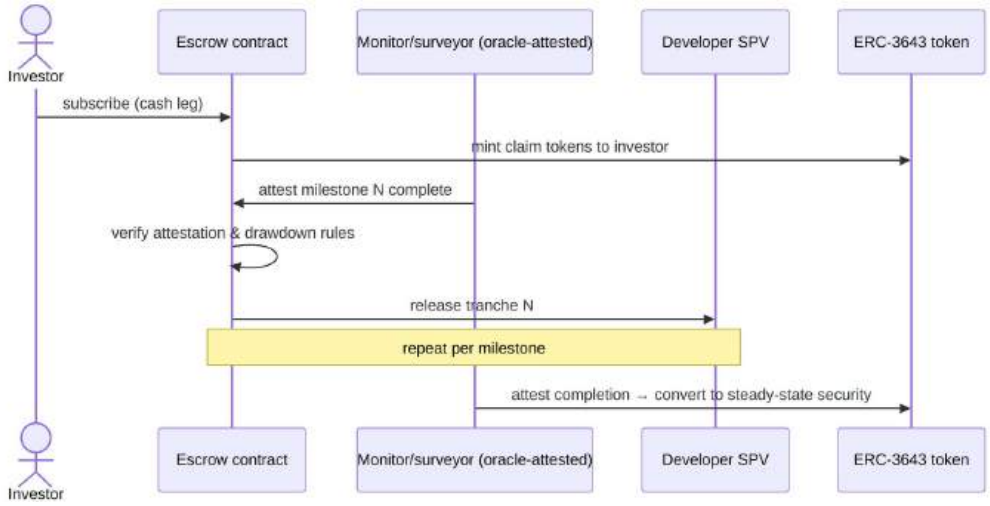
Model B — forward-funding / development finance. Capital is raised before the asset exists; subscriptions flow into an **escrow contract** and are released to the developer only as independently certified milestones are met (mirroring Vol. I Fig. 9). Tokens represent a claim on the future asset and income, converting to the steady-state security on completion.

Figure 8 — Dual-mode funding contracts (Model A / Model B).

[135] Decentralised oracle platform documentation — proof-of-reserve / secure mint, NAV feeds, DvP and interoperability for tokenised assets; regulator-supervised pilot precedents. Paraphrased from provider primary documentation.

Model A gates supply on verified backing; Model B gates the release of cash on independently certified construction milestones. Both use the same ERC-3643 token base, differing in the minting/escrow logic around it.

Figure 9 — Forward-funding escrow & milestone-drawdown sequence.



The escrow contract is the trust-minimising core of Model B: cash moves to the developer only against an attested milestone, and never ahead of construction.

3.4 Upgradeability and storage safety

Regulated infrastructure must be patchable (bug fixes, new compliance modules, new jurisdictions) without migrating the register. The architecture uses the **UUPS proxy pattern** from the OpenZeppelin Contracts library (current major line 5.x; UUPS now ships in the main `@openzeppelin/contracts` package).[136] Upgrade authority is held by a **multisig + timelock**, never a single key, so that an upgrade is a governed, observable event (§10). To prevent storage-collision bugs across upgrades, contracts use **ERC-7201 namespaced storage layouts** — for which the Solidity compiler now provides a built-in (`erc7201`) as of v0.8.35.[137] Contracts target a pinned, recent Solidity

[136] OpenZeppelin Contracts release notes — 5.x line (current 5.6.1); UUPSUpgradeable now in the main `@openzeppelin/contracts` package; EIP-7702 signer support. Verified live: https://github.com/OpenZeppelin/openzeppelin-contracts/releases

version (0.8.x line; see Appendix A), mindful of the deprecations scheduled for the forthcoming 0.9.0 breaking release.[138]

Figure 10 — UUPS upgrade flow with namespaced storage.

State lives in the proxy under collision-resistant namespaced storage; logic is swapped only by a multisig-plus-timelock authority, making every upgrade a governed, auditable event. Upgradeability and its risks (centralisation, upgrade keys) are revisited in §10 and Volume V.

CHAPTER 4 — IDENTITY, COMPLIANCE & ELIGIBILITY ENFORCEMENT

4.1 Why identity is part of the protocol

In a permissionless ERC-20, anyone can hold the token; for a security that is unlawful. ERC-3643 makes identity a **first-class part of the token**: no verified on-chain identity, no holding. Identity is expressed through **ONCHAINID**, a self-managed identity contract per investor that holds cryptographic keys (the ERC-734 key-holder pattern) and signed **claims** (the ERC-735 claim-holder pattern) issued by trusted parties.[139] Crucially, the identity contract stores **claim references and hashes, not personal data** (§1.4), so the protocol verifies eligibility without putting PII on-chain.

---

[137] Solidity compiler release notes — current 0.8.35; `erc7201` builtin for ERC-7201 namespaced storage; deprecations scheduled for 0.9.0. Verified live: https://github.com/ethereum/solidity/releases

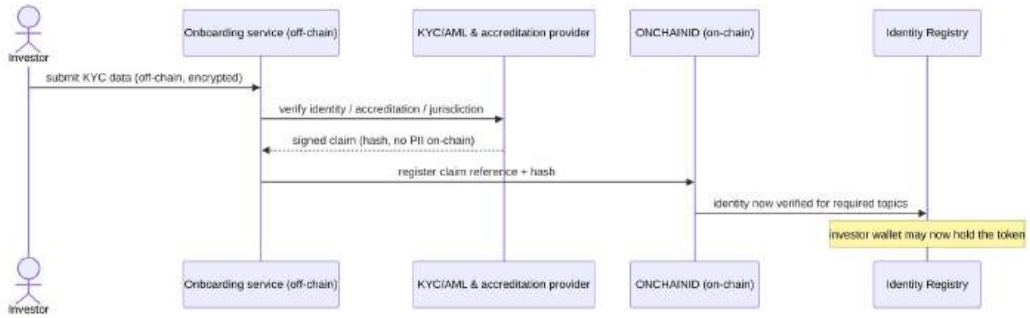
[138] Solidity compiler release notes — current 0.8.35; `erc7201` builtin for ERC-7201 namespaced storage; deprecations scheduled for 0.9.0. Verified live: https://github.com/ethereum/solidity/releases

[139] ERC-3643 Association / T-REX materials — permissioned-token suite, ONCHAINID (ERC-734/735), Agent roles, recovery, modular compliance; standard semantics confirmed via the EIP registry. Paraphrased.

4.2 Claim issuance and verification

A claim issuer (e.g. a KYC/AML provider, an accreditation verifier, a jurisdiction attestor) signs a claim about an investor; the claim is registered against the investor's ONCHAINID; the Trusted Issuers Registry says which issuers the platform accepts, and the Claim Topics Registry says which claims are required. At transfer time, the Identity Registry checks that both parties hold the required, valid claims from trusted issuers.

Figure 11 — Identity & claim-issuance flow (ONCHAINID).



Personal data stays off-chain; only a signed claim hash is anchored. Revoking the off-chain claim removes on-chain eligibility without altering the register — the mechanism that reconciles immutability with the right to erasure (Vol. I §9).

4.3 Mapping compliance modules to Volume I legal rules

The strength of the modular design is that each on-chain rule maps to a specific legal requirement established in Volume I. New jurisdictions are added by composing modules, not by re-architecting — the "substance-over-form portability" principle made concrete.

Compliance module (on-chain)	Enforces	Volume I basis
Identity/claim verification	Only KYC/AML-cleared, eligible investors hold	§4.4 (AMLA); §3.5 (eligibility)
Country/jurisdiction restriction	Offer/holding limited to permitted jurisdictions	Ch. 5–7 (per-jurisdiction perimeters)
Accreditation/professional-client gate	Restrict to qualified/professional investors where required	§4.2 (FinSA exemptions); §6 (MAS/HK)
Max-holders / holder-cap module	Stay within private-placement /	§4.2 (FinSA Art. 36); §6.2 (MAS)

Compliance module (on-chain)	Enforces	Volume I basis
	exemption thresholds	
Lock-up / transfer-window module	Enforce statutory or offering hold periods	§3.5; offering terms
Max-balance / supply-cap module	Concentration and offering-size limits	§4.2 (≤CHF 8m/12mo where relied on)
Pause / freeze / forced-transfer	AML freezes, court orders, error correction	§4.4; §4.6

Table 4 — Compliance-module → Volume I legal-rule mapping. Privacy-preserving variants of these checks — proving accreditation or jurisdiction **without revealing the underlying data** — are addressed with zero-knowledge and confidential-compute techniques in §8 and the oracle/privacy options in §5.

CHAPTER 5 — ORACLE & DATA LAYER

5.1 The data gap

A blockchain is deterministic and isolated: it knows only its own state. A tokenised real-world asset needs external truth — the price of a currency, the rate on a bond, the **net asset value (NAV)** of a fund, the **reserve** backing an asset-backed token, the occurrence of a bank payment, the certification of a construction milestone. Bringing that truth on-chain securely is the oracle problem, and the central question is not whether data can be imported but **who is trusted to import it and how much damage they can do if wrong.** The architecture therefore uses a **decentralised oracle network** rather than a single feed, and treats oracle integration as a security-critical dependency (§10, §12.3).

5.2 Oracle services and their uses

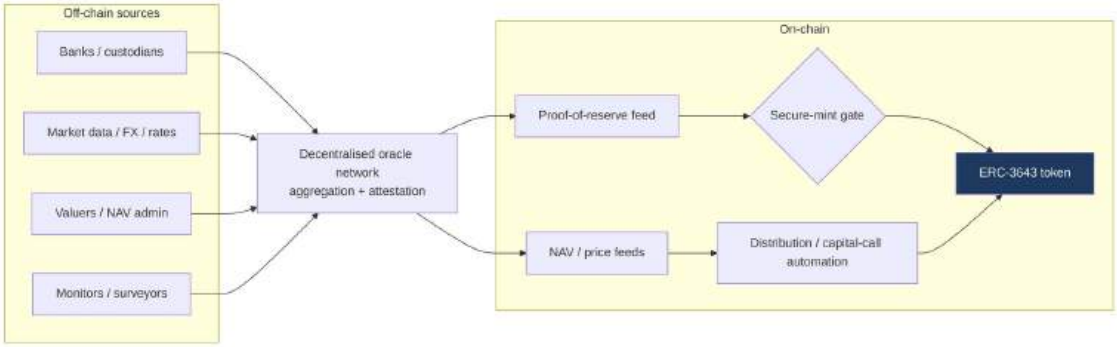
The platform consumes a layered set of oracle services. The reference candidate is a decentralised oracle platform offering data, proof-of-reserve, interoperability, compliance, and privacy services under one orchestration layer; the design, however, abstracts the oracle behind an interface so that providers can be swapped or run in parallel for resilience.

Oracle service	Platform use	Model
Price / FX / rate feeds	Valuation inputs, currency conversion, coupon math	A & B
NAV feeds	Fund/asset NAV for pricing and reporting	A (primary)

Oracle service	Platform use	Model
Proof of Reserve + “secure mint”	Gate minting on verified backing; halt mint if reserves fall short	A (critical)
Off-chain functions	Pull bank-payment confirmation, appraisal data, milestone attestations	A & B
Automation / scheduling	Trigger distributions, capital calls, recurring jobs	A & B
Verifiable randomness	Fair allocation in oversubscribed offerings (optional)	A & B
Cross-chain messaging + compliance metadata	Move value and identity attestations across chains	A & B

Table 5 — Oracle services and their uses. The **proof-of-reserve “secure mint”** capability is the linchpin of Model A integrity: reserve checks are integrated directly into the token’s mint logic so that new tokens are created only when backing is verified, preventing over-issuance.[140] NAV feeds and FX/rate feeds power valuation and reporting (Volume IV builds on this layer for the financial-intelligence models).

Figure 12 — Oracle & data-layer dataflow.



Multiple independent sources are aggregated and attested by a decentralised network before any value enters the chain; minting is gated on reserves and distributions are driven by verified NAV/rate data.

5.3 Oracle risk and mitigations

Oracles are a system property, not a black box: misconfiguration, source compromise, or slow governance can still cause failure. Mitigations specified here and deepened in §10/§12.3: use decentralised networks with multiple premium sources; set deviation thresholds and heartbeat intervals; wire **circuit breakers** (pause minting/redemptions when reserve or NAV data is stale or breaches thresholds); maintain a **fallback oracle**

[140] Decentralised oracle platform documentation — proof-of-reserve / secure mint, NAV feeds, DvP and interoperability for tokenised assets; regulator-supervised pilot precedents. Paraphrased from provider primary documentation.

or multi-provider quorum; and subject oracle configuration to the same change-control and audit as contract code. Institutional precedents for oracle-driven tokenised-asset settlement, NAV, and proof-of-reserve exist in regulator-supervised pilots, which the platform's design follows rather than invents.[141]

CHAPTER 6 — OFF-CHAIN PLATFORM: MICROSERVICES ARCHITECTURE

6.1 Why microservices, and the boundaries

The off-chain platform owns everything that should not or cannot live on-chain: workflow, personal data, documents, fiat movement, reporting, and the user experience. It is built as **independently deployable microservices** behind an API gateway, communicating through an **event bus**, so that (a) services scale and fail independently, (b) the blast radius of a fault is contained, (c) personal-data services are isolated for data-protection control, and (d) the on-chain integration is concentrated in a few adapter services rather than smeared across the system. Service boundaries follow business capabilities (onboarding, issuance, payments, valuation, reporting, marketplace, documents), not technical layers.

6.2 Microservice catalogue

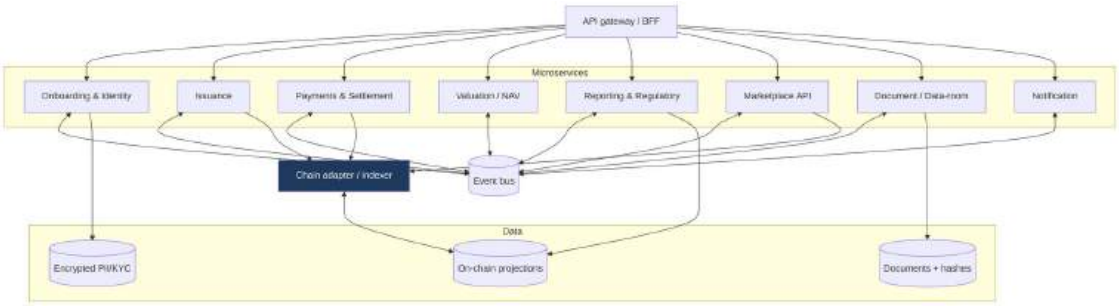
Service	Responsibility	Sensitive data?	Talks to chain?
Onboarding & Identity	KYC/AML orchestration, accreditation, ONCHAINID claim registration	Yes (PII)	Yes (identity registry)
Issuance	Offering setup, prospectus/KID gating, mint/escrow orchestration	No	Yes (token, escrow)
Payments & Settlement	Fiat/stablecoin rails, DvP coordination, reconciliation	Limited	Yes (settlement)
Valuation / NAV	NAV computation, oracle ingestion, pricing	No	Reads oracle
Reporting & Regulatory	Investor, tax (CRS/FATCA), and supervisory reporting	Yes	Reads projections
Marketplace / Trading API	Order intake, matching	No	Yes (transfer)

[141] Decentralised oracle platform documentation — proof-of-reserve / secure mint, NAV feeds, DvP and interoperability for tokenised assets; regulator-supervised pilot precedents. Paraphrased from provider primary documentation.

Service	Responsibility	Sensitive data?	Talks to chain?
	hand-off (Vol. III), quotes		
Document / Data-room	Legal docs, prospectus, valuations; hashing/anchoring	Yes (docs)	Anchors hashes
Notification	Email/SMS/push, audit notices	Limited	No
Admin / Console	Operator workflows, agent actions (guarded)	—	Yes (agent ops)

Table 6 — Microservice catalogue. Cross-cutting concerns — authentication (OIDC/OAuth2), authorization (RBAC), secrets management, audit logging, and observability — are provided as platform capabilities rather than per-service reinventions (§10, §11).

Figure 13 — Off-chain microservices container diagram.

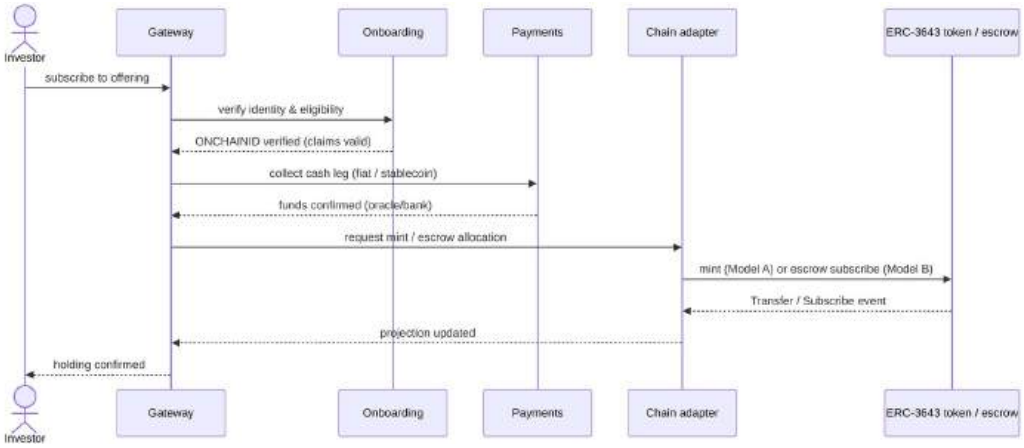


A single chain-adapter/indexer service mediates on-chain reads/writes and maintains off-chain projections of on-chain state, keeping blockchain coupling isolated and testable.

6.3 End-to-end subscription

The subscription flow shows how off-chain workflow and on-chain enforcement interlock: identity first, money second, mint last, each step gated.

Figure 14 — End-to-end subscription sequence (off-chain ↔ on-chain).



No mint occurs before both identity and money are confirmed; the chain adapter is the sole writer to the chain, and the projection store gives the UI a fast, consistent read model.

CHAPTER 7 — CUSTODY & KEY MANAGEMENT (ARCHITECTURAL)

7.1 What must be protected

Three classes of key exist: (a) **investor wallet keys** (control over their tokens); (b) **operator/agent keys** (privileged contract actions — mint, freeze, forced transfer, recovery, upgrades); and (c) **validator signing keys** (for the permissioned L1). Compromise of (b) or (c) is systemic; compromise of (a) is contained but must be recoverable because the token represents a legal title.

7.2 Custody models and key architecture

The architecture supports custodial, non-custodial, and hybrid models, and does not force investors into one. For operator/agent keys it mandates **multi-party control**: keys are generated and held under **MPC (multi-party computation) and/or HSMs validated to FIPS 140-3**, with **threshold signatures / multisig** so that no single person or device can act alone, and a **timelock** on the most sensitive actions (upgrades, large mints). Key ceremonies, quorum composition, geographic and organisational separation, and disaster recovery are specified in Volume V; this volume fixes the architectural requirement that **privileged actions require M-of-N approval and produce an immutable audit trail.**

ERC-3643's **recovery** function addresses the investor-key-loss problem unique to titled assets: an agent can, under governed conditions, re-link an investor's verified identity to a new wallet and move the balance, with the recovery recorded on-chain for

transparency.[142] This is a feature, not a bug, of regulated tokenisation: a lost private key must not mean a lost legal title.

Account abstraction for investor UX (option). To reduce the key-management burden on investors, the platform may offer **smart-contract accounts** via account-abstraction standards (ERC-4337) and the newer EOA-delegation mechanism (EIP-7702, enabled by the Ethereum Pectra upgrade), supporting social/multi-factor recovery, session keys, and sponsored gas — with the OpenZeppelin library now providing signer support for the EIP-7702 pattern.[143] These are optional UX enhancements layered on top of, never replacing, the compliance checks.

7.3 Architectural requirements (summary)

No raw private key for privileged roles exists in a single location or under single-person control; all privileged actions are M-of-N and timelocked where systemic; validator keys are HSM-protected and segregated from application keys; investor recovery is possible but governed and auditable; and all of the above is testable and observable. Depth — ceremony scripts, HSM models, rotation schedules, and dev-phase fund-run stress tests — is Volume V.

CHAPTER 8 — CRYPTOGRAPHY: ZERO-KNOWLEDGE PROOFS & POST-QUANTUM READINESS

8.1 Two cryptographic agendas

The platform has two forward-looking cryptographic agendas: **privacy** (prove eligibility and integrity without exposing personal or commercial data) and **longevity** (ensure today's cryptography does not become tomorrow's liability under quantum computing). The first is addressed with zero-knowledge proofs and confidential compute; the second with a crypto-agile path to the NIST post-quantum standards.

8.2 Zero-knowledge and confidential compute (privacy)

Several compliance checks ideally prove a fact without revealing the underlying data: *this investor is accredited* without disclosing their financial statements; *this investor is in*

---

[142] ERC-3643 Association / T-REX materials — permissioned-token suite, ONCHAINID (ERC-734/735), Agent roles, recovery, modular compliance; standard semantics confirmed via the EIP registry. Paraphrased.

[143] OpenZeppelin Contracts release notes — 5.x line (current 5.6.1); UUPSUpgradeable now in the main `@openzeppelin/contracts` package; EIP-7702 signer support. Verified live: https://github.com/OpenZeppelin/openzeppelin-contracts/releases

a permitted jurisdiction without publishing their address; *reserves exceed supply* without exposing account balances. **Zero-knowledge proofs (zk-SNARKs / zk-STARKs)** and **confidential-compute / oracle privacy** techniques make these *prove-without-revealing* checks possible, and can be combined with the ONCHAINID claim model so that the on-chain footprint is a proof, not the data.[144] Confidential token mechanics (e.g. encrypted balances via fully-homomorphic-encryption-based token extensions now emerging as standardised confidential-token work) are an option for offerings where holder balances must remain private while still compliant; these are evaluated as **options with maturity and audit caveats**, not yet as defaults.

8.3 Post-quantum readiness (longevity)

A sufficiently capable quantum computer would break the asymmetric cryptography (RSA, ECC/ECDSA) that secures wallets, TLS, and signatures. The threat is not only future: **“harvest-now, decrypt-later”** means data captured today can be decrypted later, so long-lived confidential data needs protection now. NIST has standardised the first post-quantum algorithms, and the platform’s design is **crypto-agile** so it can adopt them without re-architecture.

NIST standard	Algorithm (origin)	Function	Platform application
FIPS 203	ML-KEM (CRYSTALS-Kyber)	Key encapsulation / exchange	TLS, service-to-service channels, data-at-rest key wrapping
FIPS 204	ML-DSA (CRYSTALS-	Digital signatures	Document/claim signing,

[144] ERC-3643 Association / T-REX materials — permissioned-token suite, ONCHAINID (ERC-734/735), Agent roles, recovery, modular compliance; standard semantics confirmed via the EIP registry. Paraphrased.

NIST standard	Algorithm (origin)	Function	Platform application
	Dilithium)	(primary)	service auth, future on-chain signature schemes
FIPS 205	SLH-DSA (SPHINCS+)	Hash-based signatures (conservative backup)	High-assurance signing where lattice risk is a concern
FIPS 206 (in development)	FN-DSA (FALCON)	Signatures (compact)	Candidate where signature size matters; not yet published
HQC (selected 2025)	Code-based KEM	Backup key encapsulation	Diversity hedge against a lattice break; standard draft pending

Table 7 — NIST PQC standards and platform application. FIPS 203, 204, and 205 were **published on 13 August 2024**; **HQC** was **selected as a backup key-encapsulation mechanism on 11 March 2025**; and the FALCON-based **FIPS 206 (FN-DSA) remains in development.**[145][146] National-security guidance (NSA CNSA 2.0) targets migration by **2030**, and broad guidance recommends deprecating RSA/ECC by 2030 with full migration by 2035 — the timeline the platform's migration plan (Volume V) adopts.[147]

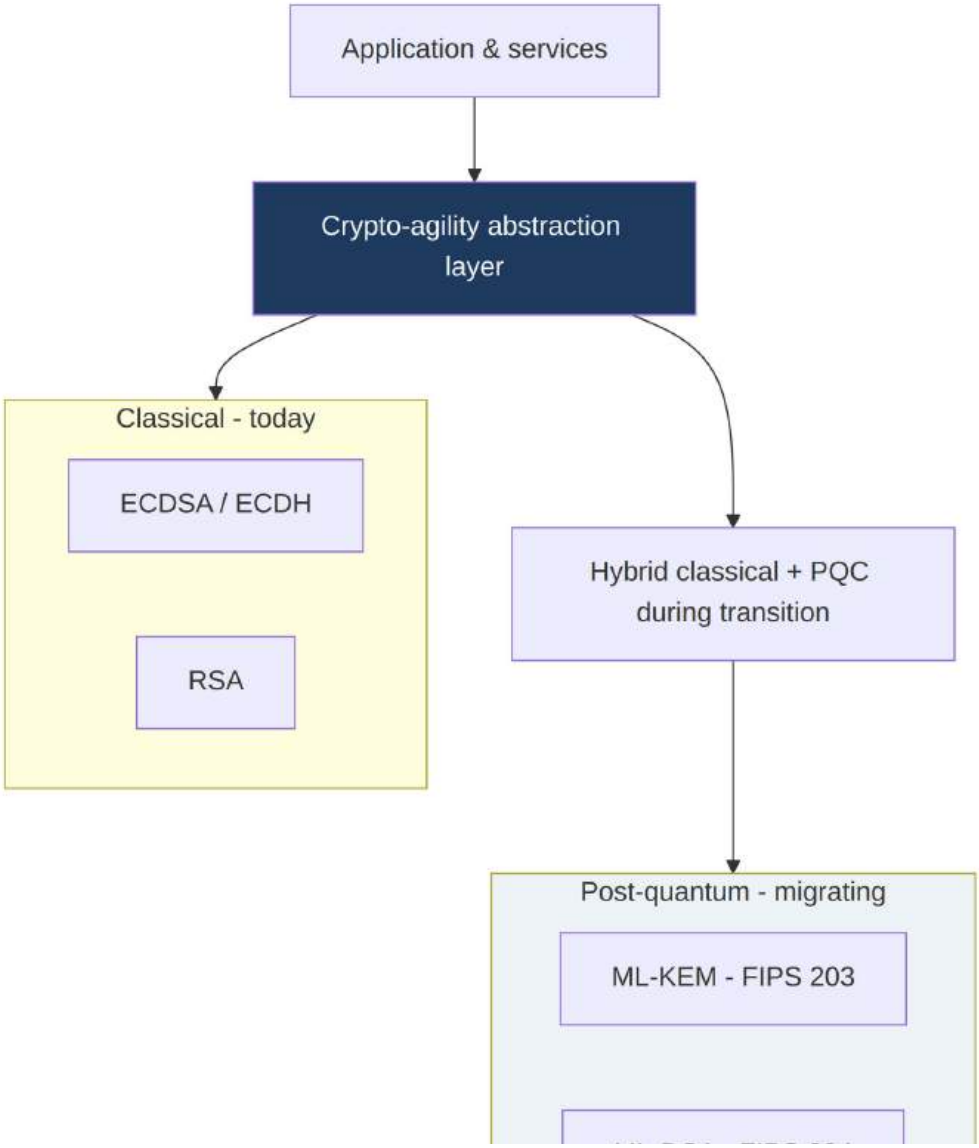
Migration strategy: hybrid + crypto-agility. The platform does not "rip and replace." It (a) abstracts cryptographic primitives behind interfaces so algorithms are configuration, not hard-coding; (b) deploys **hybrid** schemes during transition (a classical key exchange *and* ML-KEM together, so the channel is safe if either holds); (c) prioritises **long-lived secrets and harvestable channels** first; and (d) maintains an inventory of cryptographic dependencies to drive prioritised migration. A constraint to flag honestly: **on-chain** signature schemes are fixed by the underlying chain's protocol, so on-chain PQC depends on the chain adopting PQC-friendly signatures; the platform can act unilaterally off-chain (TLS, signing, data-at-rest) but must track chain-level PQC roadmaps for the on-chain layer.

Figure 15 — Crypto-agility & PQC layering.

[145] NIST Post-Quantum Cryptography standardisation programme — FIPS 203/204/205; HQC selected 11 Mar 2025; FIPS 206 (FN-DSA) in development; migration timelines. Verified live: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

[146] NIST — release of the first three finalised PQC standards (FIPS 203/204/205), 13 Aug 2024. Verified live: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[147] NIST Post-Quantum Cryptography standardisation programme — FIPS 203/204/205; HQC selected 11 Mar 2025; FIPS 206 (FN-DSA) in development; migration timelines. Verified live: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization



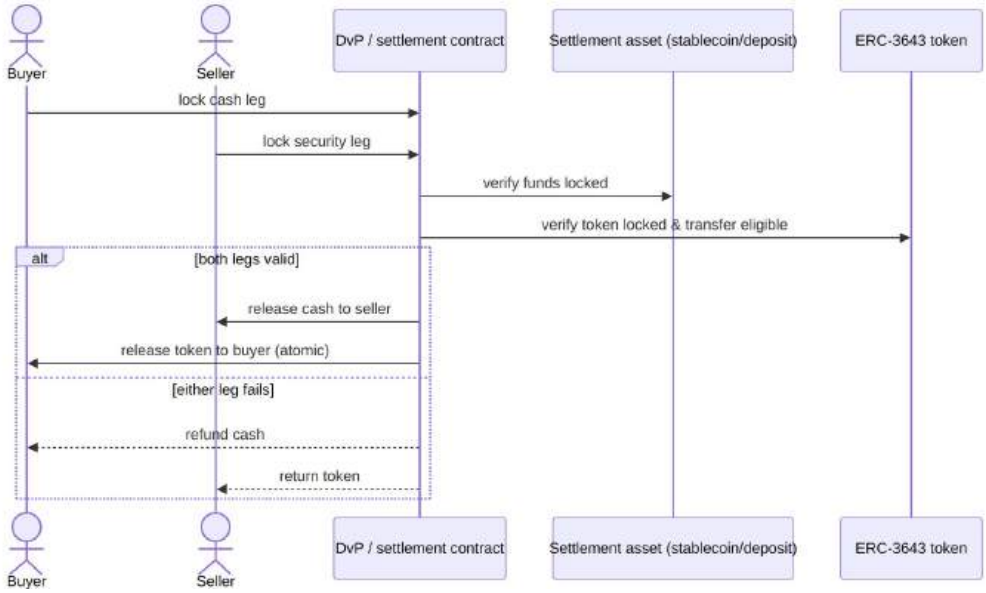
CHAPTER 9 — FIAT, BANKING & SETTLEMENT INTEGRATION

9.1 The cash leg and delivery-versus-payment

A securities transaction has two legs: the **security** (the token) and the **cash**. Settling them without one party being exposed to the other's default requires **delivery-versus-payment (DvP)** — the two legs settle atomically, or neither does. The architecture supports DvP by representing the cash leg on-chain as a **regulated settlement asset**

(a tokenised bank deposit or a fiat-backed stablecoin with proof-of-reserve) so that security and cash can be exchanged in a single atomic transaction or a coordinated cross-chain settlement.[148] Where the cash leg remains in the traditional banking system, the payments service coordinates a **hash-locked or escrow-based** settlement so the token does not move until payment is irrevocably confirmed.

Figure 16 — Delivery-versus-payment (DvP) settlement sequence.



Atomic DvP removes principal risk: the token and the cash change hands together or not at all. The transfer leg still passes ERC-3643 compliance checks, so DvP never bypasses eligibility.

9.2 Banking rails, messaging and reconciliation

Fiat on/off-ramps connect through banking partners via their APIs; payment messaging follows **ISO 20022** where the rails support it; and every on-chain settlement is reconciled against the off-chain bank/custody record by the payments service, with breaks raised as exceptions. The settlement-asset choice (tokenised deposit vs regulated stablecoin vs traditional rails with escrowed DvP) is a **design option** with trade-offs in finality, counterparty risk, and regulatory treatment (the settlement-asset classification was analysed in Vol. I §1.6); it must be fixed with treasury, banking partners, and counsel before build.

---

[148] Decentralised oracle platform documentation — proof-of-reserve / secure mint, NAV feeds, DvP and interoperability for tokenised assets; regulator-supervised pilot precedents. Paraphrased from provider primary documentation.

CHAPTER 10 — SECURITY ARCHITECTURE & DEVSECOPS

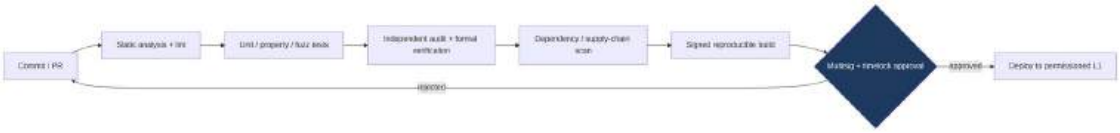
10.1 Threat model and defence in depth

Security is layered across chain, contract, oracle, service, key, and network tiers, each with its own controls, so that no single failure is catastrophic. A structured threat model (e.g. STRIDE — spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege) is applied per component, with smart-contract-specific threats (reentrancy, access-control flaws, oracle manipulation, upgrade-key compromise, front-running) treated explicitly. For EEA-facing activity the operational-resilience obligations of **DORA** (ICT risk management, incident reporting, third-party risk, resilience testing) apply and are mapped to these controls (Vol. I §1.5, §10).

10.2 Secure SDLC and pipeline gates

Smart-contract and service code passes through mandatory gates: static analysis and linting; unit/property/fuzz testing; **independent security audits** (more than one for contracts); **formal verification** of the most critical invariants (supply integrity, transfer-eligibility, escrow-drawdown conditions); dependency and supply-chain scanning; and signed, reproducible builds. Nothing reaches the permissioned L1 without passing the gate and a multisig-approved deployment.

Figure 17 — CI/CD with security gates (DevSecOps).



Security is a pipeline property: code is gated by automated checks, human audit, formal proofs of critical invariants, and a governed multisig deployment — never a single engineer pushing to production.

10.3 Runtime security and operations

Runtime controls include continuous monitoring of on-chain events and contract state (the open-source monitoring/relayer tooling that succeeds earlier hosted offerings), automated alerting and **circuit breakers** (pause minting/transfers on anomaly), an incident-response runbook, key-compromise and oracle-failure playbooks, and a **bug-bounty** programme. Privileged operator actions are logged immutably and reviewed. Deeper operational security — custody ceremonies, SOC tooling, red-team exercises, and dev-phase fund-run stress tests — is Volume V.

CHAPTER 11 — OBSERVABILITY, RESILIENCE & SCALABILITY

11.1 Observability and SRE

The platform is instrumented for metrics, logs, traces, and on-chain event indexing, with service-level objectives (SLOs) for the user-facing flows (onboarding, subscription, settlement, reporting). The chain-adapter/indexer maintains off-chain projections so dashboards and reports read a consistent model without hammering the chain.

11.2 Resilience and finality handling

Two resilience concerns are blockchain-specific. **Finality:** the platform treats a transaction as settled only at the chain's deterministic finality (sub-second on the recommended Avalanche L1 via Snowman consensus), avoiding the deep-reorg exposure of probabilistic chains.[149] **Availability:** services are deployed highly-available with disaster recovery; the permissioned L1's validator set is geographically and organisationally distributed (Volume V) so that no single site failure halts the chain. Off-chain, standard HA/DR (multi-AZ, backups, tested restores) applies.

11.3 Scalability

The off-chain platform scales horizontally per service behind the gateway and event bus. On-chain, the sovereign-L1 model scales by **isolation**: the platform's L1 does not compete for blockspace with unrelated applications, and additional throughput can be obtained by tuning the L1's parameters or, if ever needed, distributing workloads across additional application-specific L1s connected by interchain messaging.[150] Capacity planning and load targets are set with the business model (Volume VI).

---

[149] Avalanche "Etna" upgrade (Avalanche9000) — sovereign L1 model (ACP-77), Validator Manager, sub-second Snowman finality, interchain messaging; activated on mainnet 16 Dec 2024. Verified live: https://www.avax.network/about/blog/etna-enhancing-the-sovereignty-of-avalanche-l1-networks

[150] Avalanche "Etna" upgrade (Avalanche9000) — sovereign L1 model (ACP-77), Validator Manager, sub-second Snowman finality, interchain messaging; activated on mainnet 16 Dec 2024. Verified live: https://www.avax.network/about/blog/etna-enhancing-the-sovereignty-of-avalanche-l1-networks

CHAPTER 12 — TECHNOLOGY STACK, STANDARDS REGISTER & LIMITATIONS

12.1 Stack and versions (summary)

The following are the load-bearing technology choices and the versions verified on the date of documentation; the authoritative, link-bearing register is **Appendix A**.

Layer	Choice	Version / status (30 Jun 2026)
Token standard	ERC-3643 / T-REX	Final EIP; maintained by ERC-3643 Association
Identity	ONCHAINID (ERC-734/735, ERC-725)	In production use with T-REX
Contract library	OpenZeppelin Contracts	5.x line (current 5.6.1); UUPS in main package
Storage safety	ERC-7201 namespaced storage	Compiler builtin from Solidity 0.8.35
Language / compiler	Solidity	0.8.35 (pin recent 0.8.x; 0.9.0 breaking pending)
Chain	Permissioned Avalanche L1 (Subnet-EVM)	Post-Avalanche9000/Etna (mainnet 16 Dec 2024); AvalancheGo ≥ v1.12.0
Interoperability	ICM/Teleporter + cross-chain interoperability protocol	In production
Oracle	Decentralised oracle platform (feeds, NAV, proof-of-reserve, automation)	In production
PQC targets	NIST FIPS 203 / 204 / 205; HQC; FIPS 206	203/204/205 published 13 Aug 2024; HQC selected 11 Mar 2025; 206 in development
Account abstraction (option)	ERC-4337; EIP-7702 (Pectra)	EIP-7702 live since Pectra; OZ signer support

Table 8 — Technology stack & versions (summary).

12.2 What is settled vs. what is an option

Settled by this design: compliance-by-construction via ERC-3643; on-chain/off-chain data split; decentralised oracle layer with secure-mint for Model A; UUPS upgradeability with multisig+timelock and namespaced storage; crypto-agility with a PQC migration path; microservice off-chain platform. **Open options (label and decide with specialists before build):** the precise chain (recommended permissioned Avalanche L1 vs L2 fallback); the settlement asset (tokenised deposit vs regulated stablecoin vs escrowed traditional rails); confidential-token/ZK privacy depth; the oracle provider mix; and account-abstraction adoption.

12.3 Technical threats & limitations register (honest assessment)

#	Threat / limitation	Exposure	Mitigation / status
1	Smart-contract vulnerability (reentrancy, access control)	High	Multiple audits, formal verification, fuzzing, bug bounty (§10)
2	Upgrade-key / agent-key compromise	High	MPC/HSM, M-of-N multisig, timelock, monitoring (§7, §10)
3	Oracle manipulation / staleness	High	Decentralised feeds, thresholds, circuit breakers, fallback oracle (§5.3)
4	Validator-set compromise (permissioned L1)	Medium-High	Vetted PoA→PoS, HSM keys, distribution (§2.3, Vol. V)
5	Settlement-asset failure (stablecoin de-peg / bank default)	Medium-High	Proof-of-reserve, regulated asset, DvP, fallback rails (§9)
6	Key loss by investor	Medium	ERC-3643 recovery; account-abstraction recovery (§7)
7	Quantum threat to classical crypto (“harvest-now”)	Medium (rising)	Crypto-agility, hybrid, PQC migration (§8); on-chain PQC chain-dependent
8	Cross-chain bridge/message risk	Medium	Use defence-in-depth interop protocol; minimise bridged value (§2.3)
9	Data-protection breach (off-chain PII)	Medium	Encryption, isolation, no PII on-chain, erasure path (§1.4, Vol. I §9)
10	Vendor/standard deprecation (e.g. tooling sunsets)	Medium	Open-source/standards-based choices; version register (App. A)
11	Front-running / MEV on public interop	Low-Medium	Permissioned L1 mempool control; private settlement where needed
12	Regulatory change invalidating a control	Medium	Modular compliance, substance-over-form portability (§4.3)
13	Centralisation of agent powers (freeze/forced transfer)	Medium	Necessary for regulated assets; governed by multisig + audit trail (§3.1, §7)
14	Confidential-token / ZK immaturity	Medium	Treated as options with audit caveats, not defaults

#	Threat / limitation	Exposure	Mitigation / status
			(§8.2)
15	Finality assumptions wrong if chain changes	Low	Deterministic-finality chain; settlement only at finality (§11.2)

12.4 Honest limitations

This is an architecture, not an implementation: numbers such as throughput, latency, and cost are targets to be validated by load testing (Volume VI). Several choices are options pending specialist sign-off (§12.2). On-chain post-quantum protection depends on chain-level adoption the platform does not control. The agent powers that make a security lawful (freeze, forced transfer, recovery) also concentrate trust; the architecture mitigates but cannot eliminate this, and the governance around those powers is as important as the code. Finally, the security of the whole rests on dependencies — oracles, validators, custody, settlement assets — each of which is a managed risk, not a solved one.

INTERIM COMPLIANCE & COMPLETENESS AUDIT — VOLUME II

This interim audit records the volume’s self-check; the full cross-volume Compliance & Completeness Audit is run once after Volume VII and appended to every volume.

Verification performed. Every load-bearing technology version, standard status, and release date in this volume was checked against the vendor or standards body on 30 June 2026 and recorded in Appendix A and the Citation Register (Appendix D). Confirmed items include: ERC-3643 “Final” status and Association governance; OpenZeppelin Contracts 5.x (current 5.6.1) with UUPS in the main package; Solidity 0.8.35 and the ERC-7201 builtin; the Avalanche9000/Etna upgrade (mainnet 16 Dec 2024) and the sovereign-L1 (ACP-77) model; NIST FIPS 203/204/205 (13 Aug 2024), HQC selection (11 Mar 2025), and FIPS 206 in development; and the oracle proof-of-reserve / secure-mint capability.

No fabricated identifiers. No EIP number, FIPS number, ACP number, version string, or URL has been invented. Where an exact value could not be independently confirmed, it is stated generally and flagged, not guessed.

Open / flagged items for specialist sign-off. 1. Final chain selection (permissioned Avalanche L1 vs L2 fallback) — confirm with validator-operations plan (Vol. V) and counsel. 2. Settlement-asset selection and its regulatory treatment — confirm with treasury, banking partners, counsel (Vol. I §1.6). 3. Confidential-token / ZK privacy

depth — confirm maturity and audit posture before relying on it. 4. Exact pinned Solidity version and target EVM at build — re-check Appendix A; account for 0.9.0 deprecations. 5. Oracle provider mix and fallback quorum — confirm with the data/risk team. 6. On-chain PQC — track chain-level roadmap; off-chain PQC migration owned by Vol. V. 7. Throughput/latency/cost targets — to be validated by load testing (Vol. VI).

Link policy. Hyperlinks in this volume point only to official/primary sources verified live on 30 June 2026 (EIP registry, compiler and library release pages, NIST CSRC, the chain's official documentation). All other sources are cited by stable identifier (EIP/FIPS/ACP number, version string) without a hyperlink, to avoid link rot.

FUTURE JURISDICTION & TECHNOLOGY COMPATIBILITY NOTES

Jurisdiction portability. Because eligibility and offering rules are **data-driven compliance modules** (§4.3), supporting a new jurisdiction is a configuration-and-module exercise, not a re-architecture: map the jurisdiction's investor-eligibility and offering rules (from the relevant Volume I chapter) onto new or parameterised modules. The on-chain/off-chain split keeps data-protection compliance portable across regimes.

Technology watch items. (a) **Solidity 0.9.0** breaking release — track deprecations now (send/transfer, ABI coder v1, certain modifiers) to avoid a forced rewrite. (b) **Post-quantum** — adopt FIPS 203/204/205 off-chain on the CNSA-2.0 timeline; track the forthcoming FIPS 206 (FN-DSA) and HQC drafts; monitor chain-level PQC signature adoption for on-chain protection. (c) **Confidential / FHE tokens and ZK compliance** — maturing fast; revisit as defaults once audited and standardised. (d) **Account abstraction** (ERC-4337 / EIP-7702) — adopt for UX as wallet support broadens. (e) **Tooling sunset risk** — some hosted developer tools are being retired in favour of open-source equivalents; prefer open-source/standards-based dependencies (App. A). (f) **EU DLT Pilot Regime and MiCA evolution** (Vol. I) — keep the interop and settlement design ready for regulated-venue requirements.

GLOSSARY (TECHNICAL)

This glossary covers terms introduced in this volume; the master glossary is in Volume I. Canonical term reminder: the instrument is a **ledger-based security** implemented as an **ERC-3643 permissioned token**.

- **Account abstraction** — letting smart-contract logic control an account (ERC-4337) or delegating EOA behaviour to contract code (EIP-7702), enabling recovery, session keys, sponsored gas.
- **ACP** — Avalanche Community Proposal (e.g. ACP-77 “Reinventing Subnets”).
- **Avalanche L1 (formerly Subnet)** — a sovereign, application-specific chain with its own validator set and rules, the model introduced by the Avalanche9000/Etna upgrade.
- **C4 model** — a way to describe software architecture at four zoom levels: Context, Container, Component, Code.
- **CCIP** — a cross-chain interoperability protocol for transferring data and tokenised value across chains with compliance metadata.
- **Crypto-agility** — designing systems so cryptographic algorithms can be swapped via configuration, not rewrites.
- **DvP** — delivery-versus-payment: atomic settlement of the security leg against the cash leg.
- **EIP / ERC** — Ethereum Improvement Proposal / Ethereum Request for Comment (a standard).
- **ERC-3643 / T-REX** — the Final permissioned-token standard for regulated securities; “T-REX” is its reference implementation.
- **ERC-734 / ERC-735** — key-holder and claim-holder identity interfaces underpinning ONCHAINID.
- **ERC-7201** — namespaced storage layout standard preventing storage-collision bugs in upgradeable contracts.
- **FHE** — fully homomorphic encryption (computation on encrypted data); basis of emerging confidential-token work.
- **FIPS 203/204/205/206** — NIST post-quantum standards: ML-KEM, ML-DSA, SLH-DSA, and (in development) FN-DSA.
- **HNDL** — “harvest now, decrypt later”: capturing ciphertext today to decrypt once quantum computers exist.
- **HSM** — hardware security module (tamper-resistant key storage/operations), validated to FIPS 140-3.
- **ICM / Teleporter** — Avalanche Interchain Messaging for cross-chain communication within the ecosystem.
- **ML-KEM / ML-DSA / SLH-DSA** — module-lattice KEM and signatures, and stateless hash-based signatures (the NIST PQC algorithms).
- **MPC** — multi-party computation; here, splitting key control so no single party can sign alone.
- **NAV** — net asset value; the per-unit value of a fund/asset, delivered on-chain via oracle feeds.
- **ONCHAINID** — the on-chain identity contract holding keys and signed claim references (no PII).

- **Oracle / DON** — a service (decentralised oracle network) bringing off-chain truth on-chain.
- **Proof of Reserve / secure mint** — oracle-verified backing that gates token minting to prevent over-issuance.
- **Snowman consensus** — Avalanche's consensus giving sub-second deterministic finality.
- **STRIDE** — a threat-modelling taxonomy (spoofing, tampering, repudiation, info disclosure, DoS, elevation of privilege).
- **Subnet-EVM** — the EVM implementation used to run an EVM-compatible Avalanche L1.
- **UUPS** — Universal Upgradeable Proxy Standard; the upgradeable-contract pattern used here.
- **zk-SNARK / zk-STARK** — zero-knowledge proof systems that prove a statement without revealing its inputs.

APPENDIX A — STANDARDS & VERSIONS REGISTER

Authoritative register of load-bearing technologies. "Verified live 30 Jun 2026" means the official source page was retrieved on that date. Hyperlinks are given only to official sources verified live; other items are cited by stable identifier. Re-check versions before build.

#	Technology / standard	Identifier / version (30 Jun 2026)	Official source
A1	ERC-3643 (T-REX) security-token standard	Final EIP-3643; ERC-3643 Association	EIP registry — https://eips.ethereum.org/EIPS/eip-3643
A2	Solidity compiler	0.8.35 (0.9.0 breaking pending)	Release page — https://github.com/ethereum/solidity/releases
A3	OpenZeppelin Contracts	5.x (current 5.6.1); UUPS in main package	Release page — https://github.com/OpenZeppelin/openzeppelin-contracts/releases
A4	ERC-7201 namespaced storage	Compiler builtin from Solidity 0.8.35	(cited via Solidity release notes, A2)
A5	ONCHAINID / ERC-734 / ERC-735 / ERC-725	In production with T-REX	EIP registry (by number)
A6	Avalanche9000 / Etna upgrade; ACP-77 sovereign L1s	Mainnet 16 Dec 2024; AvalancheGo ≥ v1.12.0	Avalanche official blog — https://www.avax.network/about/blog/etna-enhancing-the-sovereignty-of-avalanche-

#	Technology / standard	Identifier / version (30 Jun 2026)	Official source
			l1-networks
A7	NIST PQC standardisation programme	FIPS 203/204/205 (13 Aug 2024); HQC selected 11 Mar 2025; FIPS 206 in development	NIST CSRC — https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization
A8	NIST FIPS 203/204/205 release	Published 13 Aug 2024	NIST — https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
A9	Account abstraction	ERC-4337; EIP-7702 (Ethereum Pectra)	EIP registry (by number)
A10	Confidential tokens (FHE) / ZK compliance	Emerging standardised work; option only	(by identifier; maturity-flagged)
A11	Oracle platform (feeds, NAV, proof-of-reserve, CCIP)	In production	Provider documentation (by name)
A12	DORA (EEA operational resilience)	Reg (EU) 2022/2554	EUR-Lex — https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

APPENDIX B — CONTRACT INTERFACE INVENTORY (INDICATIVE)

Indicative inventory of the on-chain contracts and their principal externally-visible functions/events; signatures to be fixed against the chosen T-REX release at build and audited.

Contract	Principal functions	Principal events
ERC-3643 Token	transfer, transferFrom, mint, burn, pause, freezePartialTokens, forcedTransfer, recoveryAddress, setCompliance, setIdentityRegistry	Transfer, Frozen, Paused, RecoverySuccess, ComplianceAdded
Identity Registry	registerIdentity, updateIdentity, deleteIdentity, isVerified	IdentityRegistered, IdentityRemoved
Identity Registry Storage	addIdentityToStorage, modifyStoredIdentity	IdentityStored, IdentityModified
Trusted Issuers Registry	addTrustedIssuer,	TrustedIssuerAdded,

Contract	Principal functions	Principal events
	removeTrustedIssuer	TrustedIssuerRemoved
Claim Topics Registry	addClaimTopic, removeClaimTopic	ClaimTopicAdded, ClaimTopicRemoved
Modular Compliance	addModule, removeModule, canTransfer	ModuleAdded, ModuleRemoved
ONCHAINID	addKey, removeKey, addClaim, removeClaim	KeyAdded, ClaimAdded, ClaimRemoved
Escrow / Drawdown (Model B)	subscribe, attestMilestone, releaseTranche, convert	Subscribed, MilestoneAttested, TrancheReleased
DvP / Settlement	lockCash, lockSecurity, settle, refund	LegLocked, Settled, Refunded

APPENDIX C — SERVICE CATALOGUE (OFF-CHAIN)

Cross-reference for Table 6; ownership, scaling, and data-classification per service is set in Volume V (operations) and Volume VI (capacity/cost).

Service	Primary API consumers	Scaling profile	Data classification
Onboarding & Identity	Investor app, admin	Spiky (campaigns)	Restricted (PII)
Issuance	Issuer app, admin	Low volume, high value	Confidential
Payments & Settlement	All flows	Steady + bursts	Confidential
Valuation / NAV	Reporting, marketplace	Scheduled + on-demand	Internal
Reporting & Regulatory	Operator, regulator (read)	Batch	Restricted
Marketplace / Trading API	Investor app (Vol. III)	High throughput	Internal
Document / Data-room	All parties	Read-heavy	Restricted
Notification	All services	High fan-out	Internal

APPENDIX D — CITATION REGISTER (TABLE — VOLUME II)

Every external source relied on in Volume II, with type and verification note. Official/primary sources are marked P; secondary/commentary (paraphrased only) S.

Ref	Source	Type	Used for	Verification note
erc3643eip	EIP-3643 (Ethereum EIP registry)	P	Standard status, semantics, roles	Verified live 30 Jun 2026

Ref	Source	Type	Used for	Verification note
erc3643	ERC-3643 Association / T-REX materials	P/S	Association governance; suite design; recovery; identity	Paraphrased; standard verified via EIP
sol	Solidity release notes (0.8.35; 0.9.0 pending; erc7201 builtin)	P	Compiler version, ERC-7201, deprecations	Verified live (release page)
oz	OpenZeppelin Contracts release notes (5.x / 5.6.1)	P	UUPS location, version, EIP-7702 signer	Verified live (release page)
etna	Avalanche Etna / ACP-77 (official blog & docs)	P	Sovereign L1 model, validator manager, finality, interop	Verified live (official blog)
acp77	Avalanche Community Proposal 77	P	Subnet→L1 mechanics	Cited by identifier
nistpqc	NIST PQC standardisation programme (CSRC)	P	FIPS 203/204/205; HQC selection; FIPS 206 status; timelines	Verified live (NIST CSRC)
nistfips	NIST news — FIPS 203/204/205 release	P	13 Aug 2024 publication	Verified live (NIST)
clpor	Oracle platform documentation (proof-of-reserve, NAV, CCIP)	P/S	Secure mint, NAV, DvP, interop precedents	Paraphrased; provider primary docs
ccip	Cross-chain interoperability protocol documentation	P/S	Interop and compliance-metadata transport	Paraphrased

APPENDIX E — CROSS-REFERENCE INDEX

Topic	This volume	Other volumes
Token = ledger-based security	§1.1, §3.1	Vol. I §1, §4.1
Eligibility / compliance rules	§4.3	Vol. I §3.5, §4.2, Ch. 5–7
Segregation / bankruptcy remoteness	§7	Vol. I §4.6
Data-protection split	§1.4, §4.2	Vol. I §9
Settlement-asset classification	§9	Vol. I §1.6

Topic	This volume	Other volumes
DORA / operational resilience	§10	Vol. I §1.5, §10
Custody / key ceremonies (depth)	§7	Vol. V
Valuation / NAV / models	§5	Vol. IV
Marketplace / trading	§3.2, §6.2	Vol. III
Tokenomics / cost / capacity	§12	Vol. VI
All diagrams consolidated	—	Vol. VII

DIAGRAM INVENTORY (Volume II)

Fig.	Title	Mermaid type	Section
1	System context (C4 L1)	flowchart	1.3
2	Container view (C4 L2)	flowchart	1.3
3	On-chain / off-chain split	flowchart	1.4
4	Network topology — permissioned Avalanche L1 & interop	flowchart	2.3
5	Chain-choice decision tree	flowchart	2.2
6	ERC-3643 / T-REX contract suite	flowchart	3.1
7	Compliant-transfer sequence	sequenceDiagram	3.2
8	Dual-mode funding contracts	flowchart	3.3
9	Forward-funding escrow & drawdown sequence	sequenceDiagram	3.3
10	UUPS upgrade flow	flowchart	3.4
11	Identity & claim-issuance flow	sequenceDiagram	4.2
12	Oracle & data-layer dataflow	flowchart	5.2
13	Off-chain microservices container diagram	flowchart	6.2
14	End-to-end subscription sequence	sequenceDiagram	6.3
15	Crypto-agility & PQC layering	flowchart	8.3

Fig.	Title	Mermaid type	Section
16	Delivery-versus-payment sequence	sequenceDiagram	9.2
17	CI/CD with security gates	flowchart	10.2

Diagram-type palette: flowchart, sequenceDiagram. Volume VII consolidates all diagrams across volumes and adds C4 component/code and ER/class views.

END OF VOLUME II (interim draft)

Next: Volume III — Marketplace & Trading. Before final delivery of the package, all seven volumes undergo a single cross-volume Compliance & Completeness Audit; forward references are resolved; versions in Appendix A are re-checked; and the package is compiled to `.docx` on explicit request.

VOLUME III — MARKETPLACE & TRADING

Institutional Digital Real Estate Capital Markets Infrastructure

Multi-Volume Documentation Package — Volume III of VII

TITLE PAGE & DOCUMENT CONTROL

Field	Detail
Document	Volume III — Marketplace & Trading
Package	Institutional Digital Real Estate Capital Markets Infrastructure (7 volumes)

Field	Detail
Status	Working draft for internal review and legal/market-structure sign-off — **not a venue rulebook or trading-system specification in this form**
Version	III-0.1 (interim; full cross-volume Compliance & Completeness Audit pending completion of Volume VII)
Date of documentation	30 June 2026
Classification	Confidential — Draft
Companion volumes	Vol. I (legal/regulatory), Vol. II (technical architecture)

Authorship and reliance caveat (read first). This volume is an AI-assisted design document prepared to institutional standards of rigour. Venue regimes, regulatory thresholds, authorisations, and market developments cited here were checked against official or primary sources **as of 30 June 2026** and footnoted. It remains a draft and **must be reviewed by qualified securities, market-infrastructure, and trading-systems counsel and specialists before any reliance, application for a venue permission, or build.** Trading-venue authorisation is jurisdiction-specific and fact-sensitive; nothing here is legal advice or a representation that any particular permission will be granted. Where a market-design choice is open it is presented as a labelled **option with trade-offs**.

On "latest releases." The regulated-venue landscape for tokenised securities is moving quickly. Every load-bearing regime status, threshold, and authorisation in this volume was re-verified against the regulator or primary source on the date of documentation and recorded in **Appendix A — Venue & Regulatory Register**; it must be re-checked before any application or build.

HOW TO READ THIS VOLUME (CONTROL FILE)

Condensed Control File, reproduced atop every volume after Volume I.

Canonical terms (do not substitute synonyms). The instrument is a **ledger-based security** (Swiss CO Art. 973d; Vol. I §4.1) implemented as an **ERC-3643 permissioned token** (Vol. II §3). "Primary market" = issuance/distribution to first holders; "secondary market" = subsequent investor-to-investor trading. "The platform" denotes the infrastructure as a whole; a **trading venue** is the specific regulated facility on which secondary trading occurs. "DvP" = delivery-versus-payment (Vol. II §9).

Cross-volume reference map.

Volume	Scope	Relationship to this volume
I	Executive & Regulatory	Supplies the eligibility, prospectus, market-conduct and per-jurisdiction

Volume	Scope	Relationship to this volume
		rules enforced at the point of trade
II	Technical Architecture	Supplies the contract, settlement (DvP) and compliance machinery this volume drives
III	**Marketplace & Trading (this volume)**	**Market structure, venue strategy, order lifecycle, settlement, surveillance**
IV	Financial Intelligence	Supplies valuation/NAV and analytics consumed by pricing and surveillance here
V	Security & Operations	Operational resilience, custody and key controls behind the venue
VI	Business & Financial Model	Fee model and volumes reference this volume's market design
VII	Architecture Atlas	Consolidates this volume's diagrams

Cross-volume items resolved in this volume. Volume I flagged two Swiss provisions for confirmation; research for this volume confirms them: the **DLT trading facility** licence sits at **FMIA (FinfraG) Art. 73a et seqq.** (with FinMIO Art. 58a et seqq.), and **segregation of crypto-based assets in bankruptcy** sits at **DEBA Art. 242a**. These are carried into the final cross-volume audit.

Rule set (unchanged). No fabricated facts or citations; venue statuses and thresholds verified against primary sources and registered in Appendix A; design options labelled with trade-offs; commentary paraphrased; hyperlinks only to official sources verified live on the date of documentation, all other sources cited by name/identifier.

DETAILED TABLE OF CONTENTS

- Market Structure & Design Principles
- Regulated Venue Strategy (Multi-Jurisdiction)
- Trading Models — Order Book, RFQ, AMM
- Order Lifecycle & Matching
- Settlement & Clearing
- Liquidity
- Market Integrity & Surveillance
- Investor Protection & Conduct at the Point of Trade
- Secondary-Market Compliance Enforcement
- Fees, Market Data & Connectivity
- Competitive Landscape & Benchmarks

- Limitations & Threats Register
35. Interim Compliance & Completeness Audit (Volume III)
36. Future Jurisdiction & Technology Compatibility Notes
37. Glossary
38. Appendices A–E
39. Diagram Inventory

LIST OF FIGURES

Figure	Title	Section
1	Asset lifecycle: primary → secondary → corporate actions	1.2
2	Market-structure overview (participants & venue)	1.3
3	Venue-strategy decision tree	2.2
4	Multi-jurisdiction venue map	2.3
5	Trading-model comparison (CLOB / RFQ / AMM)	3.2
6	Hybrid off-chain matching, on-chain settlement	3.3
7	Order lifecycle with pre-trade compliance	4.2
8	Matching-engine architecture	4.3
9	Atomic DvP settlement sequence	5.2
10	Failed-trade / settlement-exception handling	5.3
11	Liquidity sources & provision	6.2
12	Market-surveillance architecture	7.3
13	Point-of-trade conduct & suitability flow	8.2
14	Secondary-transfer compliance enforcement	9.2
15	Participant connectivity & onboarding	10.3

LIST OF TABLES

Table	Title	Section
1	Market-design principles → mechanisms	1.4
2	Regulated-venue regimes compared	2.2
3	Trading models & suitability	3.2
4	Order types supported	4.1
5	Settlement options & trade-offs	5.1
6	Market-abuse behaviours & surveillance controls	7.2
7	Point-of-trade conduct obligations by regime	8.3
8	Competitive benchmarks (venues & platforms)	11.1
9	Marketplace threats & limitations register	12.1

EXECUTIVE SUMMARY

A tokenised security is only as useful as the market it can trade in. This volume specifies how the platform supports the **primary** distribution and **secondary** trading of the ledger-based securities defined in Volume I and implemented in Volume II — under one constraint inherited from both: **every trade is a compliant transfer.** The marketplace does not bolt compliance onto trading; it inherits the ERC-3643 enforcement layer so that an ineligible buyer simply cannot take delivery, and settlement is delivery-versus-payment so neither side bears principal risk.

Four decisions shape the volume. **First, venue strategy.** Trading regulated securities requires a regulated venue, and the regimes purpose-built for DLT securities differ by jurisdiction. The platform's primary path follows Switzerland's **DLT trading facility** licence (FMIA Art. 73a et seqq.) — the regime under which the first such facility was authorised in 2025[151] — with the EU **DLT Pilot Regime** (DLT MTF/SS/TSS, Regulation (EU) 2022/858, then under ESMA's Article 14 review)[152][153] and the UK **Digital**

[151] FINMA — authorisation of the first DLT trading facility (operated by BX Digital), settlement on a public blockchain with the cash leg via the Swiss Interbank Clearing system; regime at FMIA (FinfraG) Art. 73a et seqq. and FinMIO Art. 58a et seqq.; "small facility" thresholds; segregation of crypto-based assets at DEBA Art. 242a. Verified live 30 Jun 2026: https://www.finma.ch/en/news/2025/03/20250318-mm-dlt-handelssystem/

Securities Sandbox (running to January 2029)[154] as the principal alternatives, and the fast-moving US position (the SEC's January 2026 staff statement that tokenisation does not change a security's classification, plus a proposed "innovation exemption")[155] tracked as a watch item. **Second, trading model.** Because real-estate-backed securities are relatively illiquid, the design favours a **request-for-quote (RFQ) and periodic-auction** model alongside an optional central limit order book, with **off-chain matching and on-chain atomic settlement** rather than a fully on-chain order book. **Third, integrity.** The venue runs pre-trade eligibility checks, trade surveillance for market abuse, transaction reporting, and best-execution and suitability controls mapped to each jurisdiction's regime. **Fourth, honesty about liquidity.** Tokenisation does not by itself create liquidity; the volume treats the cold-start problem directly rather than assuming it away.

The chapters develop market structure and principles; the multi-jurisdiction venue strategy; trading models and the matching engine; the order lifecycle with pre-trade compliance; settlement and failed-trade handling; liquidity; market integrity and surveillance; point-of-trade conduct and investor protection; secondary-market compliance enforcement; fees, data and connectivity; a benchmarked competitive landscape; and an honest threats register. Open items and limitations are gathered in the Interim Audit and §12.

---

[152] EUR-Lex — Regulation (EU) 2022/858 (DLT Pilot Regime): DLT MTF/SS/TSS; €6bn admission cap and €9bn transition trigger; applicable 23 March 2023. Verified live: https://eur-lex.europa.eu/eli/reg/2022/858/oj/eng

[153] ESMA — report on the functioning and review of the DLT Pilot Regime under Article 14 (June 2025), recommending revisiting the regime's caps and constraints. Verified live: https://www.esma.europa.eu/sites/default/files/2025-06/ESMA75-117376770-460_Report_on_the_functioning_and_review_of_the_DLTR_-_Art.14.pdf

[154] UK Digital Securities Sandbox — joint Bank of England / FCA FMI sandbox; notary/maintenance/settlement (DSD) optionally combined with a trading venue; open since September 2024; runs to 8 January 2029 (extendable by HM Treasury). Verified live: https://www.fca.org.uk/firms/innovation/digital-securities-sandbox and https://www.bankofengland.co.uk/financial-stability/digital-securities-sandbox

[155] SEC — staff statement on tokenised securities (January 2026): tokenising a security does not change its regulatory classification; federal securities laws apply by economic substance. A proposed "innovation exemption" for on-chain trading of tokenised securities was, as of 30 June 2026, proposed and in flux. Verified live: https://www.sec.gov/newsroom/speeches-statements/corp-fin-statement-tokenized-securities-012826-statement-tokenized-securities

CHAPTER 1 — MARKET STRUCTURE & DESIGN PRINCIPLES

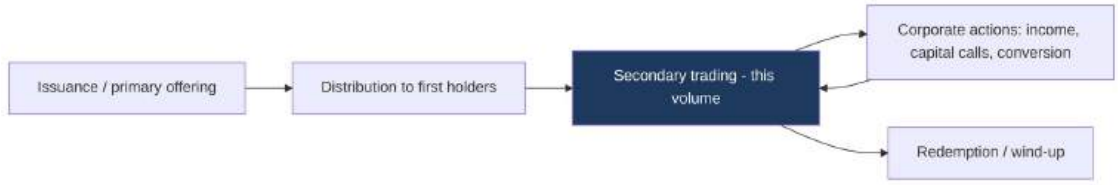
1.1 What “marketplace” means for a permissioned security

For an ordinary crypto-asset, a “marketplace” is an exchange where anyone can trade. For a **security**, trading is a regulated activity that must occur on, or through, an appropriately authorised venue, between eligible parties, with disclosure, conduct, settlement-finality and market-integrity obligations attached. The platform’s marketplace is therefore not a permissionless exchange; it is a **regulated trading and settlement environment** in which the ERC-3643 token’s eligibility logic (Vol. II §3–4) is the same logic that gates who may trade. The design question is not “how do we let everyone trade” but “how do we let *eligible* parties trade *efficiently and fairly* while the register, the compliance layer, and the settlement asset do their jobs.”

1.2 The asset lifecycle

Trading sits inside a longer lifecycle: an instrument is issued (primary market), distributed to first holders, traded among eligible investors (secondary market), subjected to corporate actions (distributions, capital calls, conversions — Vol. I Ch. 3, Vol. II §3.3), and eventually redeemed or wound up. The marketplace must serve the secondary phase without breaking the controls established at issuance.

Figure 1 — Asset lifecycle: primary, secondary and corporate actions.

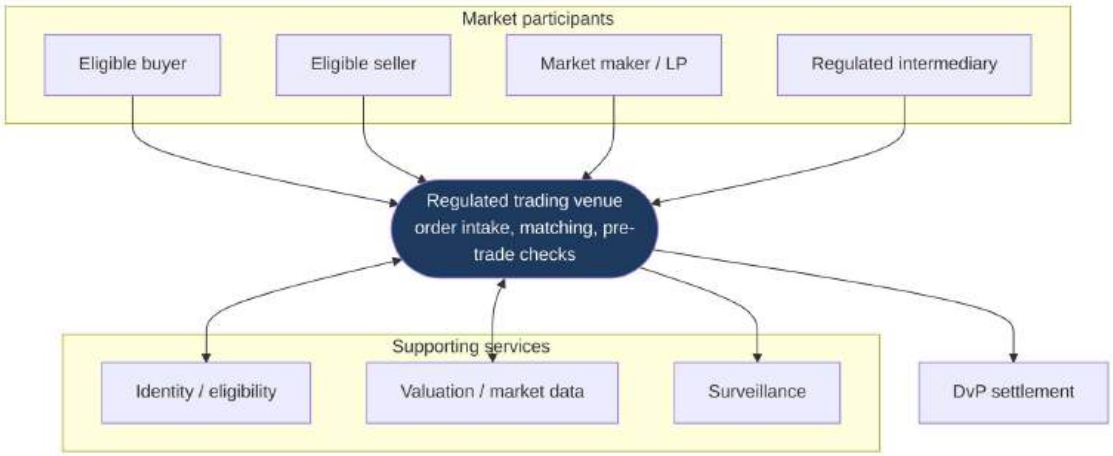


The marketplace owns the secondary-trading phase but must preserve the eligibility, disclosure and segregation controls set at issuance and honour corporate actions throughout the asset’s life.

1.3 Participants and the venue

The market connects **eligible investors** (buyers and sellers), **issuers/sponsors**, **market makers / liquidity providers**, **regulated intermediaries** (where the venue is participant-only), and the **operator** of the venue, around a regulated **trading venue** and a **settlement** mechanism, with **identity/eligibility**, **valuation/market-data**, and **surveillance** services alongside.

Figure 2 — Market-structure overview (participants and venue).



Whether investors access the venue directly or through regulated intermediaries is a venue-design and jurisdiction question (§2); in either case the venue performs pre-trade eligibility checks and feeds a surveillance function.

1.4 Design principles

Principle	Mechanism in this volume	Reference
Every trade is a compliant transfer	ERC-3643 eligibility checked pre-trade and at settlement	§4.2, §9; Vol. II §3–4
No principal risk in settlement	Atomic delivery-versus-payment	§5; Vol. II §9
Fair and orderly market	Transparent rules, surveillance, controls against abuse	§7
Best execution & investor protection	Suitability/appropriateness, disclosures, conduct rules	§8
Appropriate venue authorisation	Operate under / list on a regime built for DLT securities	§2
Liquidity realism	RFQ/auction models; market-maker programmes; honest cold-start treatment	§3, §6
Transparency & reportability	Trade/transaction reporting; on-chain auditability	§7
Portability across jurisdictions	Venue-agnostic compliance layer; modular rules	§2, §9

Table 1 — Market-design principles → mechanisms. The first two principles are the non-negotiable inheritance from Volumes I and II: a marketplace that allowed an ineligible transfer, or exposed a party to principal risk at settlement, would defeat the legal and technical architecture.

CHAPTER 2 — REGULATED VENUE STRATEGY (MULTI-JURISDICTION)

2.1 Why venue choice is a first-order decision

Secondary trading of securities on a DLT must occur within a regime that recognises both the *security* and its *DLT form*. Several jurisdictions have built such regimes, and they differ materially in structure, scope, caps, and maturity. The platform's venue strategy must (a) match its primary jurisdiction (Switzerland; Vol. I), (b) provide credible routes for cross-border investors, and (c) avoid building to a regime that is capacity-capped or time-limited in a way that strands the investment.

2.2 The venue regimes compared

Regime / jurisdiction	Instrument	Structure	Key constraints	Status (30 Jun 2026)
Swiss DLT trading facility (FMIA Art. 73a et seqq.)	DLT securities (ledger-based securities)	Combined multilateral trading **and** settlement on one infrastructure; atomic DvP	"Small" facility thresholds (reduced supervision); participant-only	First facility authorised 2025; primary path[156]
EU DLT Pilot Regime (Reg (EU) 2022/858)	DLT financial instruments (MiFID II)	DLT MTF, DLT SS, DLT TSS (TSS combines trading+settlement)	€6bn cap at admission; transition strategy at €9bn; limited instrument scope	Live since Mar 2023; under ESMA Art. 14 review (recommend raising cap)[157][158]

[156] FINMA — authorisation of the first DLT trading facility (operated by BX Digital), settlement on a public blockchain with the cash leg via the Swiss Interbank Clearing system; regime at FMIA (FinfraG) Art. 73a et seqq. and FinMIO Art. 58a et seqq.; "small facility" thresholds; segregation of crypto-based assets at DEBA Art. 242a. Verified live 30 Jun 2026: https://www.finma.ch/en/news/2025/03/20250318-mm-dlt-handelssystem/

[157] EUR-Lex — Regulation (EU) 2022/858 (DLT Pilot Regime): DLT MTF/SS/TSS; €6bn admission cap and €9bn transition trigger; applicable 23 March 2023. Verified live: https://eur-lex.europa.eu/eli/reg/2022/858/oj/eng

[158] ESMA — report on the functioning and review of the DLT Pilot Regime under Article 14 (June 2025), recommending revisiting the regime's caps and constraints. Verified live: https://www.esma.europa.eu/sites/default/files/2025-06/ESMA75-117376770-460_Report_on_the_functioning_and_review_of_the_DLTR_-_Art.14.pdf

Regime / jurisdiction	Instrument	Structure	Key constraints	Status (30 Jun 2026)
UK Digital Securities Sandbox	Digital securities (FMI sandbox)	Notary/ maintenance/ settlement (DSD) ± trading venue	Gated scaling (Gates 1–4); sandbox limits; UK-established firms	Open since Sep 2024; runs to 8 Jan 2029[159]
Singapore / Hong Kong (Vol. I §6)	Tokenised capital-markets products	Existing CMP/securities venue regimes + pilots	Per-regime licensing	Per Vol. I; pilots ongoing
United States	Tokenised securities	Existing exchange/ATS + proposed "innovation exemption"	Substance-over-form (tokenisation ≠ reclassification)	SEC Jan 2026 staff statement; innovation exemption proposed/in flux[160]

Table 2 — Regulated-venue regimes compared. Two structural points matter. First, the Swiss DLT trading facility and the EU **DLT TSS** are notable for permitting **trading and settlement on one infrastructure** — impossible under traditional market-structure rules without exemptions — which enables atomic DvP and a compressed trade-to-settlement cycle. Second, the EU regime's **€6bn admission cap (transition at €9bn)** is a real constraint that ESMA's Article 14 review recommended revisiting; building primary capacity to a capped regime is a flagged risk (§12).[161][162]

Figure 3 — Venue-strategy decision tree.

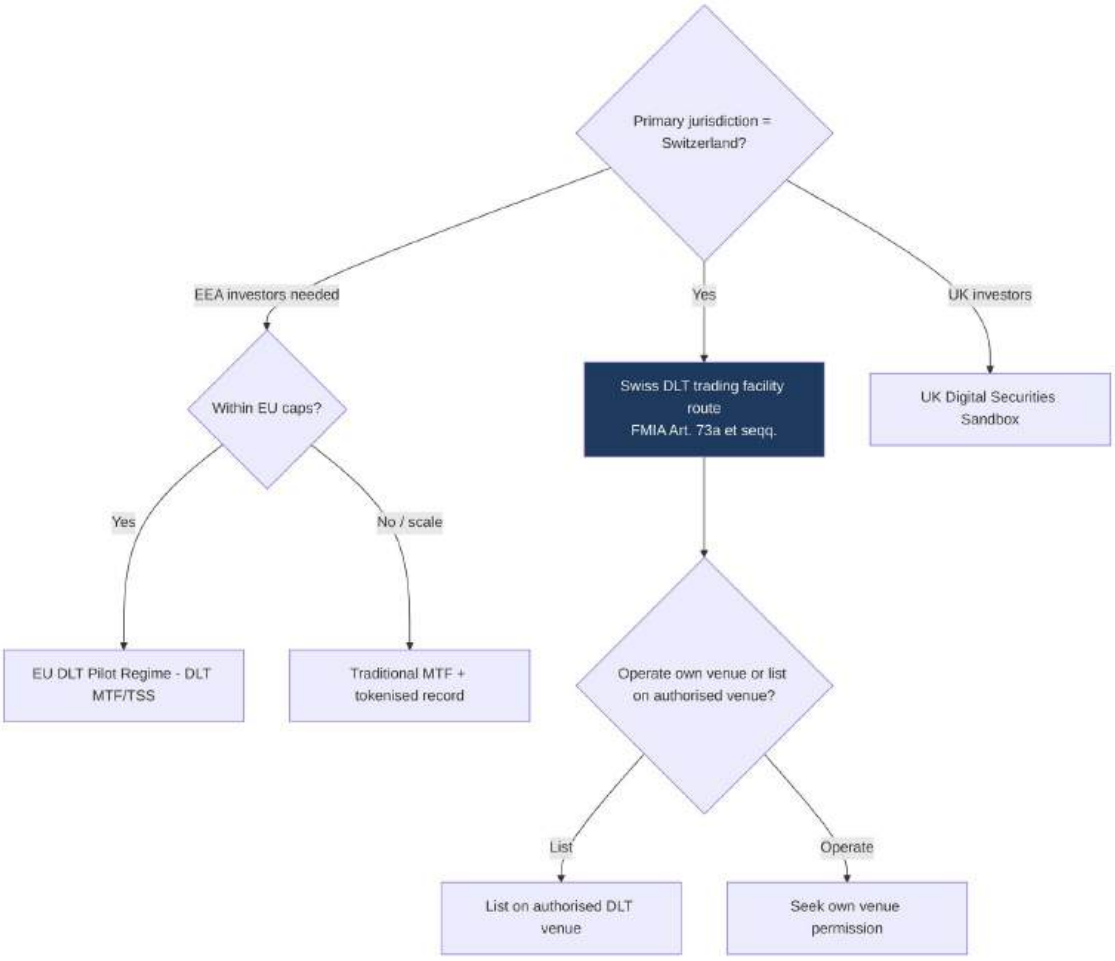
---

[159] UK Digital Securities Sandbox — joint Bank of England / FCA FMI sandbox; notary/maintenance/settlement (DSD) optionally combined with a trading venue; open since September 2024; runs to 8 January 2029 (extendable by HM Treasury). Verified live: https://www.fca.org.uk/firms/innovation/digital-securities-sandbox and https://www.bankofengland.co.uk/financial-stability/digital-securities-sandbox

[160] SEC — staff statement on tokenised securities (January 2026): tokenising a security does not change its regulatory classification; federal securities laws apply by economic substance. A proposed "innovation exemption" for on-chain trading of tokenised securities was, as of 30 June 2026, proposed and in flux. Verified live: https://www.sec.gov/newsroom/speeches-statements/corp-fin-statement-tokenized-securities-012826-statement-tokenized-securities

[161] EUR-Lex — Regulation (EU) 2022/858 (DLT Pilot Regime): DLT MTF/SS/TSS; €6bn admission cap and €9bn transition trigger; applicable 23 March 2023. Verified live: https://eur-lex.europa.eu/eli/reg/2022/858/oj/eng

[162] ESMA — report on the functioning and review of the DLT Pilot Regime under Article 14 (June 2025), recommending revisiting the regime's caps and constraints. Verified live: https://www.esma.europa.eu/sites/default/files/2025-06/ESMA75-117376770-460_Report_on_the_functioning_and_review_of_the_DLTR_-_Art.14.pdf

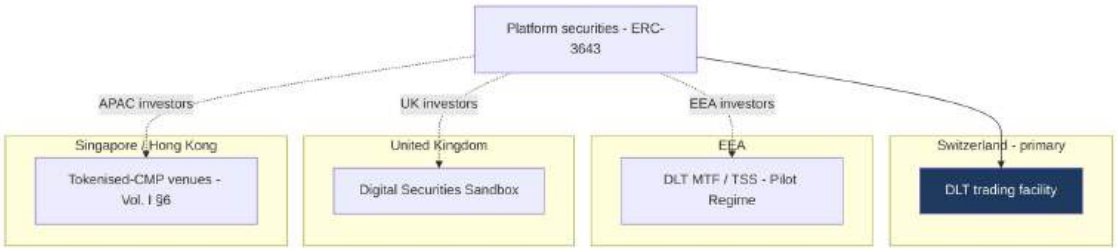


The decision is jurisdiction-first, then "operate vs list." For a new entrant, listing on an already-authorised DLT venue is faster and lower-risk than seeking a venue permission; operating a venue is a later-stage option requiring its own authorisation and Volume V operational readiness.

2.3 Operate vs list, and the multi-jurisdiction map

Design option — operate vs list (trade-offs). *Listing* the platform's securities on an already-authorised DLT trading facility (e.g. a Swiss DLT trading facility, or an EU DLT MTF/TSS) gives immediate, credible secondary trading without the platform assuming venue-operator obligations; the trade-off is dependence on a third party's rulebook, fees, and roadmap. *Operating* a venue gives control and captures more of the value chain but requires a venue authorisation, market-surveillance and conduct functions, and the operational resilience of Volume V; it is a multi-year regulatory undertaking. The recommended sequence is **list first, operate later** — begin by admitting the platform's securities to an authorised DLT venue, and consider a proprietary venue only once volumes and capabilities justify it. **This must be confirmed with market-infrastructure counsel.**

Figure 4 — Multi-jurisdiction venue map.



The platform's securities can be admitted to venues across jurisdictions, with the same on-chain compliance layer enforcing each venue's and each jurisdiction's eligibility rules (§9). Cross-venue interoperability uses the messaging/interoperability layer of Vol. II §2.3.

2.4 The US watch item

The United States is a fast-moving watch jurisdiction rather than a launch market for the platform. The conservative anchor is the SEC staff's **January 2026 statement that tokenising a security does not change its regulatory classification** — federal securities laws continue to apply by economic substance, exactly the substance-over-form principle on which Volumes I–II rest.[163] A proposed **"innovation exemption"** would create a time-limited, guardrailed path for on-chain trading of tokenised securities (with whitelisting and compliance-aware token standards), but as of the date of documentation it is **proposed and in flux**, not settled, and is treated as such here. Parallel developments — exchange-level tokenised trading and a central-depository tokenisation pilot — are noted in §11 as benchmarks, not as a regime the platform relies on.

CHAPTER 3 — TRADING MODELS: ORDER BOOK, RFQ, AMM

3.1 Matching the model to the asset

Real-estate-backed securities are **relatively illiquid, lumpy, and infrequently traded** compared with listed equities or stablecoins. The trading model must fit that reality. A

[163] SEC — staff statement on tokenised securities (January 2026): tokenising a security does not change its regulatory classification; federal securities laws apply by economic substance. A proposed "innovation exemption" for on-chain trading of tokenised securities was, as of 30 June 2026, proposed and in flux. Verified live: https://www.sec.gov/newsroom/speeches-statements/corp-fin-statement-tokenized-securities-012826-statement-tokenized-securities

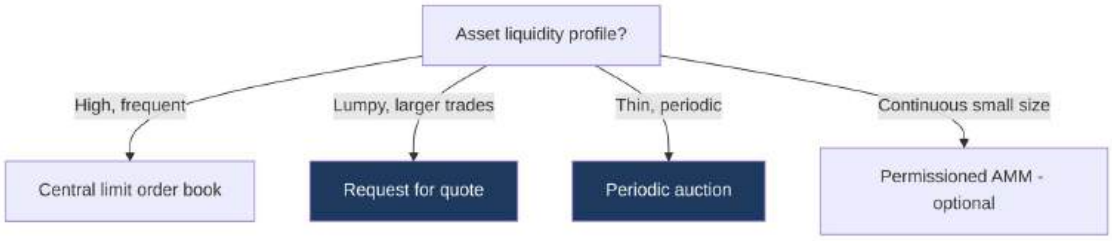
continuous central limit order book (CLOB) presupposes a steady two-sided flow that thinly-traded RWAs rarely have; a request-for-quote (RFQ) or periodic-auction model concentrates liquidity at points in time and is better suited to larger, less frequent trades. An automated market maker (AMM) provides continuous on-chain liquidity but, in a permissioned-securities context, must be a **compliance-gated** ("permissioned") AMM and carries impermanent-loss and pricing-quality issues for assets without a deep reference market.

3.2 The three models compared

Model	How it works	Best for	Cautions
Central limit order book (CLOB)	Continuous bids/asks matched by price-time priority	Liquid, frequently traded instruments	Needs steady two-sided flow; thin books → poor execution
Request for quote (RFQ)	Buyer requests quotes from market makers; bilateral execution	Larger, less frequent RWA trades	Less pre-trade transparency; relationship-dependent
Periodic auction	Orders collected and matched at intervals (call auction)	Illiquid assets; fair price formation	No continuous trading; timing risk
Permissioned AMM	On-chain pool prices trades algorithmically; transfers gated	Continuous small-size liquidity	Impermanent loss; pricing without deep reference market; needs compliant LPs

Table 3 — Trading models and suitability. **Design recommendation (option):** lead with **RFQ + periodic auctions** for the platform's securities, offering a **CLOB** only where an instrument develops enough flow to support one, and treating a **permissioned AMM** as an optional supplementary liquidity source rather than the primary mechanism. The mix is a per-instrument decision driven by expected liquidity (§6).

Figure 5 — Trading-model comparison.



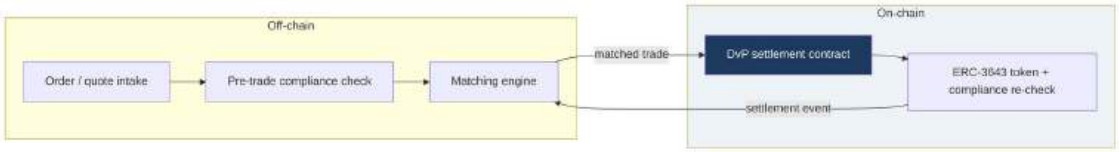
Most real-estate-backed securities sit in the middle two buckets, which is why RFQ and periodic auctions lead the design; CLOB and AMM are situational.

3.3 Off-chain matching, on-chain settlement

Regardless of model, the architecture separates **matching** from **settlement**. Matching (order intake, price formation, quote negotiation) happens **off-chain** in a performant

matching engine; **settlement** of the matched trade happens **on-chain** via atomic DvP (§5). This is the prevailing institutional pattern: it keeps the high-throughput, latency-sensitive matching off the chain while preserving on-chain finality, auditability, and atomic settlement for the value transfer. Pre-trade compliance checks run at order time off-chain, and the on-chain settlement re-checks eligibility so the chain remains the source of truth.

Figure 6 — Hybrid off-chain matching, on-chain settlement.



Matching is fast and off-chain; settlement is atomic and on-chain. Eligibility is checked twice — at order time for good UX, and at settlement because the chain is authoritative.

CHAPTER 4 — ORDER LIFECYCLE & MATCHING

4.1 Order types

The venue supports a pragmatic set of order types suited to RWA trading rather than the full high-frequency-trading menu: **market**, **limit**, **RFQ (quote request/response)**, **auction (call)**, and administrative types such as **good-till-time** and **all-or-none**. Each order carries the submitting party's identity so that eligibility can be checked before the order ever rests on the book or enters an auction.

Order type	Use
Limit	Rest a bid/ask at a price; price-time priority
Market	Execute immediately at best available (with protections)
RFQ	Request quotes from market makers; accept/decline
Auction (call)	Participate in a periodic price-forming auction
Good-till-time / All-or-none	Time and quantity constraints

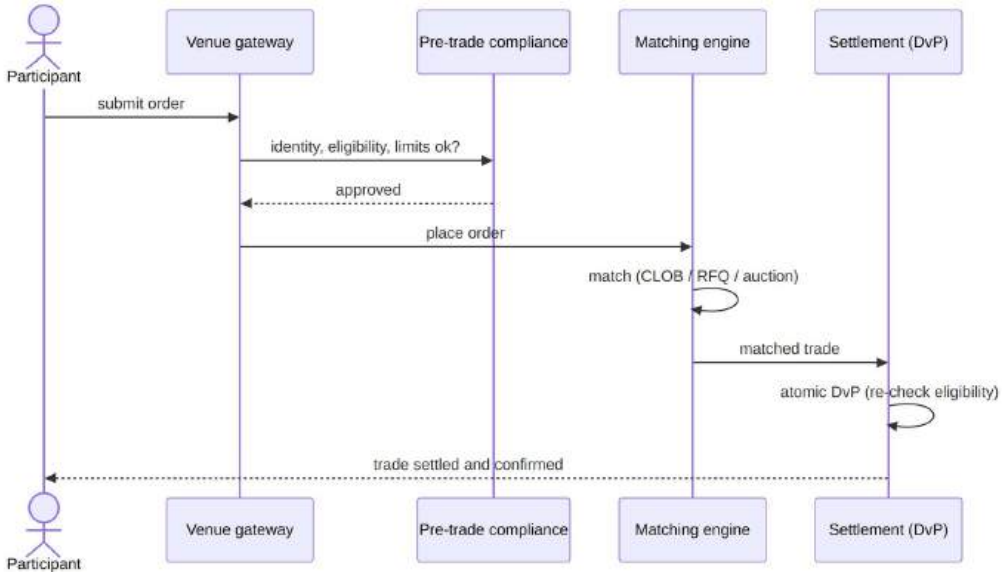
Table 4 — Order types supported.

4.2 The order lifecycle with pre-trade compliance

An order's life: submitted → identity/eligibility checked → risk/limit checked → placed (book/auction/RFQ) → matched → sent to settlement → settled on-chain (atomic DvP)

→ confirmed. Crucially, **eligibility is checked before an order can execute**, so an ineligible party cannot even create a binding match.

Figure 7 — Order lifecycle with pre-trade compliance.

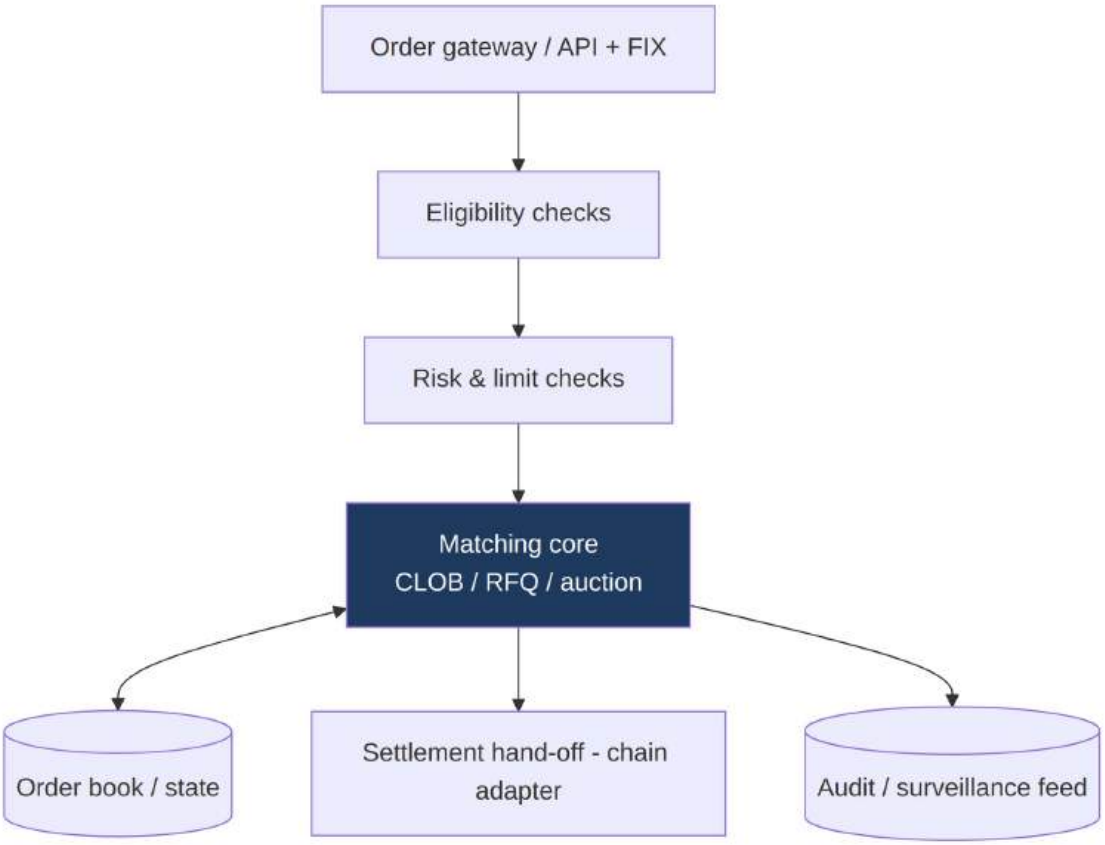


Compliance is a gate at the front of the order lifecycle, not a check after the fact; settlement re-validates because the chain is authoritative.

4.3 Matching-engine architecture

The matching engine is an off-chain, high-availability service (Vol. II §6, §11) with deterministic matching logic (price-time priority for CLOB; quote selection for RFQ; uniform-price clearing for auctions), an order store, a risk/limit module, and a settlement hand-off to the on-chain DvP contract via the chain adapter. It emits an immutable audit trail consumed by surveillance (§7).

Figure 8 — Matching-engine architecture.



The matching core is deterministic and auditable; eligibility and risk gate the path in; settlement is handed off to the on-chain DvP contract; every event feeds surveillance.

CHAPTER 5 — SETTLEMENT & CLEARING

5.1 The settlement question

Settlement converts a matched trade into a final exchange of the security for cash. The two design questions are **when** (settlement cycle) and **how** (settlement asset and mechanism). DLT enables something traditional markets cannot do without exemptions: **trading and settlement on the same infrastructure**, allowing settlement to compress from T+1/T+2 to **atomic (T+0)** — the security and cash change hands in a single, indivisible step.

Option	Cycle	Pros	Cons
Atomic DvP (T+0)	Instant, on-chain	No principal/settlement risk; no failed trades by construction; capital	Requires both legs on-ledger and pre-funded; liquidity/funding discipline

Option	Cycle	Pros	Cons
		efficiency	
Deferred net settlement (T+1)	End-of-cycle netting	Familiar; netting reduces gross flows	Reintroduces settlement risk; needs a clearing/guarantee layer
Off-ledger cash, on-ledger security	Coordinated	Works with traditional banking	Needs escrow/hash-lock; not truly atomic; reconciliation burden

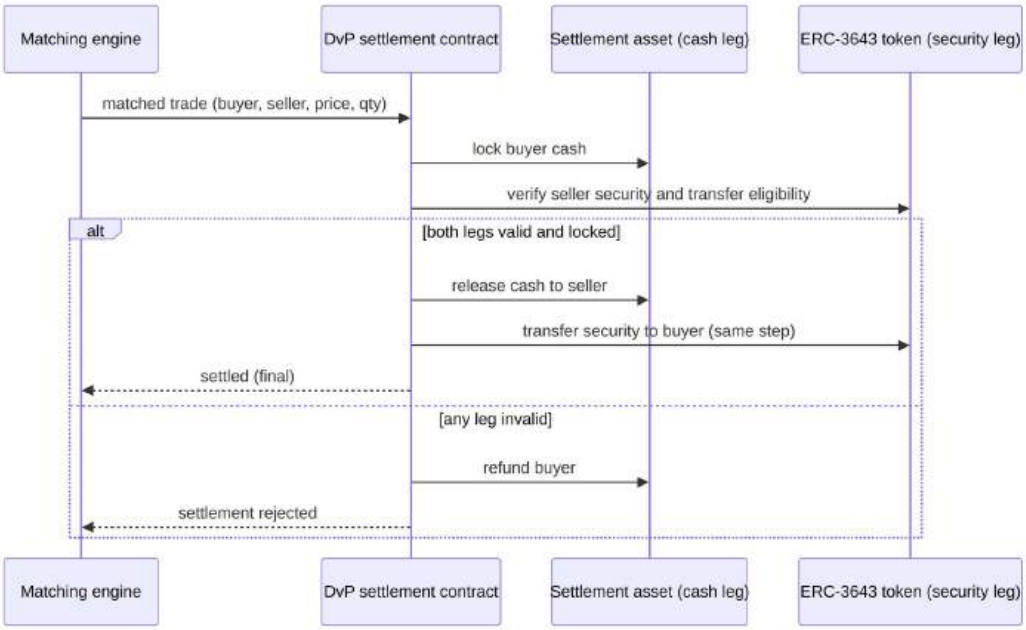
Table 5 — Settlement options and trade-offs. The platform's primary design is **atomic DvP at T+0** (Vol. II §9), which is precisely what the Swiss DLT trading facility model enables by settling the security on a public ledger against a cash leg connected to the national payment system.[164]

5.2 Atomic delivery-versus-payment

In atomic DvP the settlement contract holds both legs and releases them together or not at all, so neither counterparty is ever exposed to the other's default. The transfer leg still passes the ERC-3643 eligibility checks (§9), so atomic settlement never bypasses compliance.

Figure 9 — Atomic DvP settlement sequence.

[164] FINMA — authorisation of the first DLT trading facility (operated by BX Digital), settlement on a public blockchain with the cash leg via the Swiss Interbank Clearing system; regime at FMIA (FinfraG) Art. 73a et seqq. and FinMIO Art. 58a et seqq.; "small facility" thresholds; segregation of crypto-based assets at DEBA Art. 242a. Verified live 30 Jun 2026: https://www.finma.ch/en/news/2025/03/20250318-mm-dlt-handelssystem/

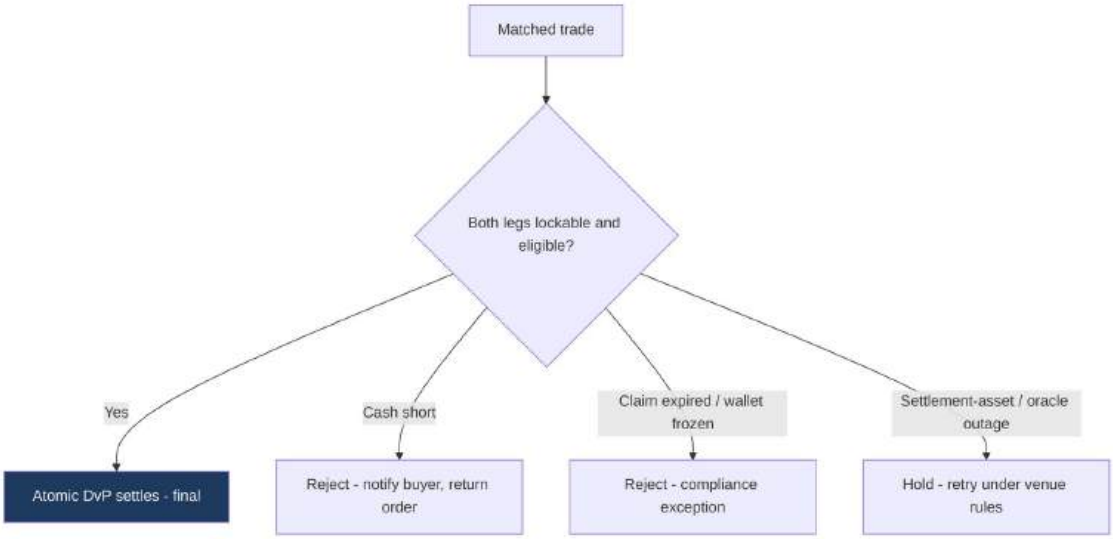


The cash and security legs settle together or not at all; the eligibility re-check inside settlement means an ineligible buyer cannot take delivery even after matching.

5.3 Finality and failed-trade handling

Settlement is treated as final only at the chain's **deterministic finality** (sub-second on the recommended chain; Vol. II §11.2), not on inclusion. Because atomic DvP cannot partially complete, the classic "failed trade" (one leg settles, the other does not) is eliminated by construction; what remains are **pre-settlement failures** — insufficient funds, an expired eligibility claim, a frozen wallet, an oracle/settlement-asset outage. These are handled deterministically: the trade does not settle, both legs are released, the cause is surfaced, and the order is returned or cancelled per the venue rules.

Figure 10 — Failed-trade / settlement-exception handling.



Atomic settlement converts the traditional "failed trade" problem into deterministic pre-settlement exceptions, each with a defined remedy.

CHAPTER 6 — LIQUIDITY

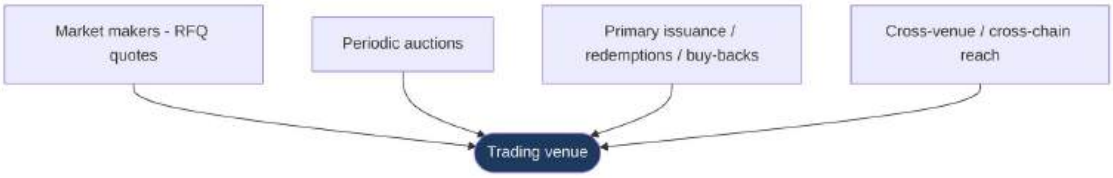
6.1 The honest problem

Tokenisation is often sold as "instant liquidity." It is not. Fractionalising an asset and putting it on a ledger lowers some barriers (minimums, settlement friction, accessibility) but does not by itself create buyers and sellers. Real-estate-backed securities are inherently **illiquid**: the underlying assets are heterogeneous, valuation is periodic not continuous, and holders are often long-term. A marketplace that pretends otherwise misleads investors. The platform therefore treats liquidity as something to be **built and managed**, not assumed, and discloses liquidity characteristics honestly at the point of trade (§8).

6.2 Sources of liquidity and how they are provided

Liquidity is assembled from several sources: **market-maker programmes** (committed two-sided quotes, often via RFQ), **periodic auctions** that concentrate natural buyers and sellers at points in time, **primary–secondary interplay** (new issuance and redemptions/buy-backs as liquidity events), and **cross-venue / cross-chain reach** so that demand is not siloed. Cross-chain liquidity uses the interoperability layer of Vol. II §2.3, moving value with compliance metadata attached so eligibility survives the hop.

Figure 11 — Liquidity sources and provision.



No single source solves illiquidity; the venue combines committed market making, time-concentrated auctions, the natural liquidity of primary and redemption events, and cross-venue reach — and still discloses that secondary liquidity may be limited.

6.3 Liquidity, redemption and the product design

Where secondary liquidity is structurally thin, the **product** can carry liquidity features instead of relying on the market: scheduled redemption windows, periodic tender/buy-back facilities, or interval-fund-style mechanics (defined in Vol. I Ch. 3 and Vol. IV). These shift liquidity provision from an uncertain secondary market to a designed feature of the instrument, and must be disclosed and modelled (Vol. IV) rather than promised.

CHAPTER 7 — MARKET INTEGRITY & SURVEILLANCE

7.1 Why integrity controls apply

Trading a security — even among eligible, identified parties — attracts market-integrity obligations: prohibitions on **insider dealing**, **unlawful disclosure of inside information**, and **market manipulation**, plus obligations to monitor, detect, report suspicious activity, and report transactions to regulators. In the EU these sit in the **Market Abuse Regulation (Regulation (EU) No 596/2014, "MAR")** and the transaction-reporting regime of **MiFIR (Regulation (EU) No 600/2014)**; in Switzerland, market-conduct rules sit in the **Financial Market Infrastructure Act (FMIA/FinfraG)**; analogous regimes apply in the UK and other jurisdictions. A DLT venue does not escape these; if anything, an identified-participant venue with an immutable ledger is well placed to satisfy them.

7.2 Behaviours and controls

Prohibited / monitored behaviour	Surveillance control
Insider dealing (trading on inside information)	Restricted lists; trade-vs-information timing analysis; access controls on material non-public information
Unlawful disclosure of inside information	Information-barrier monitoring; disclosure logging
Market manipulation (wash trades, spoofing, layering, marking the close)	Pattern detection on orders/trades; self-trade prevention; auction-price integrity checks
Front-running / misuse of order flow	Order-handling controls; segregation of duties; surveillance of operator/market-maker activity

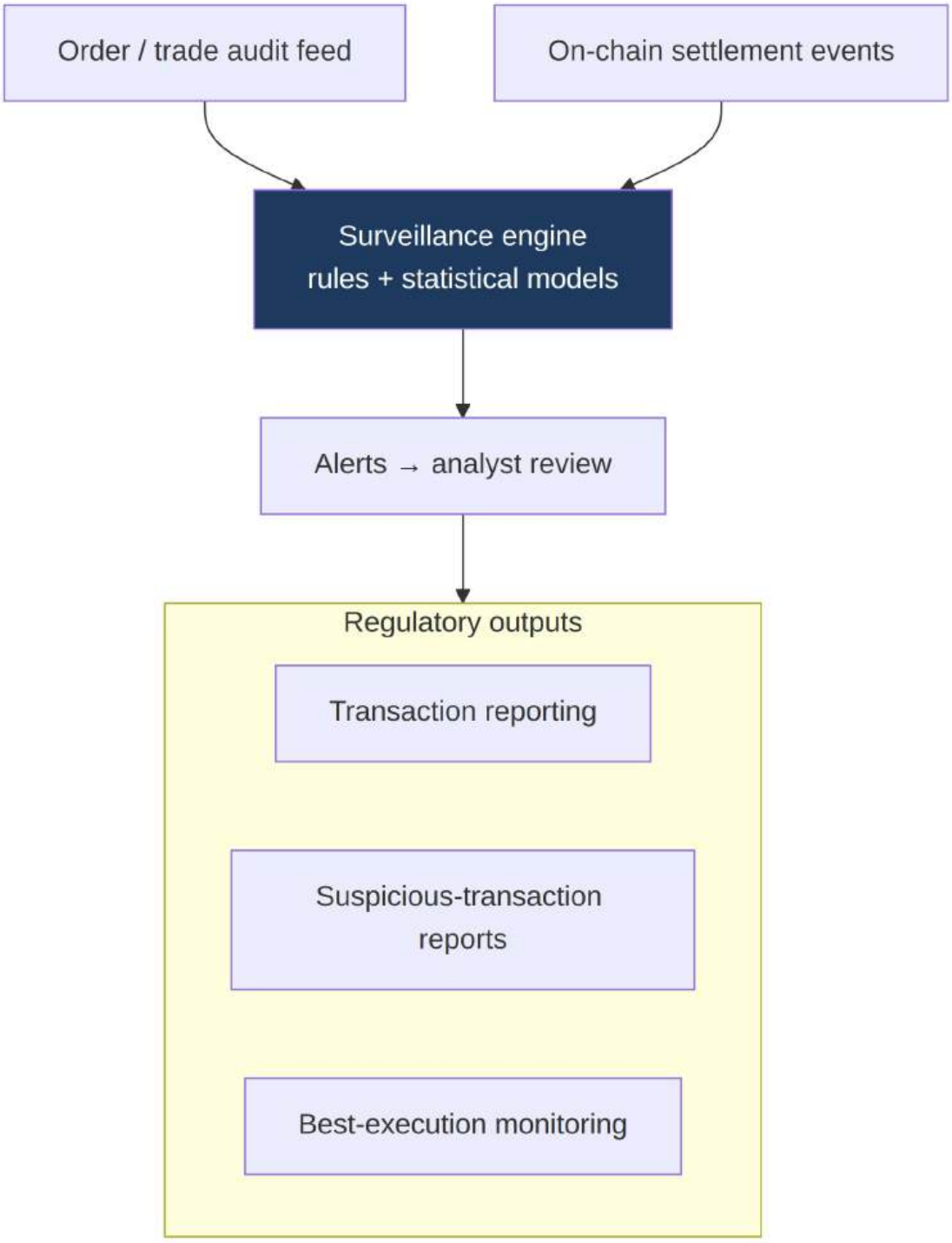
Prohibited / monitored behaviour	Surveillance control
Suspicious transactions	STOR-style suspicious-transaction-and-order reporting to the competent authority

Table 6 — Market-abuse behaviours and surveillance controls. The venue's surveillance benefits from two DLT-specific advantages: **identified participants** (no anonymous flow, because every holder has a verified identity — Vol. II §4) and an **immutable, timestamped record** of orders and on-chain settlements, which strengthens detection and evidential quality.

7.3 Surveillance architecture and reporting

Surveillance ingests the matching engine's order/trade audit feed (§4.3) and on-chain settlement events, runs detection models (rule-based and statistical), raises alerts for human review, and produces regulatory outputs: **transaction reporting** (e.g. MiFIR-style), **suspicious-transaction-and-order reports**, and **best-execution** monitoring (that participants obtained the best available result, evidenced by execution data).

Figure 12 — Market-surveillance architecture.



Identified participants and an immutable ledger make detection and reporting more tractable than in anonymous venues; surveillance is a first-class venue function, not an afterthought.

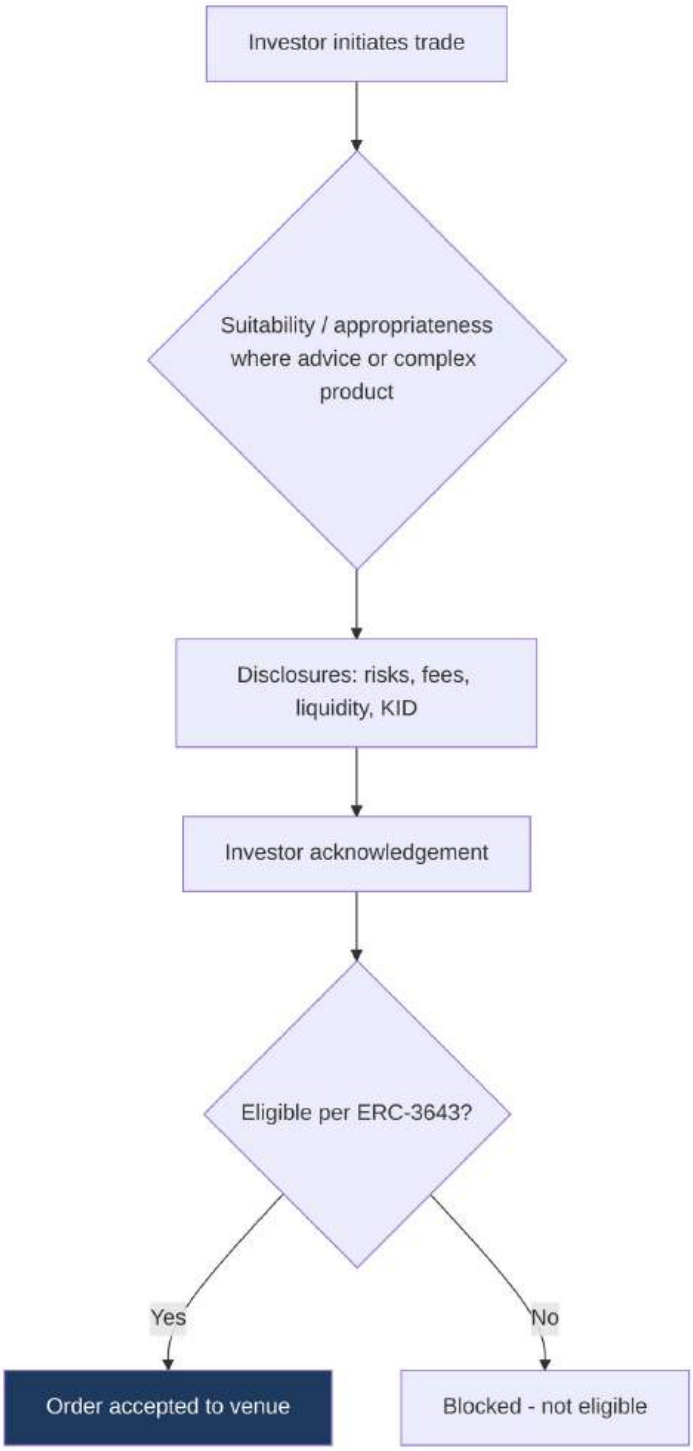
CHAPTER 8 — INVESTOR PROTECTION & CONDUCT AT THE POINT OF TRADE

8.1 Conduct does not stop at onboarding

Eligibility checks (Vol. II §4) establish *who may hold* the security; conduct rules govern *how the venue and intermediaries must behave* when that investor trades. These include **suitability/appropriateness** assessments, clear **disclosures** (including a key information document where required), fair treatment, conflict management, complaint handling, and cooling-off where applicable. The relevant regimes are Switzerland's **Financial Services Act (FinSA)** and, for EEA-facing activity, **MiFID II** plus the **PRIIPs** key-information-document regime (Vol. I §4.2, §1.4).

8.2 Point-of-trade conduct flow

Figure 13 — Point-of-trade conduct and suitability flow.



Conduct obligations (suitability, disclosure, acknowledgement) run alongside the technical eligibility gate; both must pass before an order is accepted.

8.3 Conduct obligations by regime

Obligation	Switzerland (FinSA)	EEA (MiFID II / PRIIPs)
Client classification	Retail / professional / institutional	Retail / professional / eligible counterparty
Suitability / appropriateness	Required for advice / discretionary	Required per service and product complexity
Key information document	Basisinformationsblatt where applicable	PRIIPs KID for packaged products to retail
Best execution	Best possible result	Best execution obligation with monitoring
Disclosure of risks, costs, conflicts	Required	Required

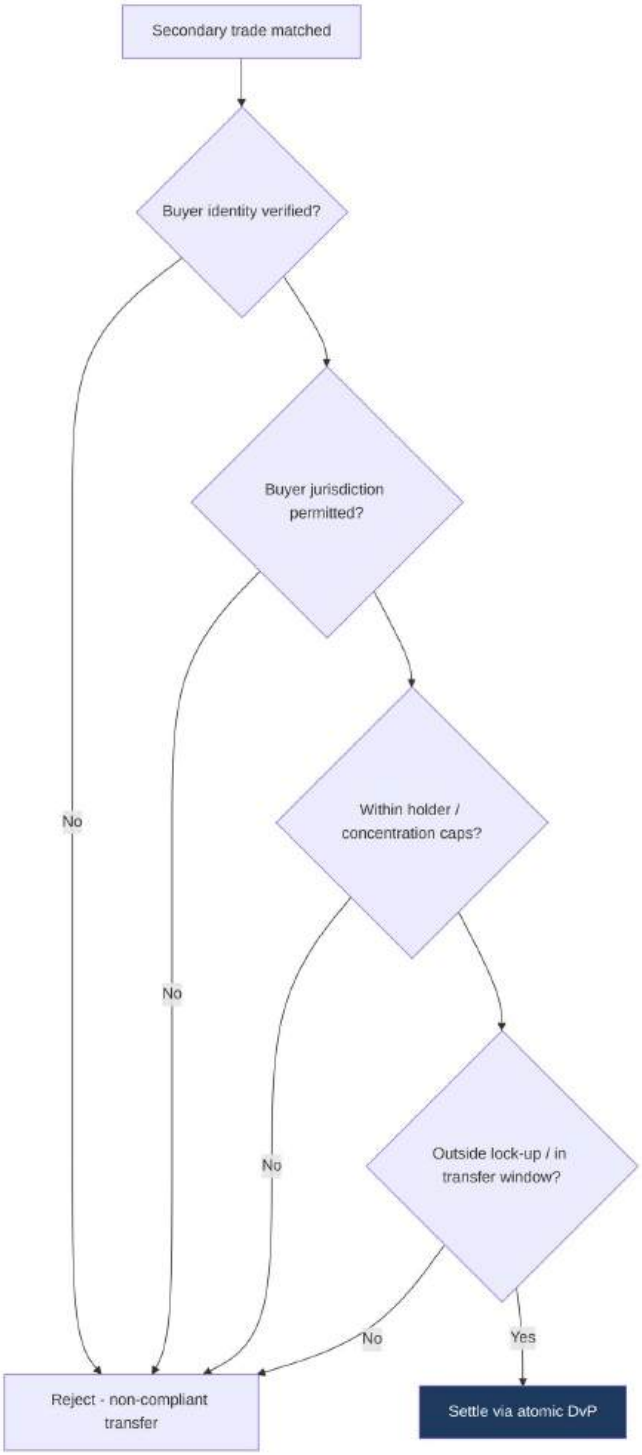
Table 7 — Point-of-trade conduct obligations by regime. The platform applies the **stricter applicable standard** where an investor could fall under more than one regime, and discloses the real liquidity profile of the instrument (§6) so that “tradeable” is never confused with “liquid.”

CHAPTER 9 — SECONDARY-MARKET COMPLIANCE ENFORCEMENT

9.1 The same enforcement, now at trade time

The compliance machinery built in Volume II is what makes secondary trading lawful without a manual gatekeeper on every trade. At the point of a secondary transfer, the ERC-3643 token re-checks **identity/eligibility**, **jurisdiction**, **holder caps**, **lock-ups/transfer windows**, and **balance/concentration limits** — the same modules that governed issuance (Vol. II §4.3) — now evaluated against the buyer. A trade that would breach any rule (e.g. selling to an investor in a non-permitted jurisdiction, or pushing holder count past an exemption threshold) **cannot settle**.

Figure 14 — Secondary-transfer compliance enforcement.



Every secondary trade is re-validated against the full rule set; the marketplace cannot create a holding that the legal architecture forbids.

9.2 Corporate actions and the transfer-agent function

Secondary markets must also handle **corporate actions** — income distributions, capital calls, conversions (e.g. Model B completion; Vol. II §3.3), splits, and redemptions — and the **transfer-agent / registrar** function of maintaining the authoritative holder register. On the platform, the register *is* the on-chain token state, and corporate actions are executed as governed on-chain operations with off-chain orchestration (Vol. II §6), keeping the cap table correct as ownership changes hands. Where a venue requires an external registrar or paying agent, the platform integrates with it rather than duplicating it.

9.3 Cross-jurisdiction enforcement

Because eligibility rules are data-driven modules (Vol. II §4.3), the same token can enforce **different rules for different buyers**: an EEA buyer is checked against the EEA module set, a Swiss buyer against the Swiss set, and a buyer from a non-permitted jurisdiction is blocked. This is what makes the multi-jurisdiction venue map (§2.3) workable without a separate token per market.

CHAPTER 10 — FEES, MARKET DATA & CONNECTIVITY

10.1 Fee model (architectural)

The venue's fee model is specified commercially in Volume VI; architecturally it supports transparent, rule-based fees: trading/commission fees, settlement fees, listing/admission fees, market-data fees, and market-maker rebates/incentives. Fees must be disclosed (a §8 conduct obligation) and computed deterministically so that participants can reconcile them.

10.2 Market data

The venue publishes **pre-trade** (quotes/auction indications, subject to the chosen transparency model) and **post-trade** (executed trade) data, plus reference and valuation data (NAV; Vol. IV). Transparency is calibrated to the trading model and regime — an RFQ/auction market has a different transparency profile from a continuous order book — and to the regulator's requirements. On-chain settlement provides an inherent, verifiable post-trade record.

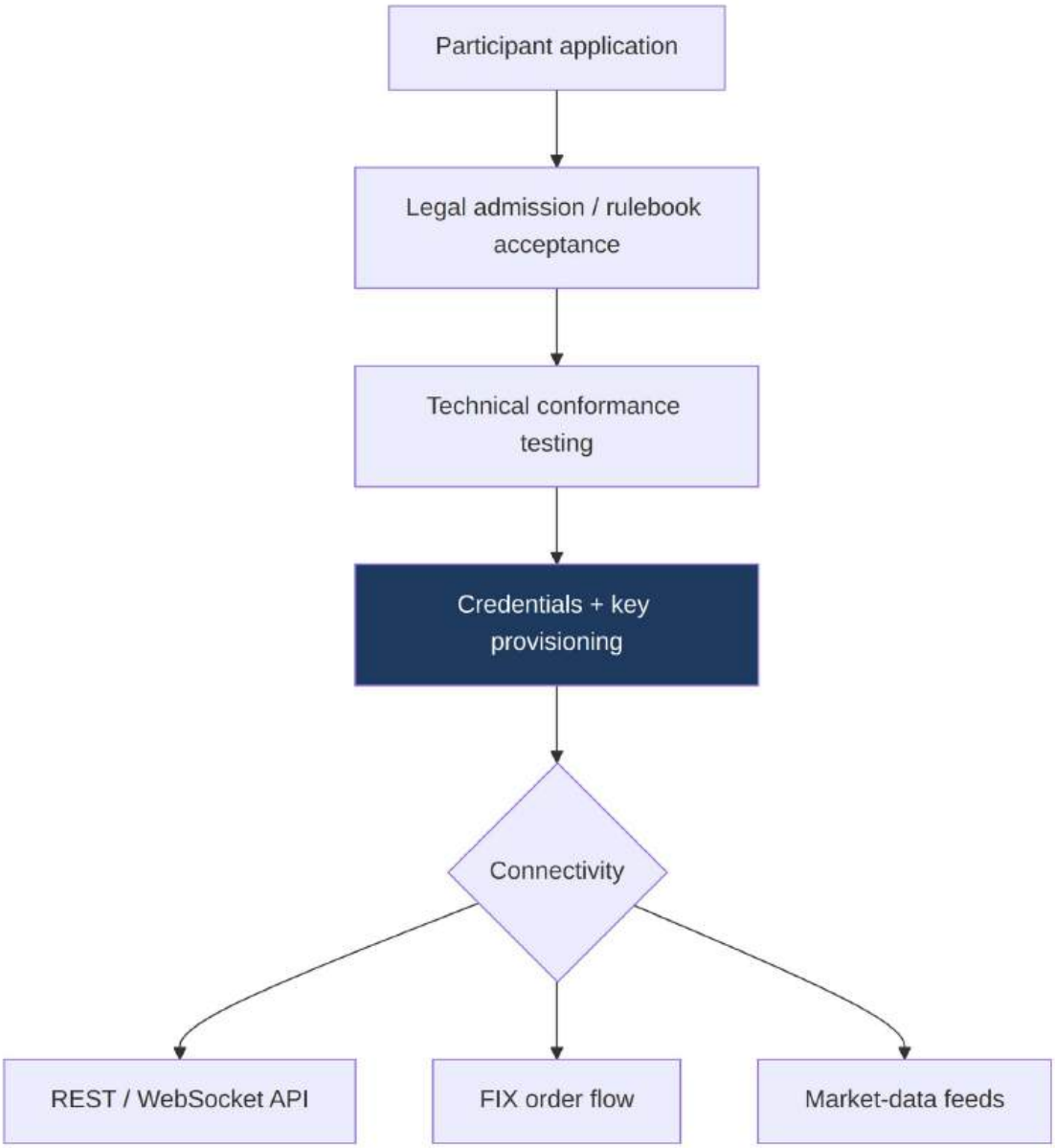
10.3 Connectivity and onboarding

Participants connect through **REST/WebSocket APIs** and, for institutional order flow, the **FIX protocol**; market data is distributed over streaming feeds. Participant onboarding (especially where the venue is participant-only, as the Swiss DLT trading

facility model is for supervised institutions[165]) is a governed process: legal admission, technical certification, conformance testing, and credential/key provisioning (keys per Vol. II §7).

Figure 15 — Participant connectivity and onboarding.

[165] FINMA — authorisation of the first DLT trading facility (operated by BX Digital), settlement on a public blockchain with the cash leg via the Swiss Interbank Clearing system; regime at FMIA (FinfraG) Art. 73a et seqq. and FinMIO Art. 58a et seqq.; “small facility” thresholds; segregation of crypto-based assets at DEBA Art. 242a. Verified live 30 Jun 2026: https://www.finma.ch/en/news/2025/03/20250318-mm-dlt-handelssystem/



Onboarding is legal admission, then technical certification, then credentialing; only certified participants get connectivity, consistent with a regulated, participant-aware venue.

CHAPTER 11 — COMPETITIVE LANDSCAPE & BENCHMARKS

11.1 Benchmarks, not targets

The following are **benchmarks for design and positioning only** — not endorsements, partnerships, or competitive claims. They illustrate the range of approaches to trading tokenised securities as of the date of documentation.

Benchmark	Approach	Relevance
Swiss DLT trading facility (first authorised 2025)	DLT trading + settlement on a public ledger, cash leg via national payment system, participant-only, "small facility" thresholds	Closest analogue to the platform's primary venue path[166]
SIX Digital Exchange (SDX)	Regulated digital exchange/CSD operating via conventional CSD licensing	Benchmark for an integrated, bank-grade digital venue
EU DLT MTF (e.g. an authorised DLT MTF, 2025)	DLT MTF under the Pilot Regime admitting tokenised securities/bonds with a CSD-integrated settlement model	Benchmark for the EU Pilot-Regime route and its caps[167][168]
UK Digital Securities Sandbox entrants	Notary/maintenance/settlement ± trading venue under a gated sandbox to 2029	Benchmark for the UK route[169]
Tokenised-equity platforms (offshore)	Tokenised wrappers of listed equities traded on crypto venues; rapid growth, US-access-restricted	Benchmark for retail demand and the risks of issuer-less wrappers
Central-depository tokenisation pilots	Incumbent post-trade infrastructure piloting tokenised settlement with major institutions	Benchmark for institutional settlement integration[170]

[166] FINMA — authorisation of the first DLT trading facility (operated by BX Digital), settlement on a public blockchain with the cash leg via the Swiss Interbank Clearing system; regime at FMIA (FinfraG) Art. 73a et seqq. and FinMIO Art. 58a et seqq.; "small facility" thresholds; segregation of crypto-based assets at DEBA Art. 242a. Verified live 30 Jun 2026: https://www.finma.ch/en/news/2025/03/20250318-mm-dlt-handelssystem/

[167] EUR-Lex — Regulation (EU) 2022/858 (DLT Pilot Regime): DLT MTF/SS/TSS; €6bn admission cap and €9bn transition trigger; applicable 23 March 2023. Verified live: https://eur-lex.europa.eu/eli/reg/2022/858/oj/eng

[168] ESMA — report on the functioning and review of the DLT Pilot Regime under Article 14 (June 2025), recommending revisiting the regime's caps and constraints. Verified live: https://www.esma.europa.eu/sites/default/files/2025-06/ESMA75-117376770-460_Report_on_the_functioning_and_review_of_the_DLTR_-_Art.14.pdf

Table 8 — Competitive benchmarks (venues and platforms). The platform's distinct positioning is the combination of (a) a **compliance-by-construction** security token (Vol. II), (b) **atomic DvP** settlement, (c) a **real-estate-specific** product and lifecycle (Vol. I, Vol. IV), and (d) a **multi-jurisdiction** venue strategy that begins by listing on authorised venues rather than by operating one.

11.2 What the benchmarks teach

Three lessons shape the design. First, the **authorised, integrated trading-and-settlement** model (Swiss DLT trading facility; EU DLT TSS) is the credible institutional path, and atomic DvP is its defining advantage. Second, **issuer-less tokenised wrappers** of third-party securities raise classification and investor-protection concerns (echoed in the US substance-over-form statement[171]); the platform avoids that posture by tokenising assets it or its SPVs legally control (Vol. I). Third, **liquidity is hard even for listed-equity wrappers**, reinforcing the honest liquidity treatment of §6.

CHAPTER 12 — LIMITATIONS & THREATS REGISTER

12.1 Honest assessment

#	Threat / limitation	Exposure	Mitigation / status
1	Thin secondary liquidity (cold start)	High	Market-maker programmes, auctions,

[169] UK Digital Securities Sandbox — joint Bank of England / FCA FMI sandbox; notary/maintenance/settlement (DSD) optionally combined with a trading venue; open since September 2024; runs to 8 January 2029 (extendable by HM Treasury). Verified live: https://www.fca.org.uk/firms/innovation/digital-securities-sandbox and https://www.bankofengland.co.uk/financial-stability/digital-securities-sandbox

[170] SEC — staff statement on tokenised securities (January 2026): tokenising a security does not change its regulatory classification; federal securities laws apply by economic substance. A proposed "innovation exemption" for on-chain trading of tokenised securities was, as of 30 June 2026, proposed and in flux. Verified live: https://www.sec.gov/newsroom/speeches-statements/corp-fin-statement-tokenized-securities-012826-statement-tokenized-securities

[171] SEC — staff statement on tokenised securities (January 2026): tokenising a security does not change its regulatory classification; federal securities laws apply by economic substance. A proposed "innovation exemption" for on-chain trading of tokenised securities was, as of 30 June 2026, proposed and in flux. Verified live: https://www.sec.gov/newsroom/speeches-statements/corp-fin-statement-tokenized-securities-012826-statement-tokenized-securities

#	Threat / limitation	Exposure	Mitigation / status
			product-level redemption features; honest disclosure (§6, §8)
2	Venue-authorisation risk / timeline	High	List on authorised venues first; operate later; counsel-led (§2.3)
3	EU Pilot-Regime caps (€6bn/€9bn) constrain scale	Medium-High	Track ESMA Art. 14 review; use Swiss route as primary; transition strategy (§2.2)[172]
4	US “innovation exemption” uncertain / in flux	Medium	Treat US as watch item; rely on substance-over-form statement, not the proposed exemption (§2.4)[173]
5	Market abuse / manipulation	Medium	Surveillance, identified participants, immutable record, STOR reporting (§7)
6	Settlement-asset failure (de-peg / outage)	Medium-High	Proof-of-reserve asset, atomic DvP, fallback rails (§5; Vol. II §9)
7	Best-execution / suitability failures	Medium	Conduct controls, monitoring, stricter-standard rule (§8)
8	Cross-venue / cross-chain settlement risk	Medium	Defence-in-depth interop, compliance-metadata transport (§6; Vol. II §2.3)
9	Operate-vs-list dependency on third-party venue	Medium	Multi-venue strategy; avoid single-venue lock-in (§2.3)
10	Mismatch between on-chain finality and off-chain matching	Low-Medium	Settle only at deterministic finality; reconcile projections (§5.3; Vol. II

[172] ESMA — report on the functioning and review of the DLT Pilot Regime under Article 14 (June 2025), recommending revisiting the regime’s caps and constraints. Verified live: https://www.esma.europa.eu/sites/default/files/2025-06/ESMA75-117376770-460_Report_on_the_functioning_and_review_of_the_DLTR_-_Art.14.pdf

[173] SEC — staff statement on tokenised securities (January 2026): tokenising a security does not change its regulatory classification; federal securities laws apply by economic substance. A proposed “innovation exemption” for on-chain trading of tokenised securities was, as of 30 June 2026, proposed and in flux. Verified live: https://www.sec.gov/newsroom/speeches-statements/corp-fin-statement-tokenized-securities-012826-statement-tokenized-securities

#	Threat / limitation	Exposure	Mitigation / status
			§11)
11	Corporate-action errors affecting cap table	Medium	Governed on-chain operations; register = token state; audits (§9.2)
12	Regulatory change to venue/market-abuse regimes	Medium	Modular compliance; venue-agnostic design; monitoring (§2, §9)
13	Over-promising “liquidity” / mis-selling	Medium	Liquidity realism and disclosure as a conduct obligation (§6, §8)

12.2 Honest limitations

This is a market-design document, not a venue rulebook or matching-engine specification; throughput, latency, and depth figures are to be validated by testing (Vol. V/VI). Venue authorisation is jurisdiction-specific and not guaranteed. The single largest honest caveat is **liquidity**: the platform can make a security *tradeable and compliant*, but it cannot manufacture a deep secondary market for an inherently illiquid asset, and it must say so to investors. The US route is genuinely unsettled as of the date of documentation and must be re-checked.

INTERIM COMPLIANCE & COMPLETENESS AUDIT — VOLUME III

Verification performed. Venue regimes, thresholds, authorisations, and developments were checked against primary sources on 30 June 2026 and recorded in Appendix A: the Swiss **DLT trading facility** regime (FMIA Art. 73a et seqq.) and the first authorisation under it[174]; the EU **DLT Pilot Regime** (Reg (EU) 2022/858), its **€6bn/€9bn** caps and the ESMA **Article 14** review[175][176]; the UK **Digital Securities Sandbox** and its run to **8 Jan 2029**[177]; and the US position (the SEC **Jan 2026** staff statement on

[174] FINMA — authorisation of the first DLT trading facility (operated by BX Digital), settlement on a public blockchain with the cash leg via the Swiss Interbank Clearing system; regime at FMIA (FinfraG) Art. 73a et seqq. and FinMIO Art. 58a et seqq.; “small facility” thresholds; segregation of crypto-based assets at DEBA Art. 242a. Verified live 30 Jun 2026: https://www.finma.ch/en/news/2025/03/20250318-mm-dlt-handelssystem/

[175] EUR-Lex — Regulation (EU) 2022/858 (DLT Pilot Regime): DLT MTF/SS/TSS; €6bn admission cap and €9bn transition trigger; applicable 23 March 2023. Verified live: https://eur-lex.europa.eu/eli/reg/2022/858/oj/eng

tokenised securities and the proposed, in-flux **innovation exemption**)[178]. EU **MAR (596/2014)**, **MiFIR (600/2014)**, **MiFID II (2014/65/EU)**, Swiss **FMIA/FinSA**, and **PRIIPs** are cited by their stable legislative identifiers.

Cross-volume items resolved. Two Volume I flagged items are confirmed here and carried to the final cross-volume audit: the DLT trading facility licence at **FMIA Art. 73a et seqq.** (with FinMIO Art. 58a et seqq.), and bankruptcy **segregation of crypto-based assets at DEBA Art. 242a**.[179]

No fabricated identifiers. No regulation number, threshold, authorisation, or URL has been invented; uncertain items (notably the US innovation exemption) are flagged as proposed/in flux rather than stated as settled.

Open / flagged items for specialist sign-off. 1. Operate-vs-list venue decision and sequencing — confirm with market-infrastructure counsel (§2.3). 2. EU Pilot-Regime capacity caps vs the platform's target scale — monitor the ESMA review and EC response (§2.2, §12). 3. US innovation exemption — track to final text; do not design to it until settled (§2.4). 4. Trading-model mix per instrument (RFQ/auction/CLOB/AMM) — confirm with liquidity/market-making strategy (§3). 5. Settlement-asset selection and finality assumptions — confirm with Vol. II §9 and treasury. 6. Market-abuse and transaction-reporting obligations per venue — confirm exact templates/regimes with counsel (§7).

---

[176] ESMA — report on the functioning and review of the DLT Pilot Regime under Article 14 (June 2025), recommending revisiting the regime's caps and constraints. Verified live: https://www.esma.europa.eu/sites/default/files/2025-06/ESMA75-117376770-460_Report_on_the_functioning_and_review_of_the_DLTR_-_Art.14.pdf

[177] UK Digital Securities Sandbox — joint Bank of England / FCA FMI sandbox; notary/maintenance/settlement (DSD) optionally combined with a trading venue; open since September 2024; runs to 8 January 2029 (extendable by HM Treasury). Verified live: https://www.fca.org.uk/firms/innovation/digital-securities-sandbox and https://www.bankofengland.co.uk/financial-stability/digital-securities-sandbox

[178] SEC — staff statement on tokenised securities (January 2026): tokenising a security does not change its regulatory classification; federal securities laws apply by economic substance. A proposed "innovation exemption" for on-chain trading of tokenised securities was, as of 30 June 2026, proposed and in flux. Verified live: https://www.sec.gov/newsroom/speeches-statements/corp-fin-statement-tokenized-securities-012826-statement-tokenized-securities

[179] FINMA — authorisation of the first DLT trading facility (operated by BX Digital), settlement on a public blockchain with the cash leg via the Swiss Interbank Clearing system; regime at FMIA (FinfraG) Art. 73a et seqq. and FinMIO Art. 58a et seqq.; "small facility" thresholds; segregation of crypto-based assets at DEBA Art. 242a. Verified live 30 Jun 2026: https://www.finma.ch/en/news/2025/03/20250318-mm-dlt-handelssystem/

Link policy. Hyperlinks point only to official/primary sources verified live on 30 June 2026 (EUR-Lex, ESMA, FINMA, FCA, the Bank of England, the SEC). All other sources are cited by stable identifier.

FUTURE JURISDICTION & TECHNOLOGY COMPATIBILITY NOTES

Jurisdiction portability. The same security can be admitted to venues in multiple jurisdictions because the on-chain compliance layer enforces each jurisdiction's eligibility rules per buyer (§9.3). Adding a market is a matter of (a) a venue route (operate or list) and (b) a compliance-module set, not a new token.

Watch items. (a) **EU DLT Pilot Regime** — ESMA's Article 14 review recommended revisiting the €6bn/€9bn caps and other constraints; track the European Commission's response, which could materially change EU capacity.[180] (b) **US innovation exemption** — track to final text; the conservative anchor remains that tokenisation does not change classification.[181] (c) **UK DSS** — track the gated scaling and the intended transition to a permanent regime before 2029.[182] (d) **Settlement assets** — tokenised deposits, regulated stablecoins, and wholesale central-bank-money experiments may change the cash leg; keep the DvP design asset-agnostic (Vol. II §9). (e) **Cross-border venue links** — bilateral initiatives between markets may open new routes; keep interoperability standards-based (Vol. II §2.3).

---

[180] ESMA — report on the functioning and review of the DLT Pilot Regime under Article 14 (June 2025), recommending revisiting the regime's caps and constraints. Verified live: https://www.esma.europa.eu/sites/default/files/2025-06/ESMA75-117376770-460_Report_on_the_functioning_and_review_of_the_DLTR_-_Art.14.pdf

[181] SEC — staff statement on tokenised securities (January 2026): tokenising a security does not change its regulatory classification; federal securities laws apply by economic substance. A proposed "innovation exemption" for on-chain trading of tokenised securities was, as of 30 June 2026, proposed and in flux. Verified live: https://www.sec.gov/newsroom/speeches-statements/corp-fin-statement-tokenized-securities-012826-statement-tokenized-securities

[182] UK Digital Securities Sandbox — joint Bank of England / FCA FMI sandbox; notary/maintenance/settlement (DSD) optionally combined with a trading venue; open since September 2024; runs to 8 January 2029 (extendable by HM Treasury). Verified live: https://www.fca.org.uk/firms/innovation/digital-securities-sandbox and https://www.bankofengland.co.uk/financial-stability/digital-securities-sandbox

GLOSSARY

Covers terms introduced in this volume; master glossary in Volume I, technical glossary in Volume II. Canonical reminder: the instrument is a **ledger-based security** implemented as an **ERC-3643 permissioned token**.

- **AMM (automated market maker)** — an on-chain mechanism that prices and executes trades against a liquidity pool; here, necessarily compliance-gated.
- **Atomic DvP** — settlement in which the security and cash legs transfer together or not at all.
- **Best execution** — the obligation to obtain the best possible result for a client's order.
- **CLOB (central limit order book)** — continuous order matching by price-time priority.
- **Corporate action** — an event affecting holders (distribution, capital call, conversion, split, redemption).
- **DLT MTF / SS / TSS** — under the EU Pilot Regime: DLT multilateral trading facility / settlement system / combined trading-and-settlement system.
- **DLT trading facility** — the Swiss licence (FMIA Art. 73a et seqq.) for multilateral trading (and settlement) of DLT securities.
- **DSD (Digital Securities Depository)** — a notary/maintenance/settlement function in the UK Digital Securities Sandbox.
- **DSS (Digital Securities Sandbox)** — the UK BoE/FCA FMI sandbox for digital securities (to Jan 2029).
- **FIX** — Financial Information eXchange, the standard messaging protocol for institutional order flow.
- **Innovation exemption (US)** — a proposed, time-limited SEC exemption for on-chain trading of tokenised securities (in flux).
- **MAR** — EU Market Abuse Regulation (Regulation (EU) No 596/2014).
- **MiFID II / MiFIR** — EU markets-in-financial-instruments Directive 2014/65/EU and Regulation (EU) No 600/2014 (incl. transaction reporting).
- **Periodic auction** — collecting orders and matching them at intervals at a single clearing price.
- **PRIIPs KID** — the key information document for packaged retail and insurance-based investment products.
- **Primary / secondary market** — issuance/distribution to first holders / subsequent investor-to-investor trading.
- **RFQ (request for quote)** — a model where a participant requests quotes from market makers and executes bilaterally.
- **STOR** — suspicious-transaction-and-order report to a competent authority.
- **Transfer agent / registrar** — maintainer of the authoritative holder register (here, the on-chain token state).

APPENDIX A — VENUE & REGULATORY REGISTER

Authoritative register of venue regimes relied on. "Verified live 30 Jun 2026" means the official source was retrieved on that date. Hyperlinks only to official sources verified live; other items cited by stable identifier. Re-check before any application or build.

#	Regime / source	Identifier / key facts	Official source
A1	EU DLT Pilot Regime	Reg (EU) 2022/858; DLT MTF/SS/TSS; €6bn cap, €9bn transition; applicable 23 Mar 2023	EUR-Lex — https://eur-lex.europa.eu/eli/reg/2022/858/oj/eng
A2	ESMA Art. 14 review of the DLTR	Review report (June 2025) recommending revisiting caps/constraints	ESMA — https://www.esma.europa.eu/sites/default/files/2025-06/ESMA75-117376770-460_Report_on_the_functioning_and_review_of_the_DLTR_-_Art.14.pdf
A3	Swiss DLT trading facility	FMIA Art. 73a et seqq.; FinMIO Art. 58a et seqq.; first facility authorised 2025; public-ledger settlement + national payment-system cash leg; "small facility" thresholds	FINMA — https://www.finma.ch/en/news/2025/03/20250318-mm-dlt-handelssystem/
A4	UK Digital Securities Sandbox (FCA)	DSD ± trading venue; Gates 1–4; open since Sep 2024	FCA — https://www.fca.org.uk/firms/innovation/digital-securities-sandbox
A5	UK Digital Securities Sandbox (BoE)	Runs to 8 Jan 2029 (extendable by HMT)	Bank of England — https://www.bankofengland.co.uk/financial-stability/digital-securities-sandbox
A6	US — tokenised securities classification	SEC staff statement (Jan 2026): tokenisation does not change classification; substance-over-form	SEC — https://www.sec.gov/newsroom/speeches-statements/corp-fin-statement-tokenized-securities-012826-statement-tokenized-securities
A7	EU MAR	Regulation (EU) No 596/2014 (market abuse)	Cited by identifier
A8	EU MiFID II / MiFIR	Directive 2014/65/EU; Regulation (EU) No 600/2014 (incl. transaction	Cited by identifier

#	Regime / source	Identifier / key facts	Official source
		reporting)	
A9	Swiss FMIA / FinSA	FMIA (FinfraG) market conduct; FinSA conduct/suitability; DEBA Art. 242a (segregation)	Cited by identifier (see Vol. I register)
A10	PRIIPs KID	Packaged-product key information document regime	Cited by identifier

APPENDIX B — ORDER-TYPE & MESSAGE CATALOGUE (INDICATIVE)

Indicative; to be fixed against the chosen venue rulebook and matching-engine specification, and conformance-tested at onboarding (§10.3).

Category	Items
Order types	Limit; Market (protected); RFQ request/response; Auction (call); Good-till-time; All-or-none
Order events	New; Amend; Cancel; Reject; Partial fill; Fill; Expire
Trade/settlement messages	Match notification; Settlement instruction; Settlement confirmed; Settlement rejected; Exception
Market-data messages	Quote/indication; Auction imbalance/indicative price; Trade print; Reference/NAV update
Connectivity	REST; WebSocket; FIX session (logon, heartbeat, order, execution report)

APPENDIX C — SURVEILLANCE SCENARIO LIBRARY (INDICATIVE)

Indicative detection scenarios; to be calibrated with compliance and the competent authority's expectations (§7).

Scenario	Signal
Wash trading	Self-matched or circular trades among related accounts
Spoofing / layering	Large orders placed and cancelled to move price
Marking the close / auction	Disproportionate activity at price-forming points

Scenario	Signal
Insider dealing	Trading ahead of price-sensitive disclosures (corporate actions, valuations)
Front-running	Operator/market-maker trading ahead of known client flow
Manipulative RFQ behaviour	Quote manipulation or collusion in bilateral flow
Settlement abuse	Patterned pre-settlement failures to disrupt counterparties

APPENDIX D — CITATION REGISTER (TABLE — VOLUME III)

Sources relied on in Volume III. P = official/primary; S = secondary/commentary (paraphrased only).

Ref	Source	Type	Used for	Verification note
bxd	FINMA — first DLT trading facility authorisation	P	Swiss DLT trading facility regime; public-ledger settlement; thresholds; FMIA Art. 73a; DEBA Art. 242a	Verified live 30 Jun 2026
dltr	EUR-Lex — Reg (EU) 2022/858 (DLT Pilot Regime)	P	DLT MTF/SS/TSS; caps; applicability	Verified live
esmadltr	ESMA — Art. 14 review report (June 2025)	P	Review findings; cap recommendation	Verified live
dss	FCA / Bank of England — Digital Securities Sandbox	P	UK route; DSD ± trading venue; run to 8 Jan 2029	Verified live
sects	SEC — staff statement on tokenised securities (Jan 2026)	P	Substance-over-form; US watch item; benchmark	Verified live

APPENDIX E — CROSS-REFERENCE INDEX

Topic	This volume	Other volumes
Token = ledger-based security	§1.1	Vol. I §1, §4.1; Vol. II §3

Topic	This volume	Other volumes
Eligibility enforced at trade	§4.2, §9	Vol. II §3–4
Atomic DvP settlement	§5	Vol. II §9
Venue regimes (CH/EU/UK/US)	§2	Vol. I §4.3, §5–7
Market abuse / surveillance	§7	Vol. I §4 (conduct)
Suitability / disclosure / KID	§8	Vol. I §4.2, §1.4
Liquidity / redemption features	§6	Vol. I Ch. 3; Vol. IV
Valuation / NAV / market data	§10.2	Vol. IV; Vol. II §5
Operational resilience of venue	§10.3	Vol. V
Fee model / volumes	§10.1	Vol. VI
Diagrams consolidated	—	Vol. VII

DIAGRAM INVENTORY (Volume III)

Fig.	Title	Mermaid type	Section
1	Asset lifecycle	flowchart	1.2
2	Market-structure overview	flowchart	1.3
3	Venue-strategy decision tree	flowchart	2.2
4	Multi-jurisdiction venue map	flowchart	2.3
5	Trading-model comparison	flowchart	3.2
6	Hybrid off-chain matching, on-chain settlement	flowchart	3.3
7	Order lifecycle with pre-trade compliance	sequenceDiagram	4.2
8	Matching-engine architecture	flowchart	4.3
9	Atomic DvP settlement sequence	sequenceDiagram	5.2
10	Failed-trade / settlement-exception handling	flowchart	5.3
11	Liquidity sources & provision	flowchart	6.2

Fig.	Title	Mermaid type	Section
12	Market-surveillance architecture	flowchart	7.3
13	Point-of-trade conduct & suitability flow	flowchart	8.2
14	Secondary-transfer compliance enforcement	flowchart	9.2
15	Participant connectivity & onboarding	flowchart	10.3

Volume VII consolidates all diagrams across volumes.

END OF VOLUME III (interim draft)

Next: Volume IV — Financial Intelligence (valuation, NAV models, analytics). Before final delivery, all seven volumes undergo a single cross-volume Compliance & Completeness Audit; forward references are resolved; registers are re-checked; and the package is compiled to `.docx` on explicit request.

VOLUME IV — FINANCIAL INTELLIGENCE

Institutional Digital Real Estate Capital Markets Infrastructure

Multi-Volume Documentation Package — Volume IV of VII

TITLE PAGE & DOCUMENT CONTROL

Field	Detail
Document	Volume IV — Financial Intelligence (Valuation, NAV, Risk & Model Governance)
Package	Institutional Digital Real Estate Capital Markets Infrastructure (7 volumes)
Status	Working draft for internal review and valuation/model-risk/AI-governance sign-off — **not a valuation report, model specification, or validation in this form**
Version	IV-0.1 (interim; full cross-volume Compliance & Completeness Audit pending completion of Volume VII)
Date of documentation	30 June 2026

Field	Detail
Classification	Confidential — Draft
Companion volumes	Vol. I (legal), Vol. II (technical — oracle/NAV layer), Vol. III (marketplace — pricing/data)

Authorship and reliance caveat (read first). This volume is an AI-assisted design document prepared to institutional standards of rigour. Valuation standards, AI-governance frameworks, regulatory timelines, and model identifiers cited here were checked against official or primary sources **as of 30 June 2026** and footnoted. It remains a draft and **must be reviewed and validated by qualified RICS-registered valuers, model-risk and validation specialists, and AI-governance/legal advisers before any reliance, valuation, model deployment, or capital decision.** Nothing here is a valuation, investment advice, or a representation of any model's accuracy; all valuations must be produced by qualified valuers under the applicable standards, and all models must be independently validated.

On "latest releases." Valuation standards and AI-governance rules have changed materially in the last 18 months. Every load-bearing standard, framework edition, and regulatory date in this volume was re-verified against the standard-setter or regulator on the date of documentation and recorded in **Appendix A — Standards & Frameworks Register**; it must be re-checked before reliance.

HOW TO READ THIS VOLUME (CONTROL FILE)

Condensed Control File, reproduced atop every volume after Volume I.

Canonical terms (do not substitute synonyms). The instrument is a **ledger-based security** (Vol. I §4.1) implemented as an **ERC-3643 permissioned token** (Vol. II §3). "Valuation" means an assessment of value by a qualified valuer under recognised standards; "NAV" (net asset value) is the per-unit value used for pricing, reporting and distributions. "Model" means any quantitative or AI/ML method that produces an estimate or decision input. "LLM" means a large language model. "The platform" denotes the infrastructure as a whole.

Cross-volume reference map.

Volume	Scope	Relationship to this volume
I	Executive & Regulatory	Supplies disclosure, data-protection, and fair-value/reporting obligations
II	Technical Architecture	Supplies the oracle/data layer (§5) that delivers valuation/NAV/reserve data on-chain

Volume	Scope	Relationship to this volume
III	Marketplace & Trading	Consumes valuation/NAV for pricing, market data and surveillance
IV	**Financial Intelligence (this volume)**	**Valuation, NAV, risk models, AI/ML, model governance, LLM policy**
V	Security & Operations	Operational controls and resilience for the model/data platform
VI	Business & Financial Model	Consumes valuation/NAV and risk outputs for the financial model
VII	Architecture Atlas	Consolidates this volume's diagrams

Rule set (unchanged). No fabricated facts or citations; standards/framework editions and regulatory dates verified against primary sources and registered in Appendix A; design options labelled with trade-offs; commentary paraphrased; hyperlinks only to official sources verified live on the date of documentation, all other sources cited by stable identifier.

DETAILED TABLE OF CONTENTS

- Principles & the Intelligence Architecture
- Valuation Foundations & Standards (IVS 2025, RICS Red Book 2025)
- NAV Computation & the Oracle Pipeline
- Discounted-Cash-Flow & Income Modelling
- Risk Modelling & Monte Carlo Simulation
- Automated Valuation & Machine-Learning Models
- Explainability & Model Cards
- Model Governance & Model-Risk Management
- AI Regulatory Alignment (EU AI Act, NIST AI RMF, ISO/IEC 42001)
- Large-Language-Model Usage Policy
- Data Architecture for Intelligence
- Limitations & Threats Register

59. Interim Compliance & Completeness Audit (Volume IV)
60. Future Jurisdiction & Technology Compatibility Notes
61. Glossary
62. Appendices A–E
63. Diagram Inventory

LIST OF FIGURES

Figure	Title	Section
1	Financial-intelligence architecture (data → model → decision → disclosure)	1.3
2	Valuation approaches & bases of value	2.2
3	NAV computation & oracle pipeline	3.2
4	DCF model structure	4.2
5	Sensitivity / tornado view	4.3
6	Monte Carlo simulation flow	5.2
7	Risk-metric distribution (VaR / expected shortfall)	5.3
8	Machine-learning model pipeline	6.2
9	Explainability (SHAP) & model card	7.2
10	Model lifecycle & three lines of defence	8.2
11	AI Act risk-tier mapping	9.2
12	LLM control flow (retrieval-grounded, human-in-loop)	10.3
13	Data architecture for intelligence	11.2

LIST OF TABLES

Table	Title	Section
1	Intelligence principles → mechanisms	1.4
2	Valuation approaches & applicability	2.3
3	DCF inputs & sources	4.2
4	Risk metrics & uses	5.3
5	Model types across the platform	6.1
6	Model-card contents	7.3
7	Model-risk-management controls	8.3
8	Platform AI uses → EU AI Act risk tier & obligations	9.2

Table	Title	Section
9	LLM risks → controls	10.2
10	Financial-intelligence threats & limitations register	12.1

EXECUTIVE SUMMARY

A tokenised security inherits the valuation problem of its underlying asset, plus the model-governance problem of every estimate and AI system used to value, price, and analyse it. This volume specifies the platform's **financial-intelligence** layer — how value is assessed, how net asset value reaches the chain, how risk is modelled, how machine-learning and large-language-model systems are used, and, above all, how all of this is **governed** so that an institution and its regulators can trust the numbers.

Five decisions frame the volume. **First, standards-anchored valuation.** Real-estate value is assessed under the **International Valuation Standards (IVS), 2025 edition (effective 31 January 2025)** and the **RICS Valuation – Global Standards (Red Book), 2025 edition (effective 31 January 2025)** — both of which, for the first time, contain dedicated valuation-model standards (IVS 105; RICS VPS 5) and explicit expectations for the governed use of AI and automated valuation models with human oversight.[183][184] **Second, NAV as an oracle-delivered fact.** Valuation produces a net asset value that reaches the chain only through the decentralised oracle/NAV layer of Volume II §5, with proof-of-reserve gating where the model is asset-backed. **Third, quantitative rigour with honesty about uncertainty.** Discounted-cash-flow and comparable methods are complemented by **Monte Carlo simulation** and scenario/stress analysis, with the limits of every model stated rather than hidden. **Fourth, model governance by construction.** Every model — statistical, ML, or LLM — lives inside a model-risk-management framework (development, independent validation, ongoing monitoring; three lines of defence) aligned to **ISO/IEC 42001**, the **NIST AI Risk Management Framework** (and its 2024 Generative AI Profile), and the **EU AI Act (Regulation (EU) 2024/1689)**.[185][186][187] **Fifth, a disciplined LLM policy.** LLMs are used for drafting, document analysis and Q&A — never as an autonomous decision-

[183] IVSC — International Valuation Standards (IVS) 2025 edition; published 31 January 2024, effective 31 January 2025; introduces IVS 104 (Data & Inputs) and IVS 105 (Valuation Models) and expanded ESG content. Verified live 30 Jun 2026: https://ivsc.org/new-edition-of-the-international-valuation-standards-ivs-published/

[184] RICS — Valuation – Global Standards (Red Book), 2025 edition, effective 31 January 2025; incorporates IVS; new VPS 5 (Valuation Models); permits governed use of AI/AVMs with human oversight; VPGA 1 references IFRS 13 (fair value). Verified live: https://www.rics.org/profession-standards/rics-standards-and-guidance/sector-standards/valuation-standards/red-book/red-book-global

maker over money — with retrieval-grounding, human-in-the-loop review, and controls against hallucination, prompt injection, and data leakage.

The chapters develop the intelligence architecture; valuation foundations and standards; NAV and the oracle pipeline; DCF and income modelling; risk modelling and Monte Carlo; automated valuation and ML; explainability and model cards; model governance and model-risk management; AI regulatory alignment; the LLM usage policy; the data architecture; and an honest threats register. Open items and limitations are gathered in the Interim Audit and §12.

CHAPTER 1 — PRINCIPLES & THE INTELLIGENCE ARCHITECTURE

1.1 What “financial intelligence” means here

Financial intelligence is everything the platform does to turn raw inputs (rents, comparables, market data, reserves, bank events) into trustworthy outputs (valuations, NAV, risk metrics, analytics, disclosures). Its defining requirement is **trust**: the numbers feed pricing (Vol. III), distributions and minting (Vol. II), reporting (Vol. I), and the financial model (Vol. VI), so an error or an ungoverned model propagates directly into investor outcomes and regulatory exposure. The layer is therefore designed around **standards-anchored valuation** and **model governance by construction** — the same philosophy as the rest of the platform: controls are built into the pipeline, not bolted on after.

---

[185] ISO/IEC 42001:2023 — Artificial intelligence management system (AIMS); certifiable management-system standard complementary to the NIST AI RMF. Cited by identifier.

[186] NIST — AI Risk Management Framework (AI RMF 1.0; Govern/Map/Measure/Manage) and the Generative AI Profile (NIST AI 600-1, released July 2024) identifying LLM-specific risk categories (e.g. confabulation/hallucination, prompt injection, data poisoning, over-reliance). Verified live: https://www.nist.gov/itl/ai-risk-management-framework

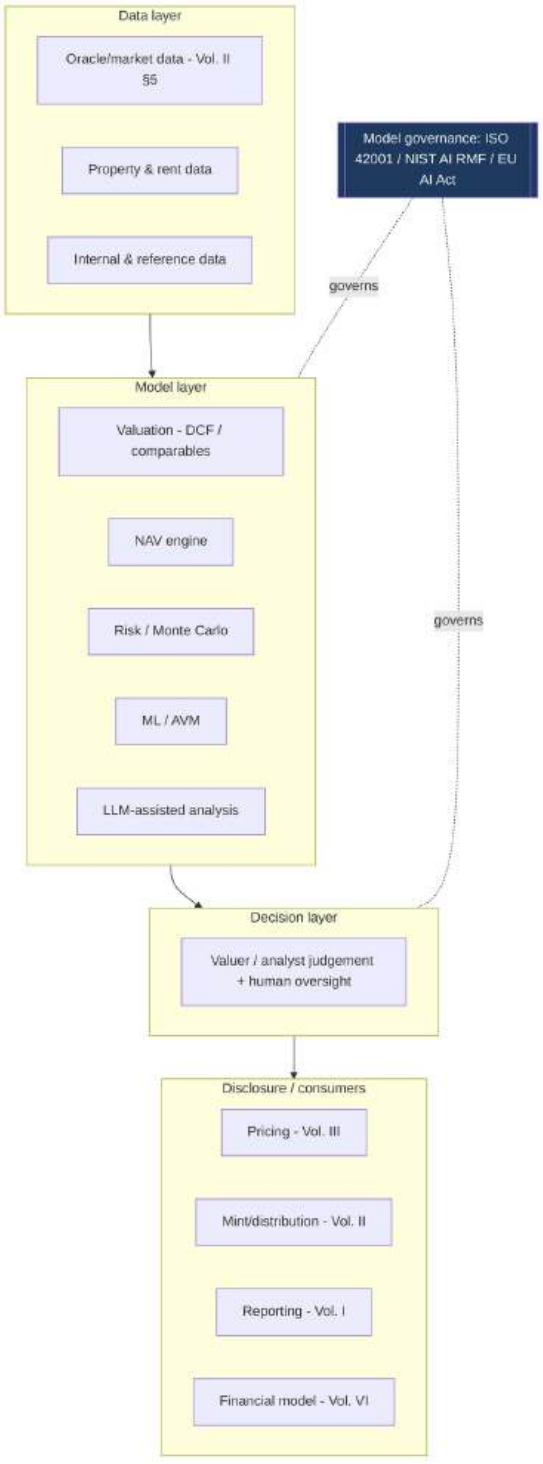
[187] European Commission — EU AI Act (Regulation (EU) 2024/1689): risk-based framework; prohibited practices/AI literacy from 2 Feb 2025; GPAI obligations from 2 Aug 2025; high-risk (Annex III) originally from 2 Aug 2026 and being deferred under the 2026 “Digital Omnibus” simplification (politically agreed May 2026, proceeding through adoption); penalties up to €35m/7% turnover; extraterritorial. Verified live: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

1.2 The intelligence is a pipeline, not a black box

Every output is the end of a traceable chain: **data → model → decision → disclosure**, with governance wrapped around all four. Data has lineage and quality controls (IVS 104; §11); models are selected, validated and monitored (IVS 105; §8); decisions involve professional judgement and human oversight; and disclosures are made to investors and regulators. Nothing in the chain is permitted to be an unexplained black box — a requirement of both the valuation standards and the AI-governance frameworks.

1.3 The architecture

Figure 1 — Financial-intelligence architecture (data → model → decision → disclosure).



Data flows through models to human-supervised decisions and then to disclosures; a governance layer wraps the model and decision stages so every number is traceable, validated, and explainable.

1.4 Principles and mechanisms

Principle	Mechanism	Reference
Standards-anchored valuation	IVS 2025 + RICS Red Book 2025; qualified valuers	§2
NAV as an oracle-delivered fact	Decentralised oracle/NAV layer; proof-of-reserve	§3; Vol. II §5
Honesty about uncertainty	Sensitivity, scenarios, Monte Carlo; stated model limits	§4–5, §12
Model governance by construction	MRM lifecycle; three lines of defence; ISO 42001 / NIST AI RMF	§8
Explainability	SHAP/feature importance; model cards; IVS 105 transparency	§7
Human-in-the-loop	No autonomous AI decisions over money; valuer/analyst judgement	§8, §10
Data quality & lineage	IVS 104 data standards; lineage; quality controls	§11
Regulatory alignment	EU AI Act risk tiers; reporting; data protection	§9; Vol. I

Table 1 — Intelligence principles → mechanisms.

CHAPTER 2 — VALUATION FOUNDATIONS & STANDARDS

2.1 Why standards come first

A tokenised real-estate security is only as credible as the valuation of the asset behind it. The platform therefore anchors all valuation to the two recognised global standards, both of which were updated to new editions effective **31 January 2025**: the **International Valuation Standards (IVS) 2025** (set by the IVSC) and the **RICS Valuation – Global Standards (Red Book) 2025**, which incorporates IVS in full.[188][189]

[188] IVSC — International Valuation Standards (IVS) 2025 edition; published 31 January 2024, effective 31 January 2025; introduces IVS 104 (Data & Inputs) and IVS 105 (Valuation Models) and expanded ESG content. Verified live 30 Jun 2026: https://ivsc.org/new-edition-of-the-international-valuation-standards-ivs-published/

[189] RICS — Valuation – Global Standards (Red Book), 2025 edition, effective 31 January 2025; incorporates IVS; new VPS 5 (Valuation Models); permits governed use of AI/AVMs with human oversight; VPGA 1 references IFRS 13 (fair value). Verified live: https://www.rics.org/profession-standards/rics-standards-and-guidance/sector-standards/valuation-standards/red-book/red-book-global

Two features of these new editions matter directly to a technology platform: each now contains a dedicated **valuation-model standard** (IVS 105 Valuation Models; RICS VPS 5 Valuation Models), and each addresses the **governed use of technology, AI and automated valuation models (AVMs)** — permitting them, but requiring appropriate governance, data quality, transparency, and **human professional judgement**, and cautioning against over-reliance on technology.[190][191] This is the standard-setters meeting the platform where it operates.

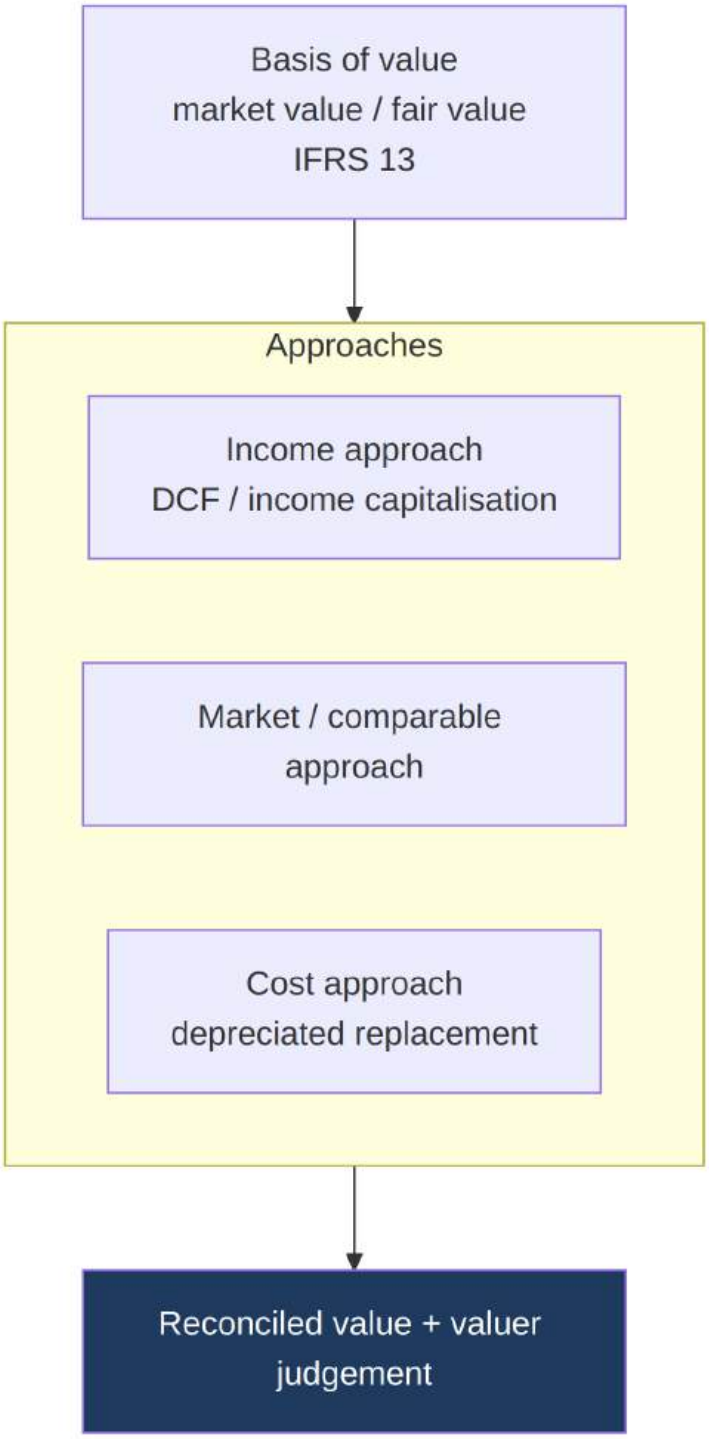
2.2 Bases of value and the three approaches

A valuation must state its **basis of value** (e.g. *market value*, or *fair value* — including fair value for financial reporting under **IFRS 13**, referenced by RICS VPGA 1) and the **approach/method** used. The three classical approaches are the income approach (including discounted cash flow), the market/comparable approach, and the cost approach.

Figure 2 — Valuation approaches and bases of value.

[190] IVSC — International Valuation Standards (IVS) 2025 edition; published 31 January 2024, effective 31 January 2025; introduces IVS 104 (Data & Inputs) and IVS 105 (Valuation Models) and expanded ESG content. Verified live 30 Jun 2026: https://ivsc.org/new-edition-of-the-international-valuation-standards-ivs-published/

[191] RICS — Valuation – Global Standards (Red Book), 2025 edition, effective 31 January 2025; incorporates IVS; new VPS 5 (Valuation Models); permits governed use of AI/AVMs with human oversight; VPGA 1 references IFRS 13 (fair value). Verified live: https://www.rics.org/profession-standards/rics-standards-and-guidance/sector-standards/valuation-standards/red-book/red-book-global



The valuer selects approach(es) appropriate to the asset and basis, then reconciles to a value using professional judgement — the standards require the model to serve judgement, not replace it.

2.3 Applicability to the platform's assets

Approach	How it works	Best for	Platform use
Income / DCF	Discount projected net cash flows to present value	Income-producing real estate (rental)	Primary for Model A assets and Model B completed assets (§4)
Income capitalisation	Capitalise stabilised net income at a market yield	Stabilised, steady-income assets	Cross-check to DCF
Market / comparable	Derive value from comparable transactions	Assets with active comparable markets	Cross-check; AVM candidate (§6)
Cost / depreciated replacement	Land + depreciated rebuild cost	Specialised assets; new build	Model B development context; insurance

Table 2 — Valuation approaches and applicability. For the platform's income-producing real estate, the **income/DCF approach is primary**, cross-checked against the comparable approach where data allows. Independent, qualified (e.g. RICS-registered) valuers produce the valuations; the platform's models support, document, and operationalise those valuations but do not substitute for the valuer's signed opinion. Where automated models (§6) are used, they are governed under VPS 5 / IVS 105 with human oversight.

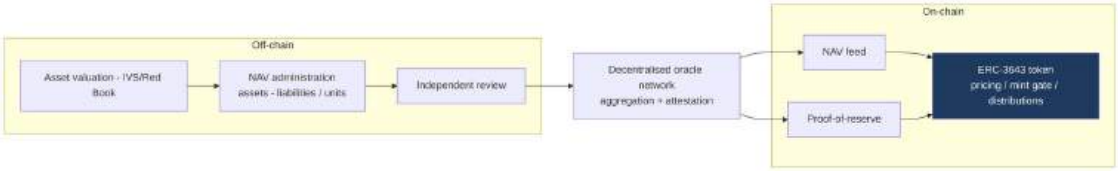
CHAPTER 3 — NAV COMPUTATION & THE ORACLE PIPELINE

3.1 From valuation to NAV to the chain

A valuation of the asset feeds a **net asset value (NAV)** for the security: broadly, the value of assets less liabilities, divided by units outstanding, computed at a stated frequency and basis. NAV is the number that prices the token (Vol. III), drives distributions and (for asset-backed Model A) gates minting (Vol. II §3.3). Because the chain is deterministic and isolated (Vol. II §5), NAV must be delivered on-chain through the **decentralised oracle/NAV layer** rather than written by a single trusted party — and, for asset-backed tokens, reinforced by **proof-of-reserve** so that supply cannot exceed verified backing.

3.2 The NAV pipeline

Figure 3 — NAV computation and oracle pipeline.



Valuation feeds NAV administration and independent review off-chain; the oracle network attests and delivers NAV (and proof-of-reserve) on-chain, where it prices the token and gates minting and distributions. No single party writes NAV directly to the chain.

3.3 Frequency, basis and controls

NAV frequency is a product decision (Vol. I Ch. 3, Vol. VI): periodic (e.g. quarterly) for illiquid real estate, with interim indicative marks where appropriate. Controls include a documented NAV policy (basis, sources, frequency, error-correction), independent review/administration, oracle deviation thresholds and staleness checks with **circuit breakers** (Vol. II §5.3), and full audit trails. A NAV error-correction and restatement procedure is defined so that a mispriced NAV is detected, corrected, disclosed, and — where investors transacted on it — remediated per policy and regulation.

CHAPTER 4 — DISCOUNTED-CASH-FLOW & INCOME MODELLING

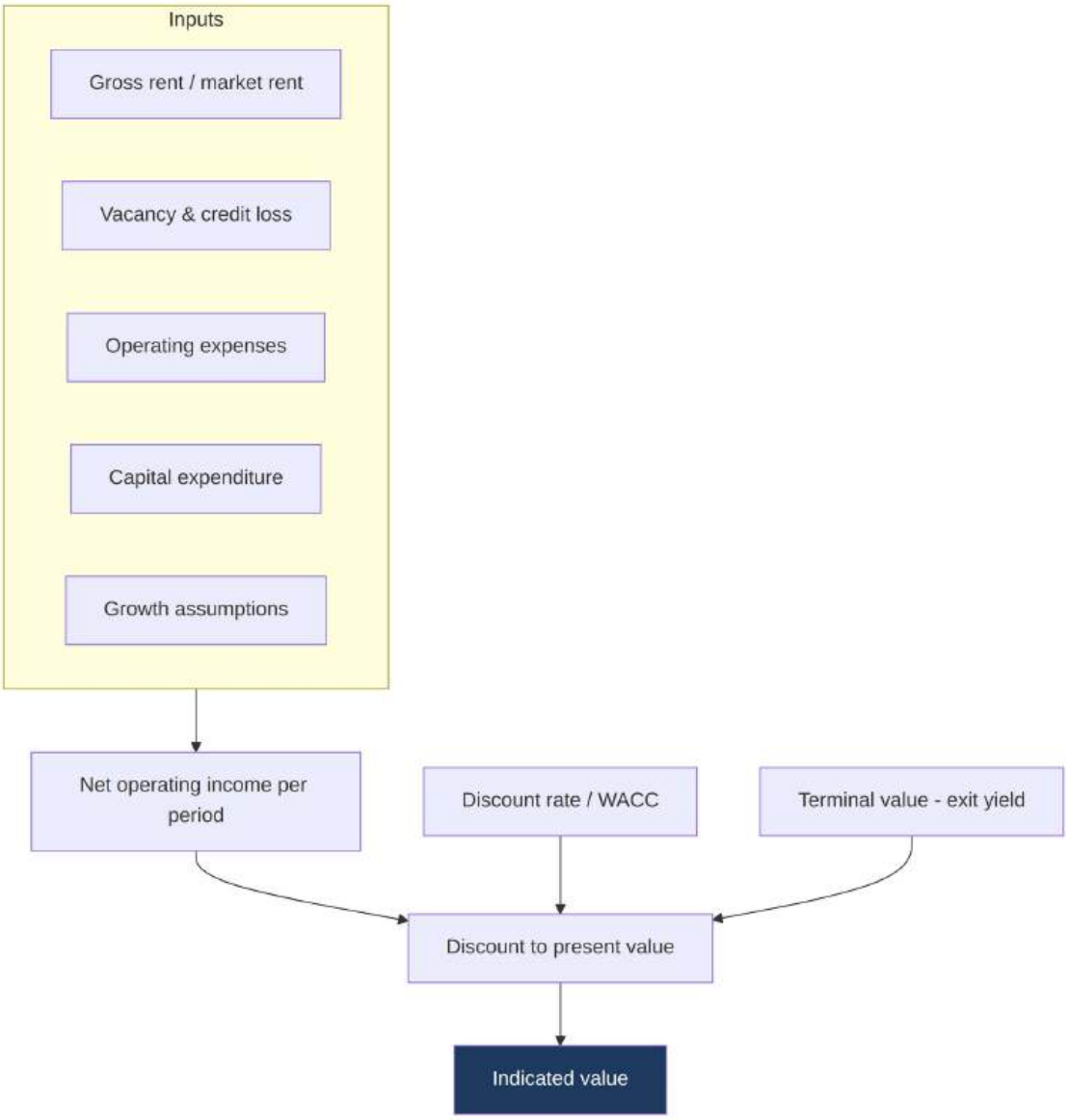
4.1 The role of DCF

For income-producing real estate, the **discounted-cash-flow (DCF)** model is the workhorse: it projects the asset's net cash flows over a holding period, adds a terminal value, and discounts everything to present value at a rate reflecting the time value of money and risk. RICS provides dedicated practice material on the governed use of DCF; the platform follows it, treating DCF as a model under IVS 105 / VPS 5 — selected for fitness, fed quality data (IVS 104), documented, and subject to professional judgement rather than mechanical output.[192]

4.2 Model structure and inputs

Figure 4 — DCF model structure.

[192] RICS — Valuation – Global Standards (Red Book), 2025 edition, effective 31 January 2025; incorporates IVS; new VPS 5 (Valuation Models); permits governed use of AI/AVMs with human oversight; VPGA 1 references IFRS 13 (fair value). Verified live: https://www.rics.org/profession-standards/rics-standards-and-guidance/sector-standards/valuation-standards/red-book/red-book-global



The DCF turns rent and cost assumptions into periodic net operating income, adds a terminal value, and discounts to a present value; each input is an explicit, sourced, challengeable assumption.

Input	Typical source	Sensitivity
Market rent / rent roll	Lease data; market evidence; comparables	High
Vacancy & credit loss	Market data; tenant covenant	Medium
Operating expenses	Historic actuals; budgets	Medium
Capital expenditure	Building surveys; plans	Medium

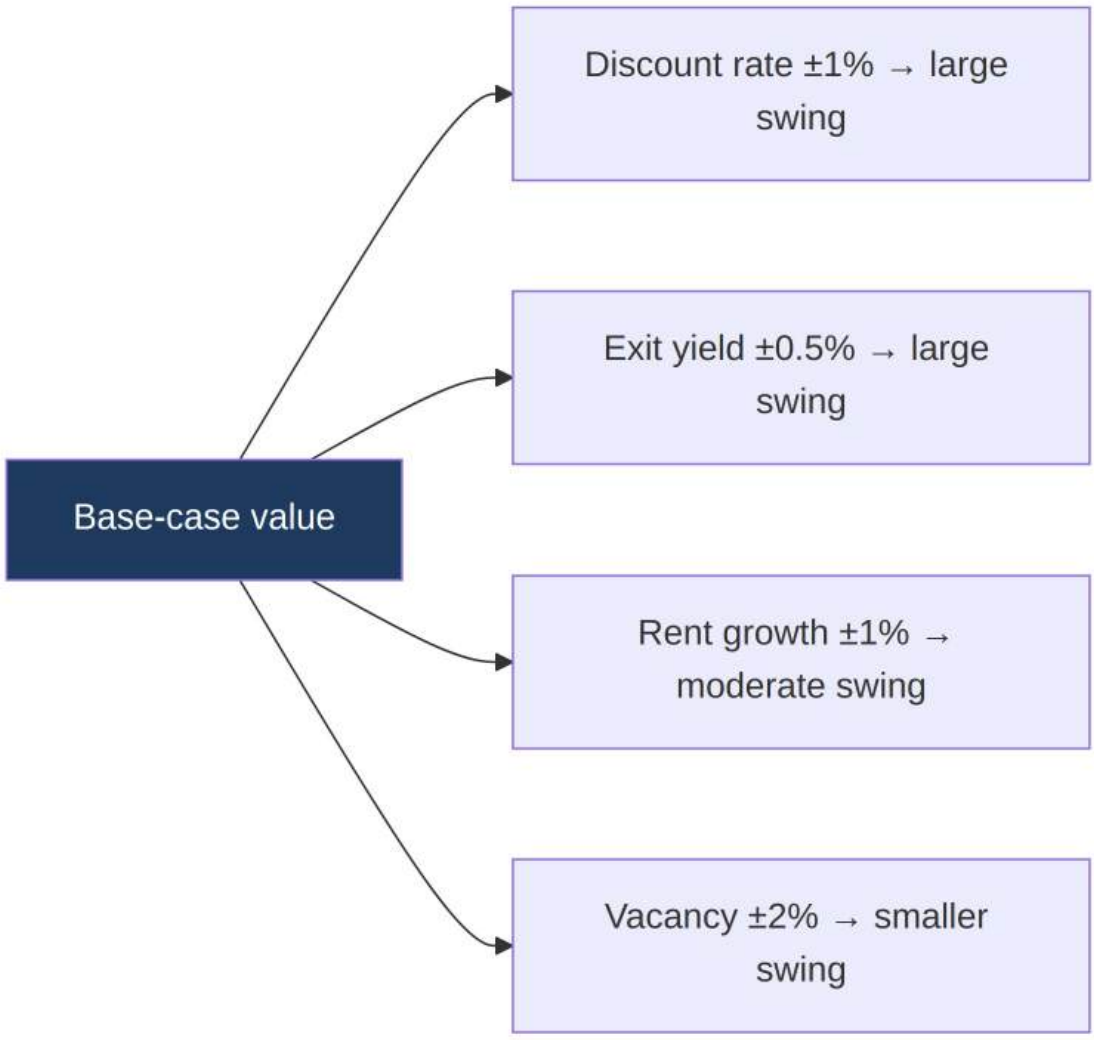
Input	Typical source	Sensitivity
Discount rate	Market-derived; risk build-up	Very high
Terminal / exit yield	Comparable yields; market outlook	Very high

Table 3 — DCF inputs and sources.

4.3 Sensitivity and the limits of a point estimate

A single DCF value is a point estimate that hides its own uncertainty. The platform always pairs a DCF with **sensitivity analysis** — varying the highest-impact inputs (discount rate, exit yield, rent growth) to show how the value moves — and presents it transparently rather than reporting a false-precision single number.

Figure 5 — Sensitivity / tornado view.



Sensitivity makes the model's dependence on its riskiest assumptions explicit; the discount rate and exit yield typically dominate, which is why they receive the most scrutiny and disclosure. This leads naturally to full simulation (§5).

CHAPTER 5 — RISK MODELLING & MONTE CARLO SIMULATION

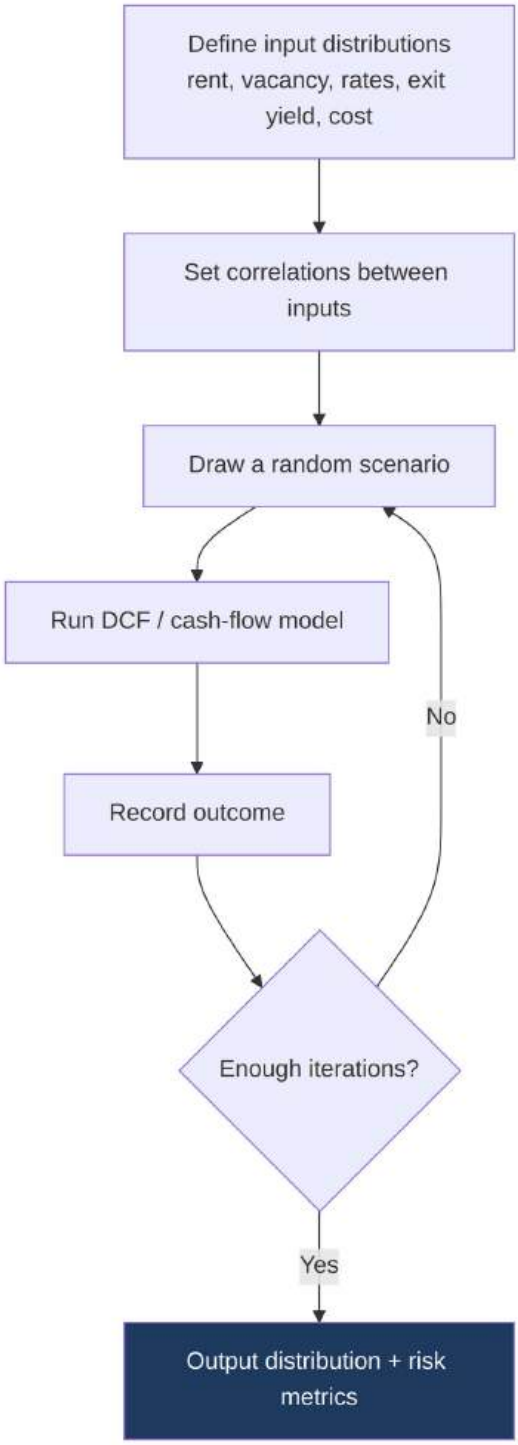
5.1 From point estimates to distributions

Sensitivity analysis (§4.3) varies one input at a time; real assets face many uncertain inputs moving together. **Monte Carlo simulation** addresses this by assigning probability distributions to the key inputs (rent growth, vacancy, discount rate, exit yield,

construction cost for Model B), accounting for correlations between them, and running the model thousands of times to produce a **distribution of outcomes** rather than a single value. This converts “the value is X” into “the value is most likely around X, with this probability of falling below Y” — far more honest and useful for risk management, pricing, and disclosure.

5.2 The simulation flow

Figure 6 — Monte Carlo simulation flow.

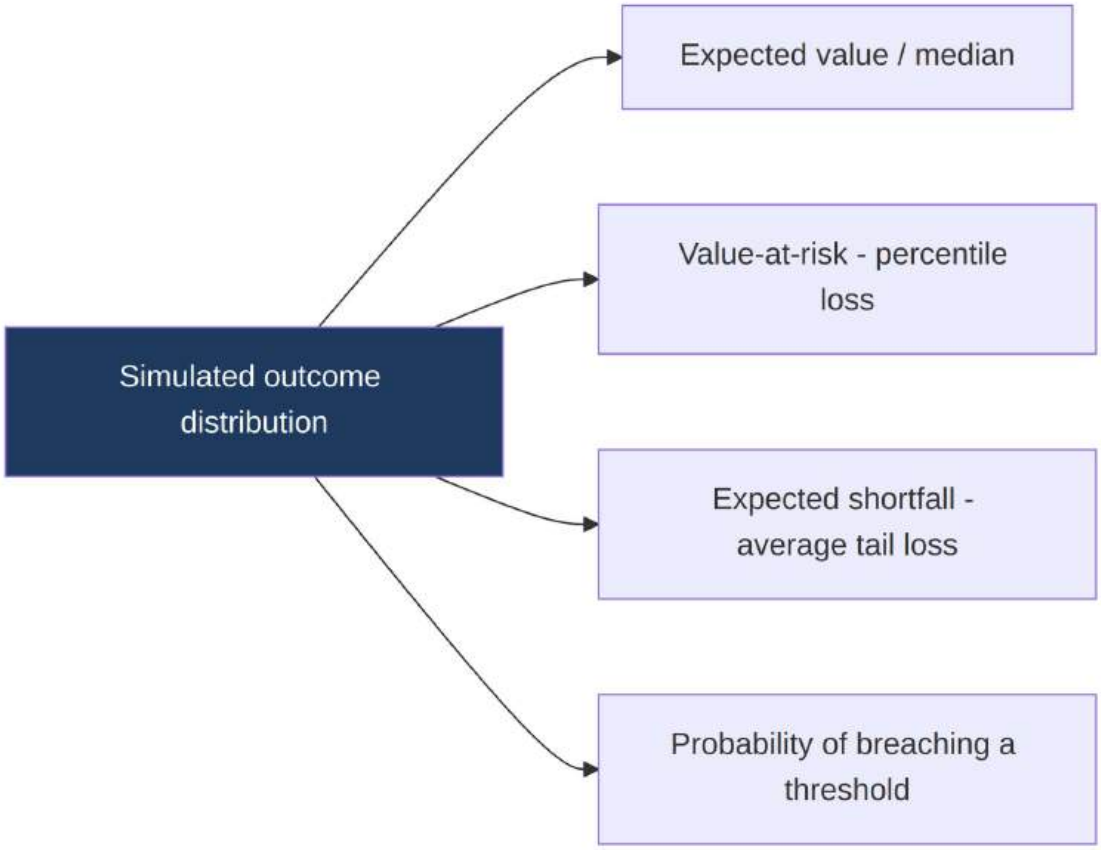


Each iteration draws a correlated scenario, runs the valuation/cash-flow model, and records the result; thousands of iterations build a distribution from which risk metrics are read.

5.3 Risk metrics and stress testing

From the simulated distribution the platform reads risk metrics, and complements them with **deterministic stress tests** (named adverse scenarios — e.g. a rate shock, a major tenant default, a construction overrun) because tail events are not always well captured by fitted distributions.

Figure 7 — Risk-metric distribution (VaR / expected shortfall).



Risk is summarised by central tendency and by tail measures; expected shortfall is preferred over value-at-risk alone because it describes the severity of the tail, not just its threshold.

Metric	What it tells you	Use
Expected value / median	Central outcome	Pricing, base-case NAV context
Value-at-risk (VaR)	Loss not exceeded at a confidence level	Risk limits, disclosure
Expected shortfall (ES)	Average loss in the tail beyond VaR	Tail-risk management
Probability of threshold breach	Chance of falling below a key level	Covenant / distribution decisions

Metric	What it tells you	Use
Stress-scenario outcomes	Impact of named adverse events	Resilience, capital planning (Vol. VI)

Table 4 — Risk metrics and uses. All risk models carry the same governance as valuation models (§8) and the same honesty caveat (§12): a simulation is only as good as its distributions and correlations, which are themselves assumptions.

CHAPTER 6 — AUTOMATED VALUATION & MACHINE-LEARNING MODELS

6.1 Where ML helps — and where it does not

Machine learning can add value in specific, bounded places: **automated valuation models (AVMs)** for indicative pricing and cross-checking; comparable selection and adjustment; rent and vacancy prediction; anomaly detection in data and surveillance (Vol. III §7); and document/data extraction. It does **not** replace the qualified valuer's signed opinion — both IVS 2025 and the RICS Red Book 2025 permit AVMs and AI only with appropriate governance, data quality, transparency, and human oversight, and warn against over-reliance.[193][194] The platform's stance: ML informs and accelerates; humans decide; everything is governed (§8).

Model type	Example use	Human oversight
AVM (hedonic / gradient-boosted)	Indicative value; cross-check to DCF	Valuer reviews; not a standalone valuation
Comparable selection	Rank/adjust comparables	Analyst confirms
Rent / vacancy forecast	DCF input support	Reviewed assumption
Anomaly detection	Data quality; market surveillance	Analyst triage
Document extraction	Lease/contract data capture	Verified against source

[193] IVSC — International Valuation Standards (IVS) 2025 edition; published 31 January 2024, effective 31 January 2025; introduces IVS 104 (Data & Inputs) and IVS 105 (Valuation Models) and expanded ESG content. Verified live 30 Jun 2026: https://ivsc.org/new-edition-of-the-international-valuation-standards-ivs-published/

[194] RICS — Valuation – Global Standards (Red Book), 2025 edition, effective 31 January 2025; incorporates IVS; new VPS 5 (Valuation Models); permits governed use of AI/AVMs with human oversight; VPGA 1 references IFRS 13 (fair value). Verified live: https://www.rics.org/profession-standards/rics-standards-and-guidance/sector-standards/valuation-standards/red-book/red-book-global

Table 5 — Model types across the platform.

6.2 The ML pipeline

ML models follow a disciplined pipeline with validation and monitoring built in — not a one-off training exercise. Data is sourced and quality-checked (IVS 104; §11), features are engineered with documented lineage, models are trained and **validated on held-out and out-of-time data**, deployed behind the governance gate (§8), and **monitored for drift** so that a model whose performance decays is caught and retrained or retired.

Figure 8 — Machine-learning model pipeline.

Validation and monitoring are first-class stages; a model is never "finished," it is registered, deployed under governance, and watched for drift, with a path back to retraining.

6.3 Accuracy, data and honest limits

AVM and ML accuracy depends on data density and market homogeneity — both often weak for heterogeneous commercial real estate, where comparable sales are sparse and each asset is idiosyncratic. The platform therefore (a) reports AVM outputs with **confidence/accuracy measures**, never as bare point values; (b) uses ML as a **cross-check and accelerant**, not the primary valuation for material assets; and (c) discloses where a value rests on a model versus a full valuer inspection. These limits are recorded in §12 and in each model's card (§7).

CHAPTER 7 — EXPLAINABILITY & MODEL CARDS

7.1 Why explainability is non-negotiable

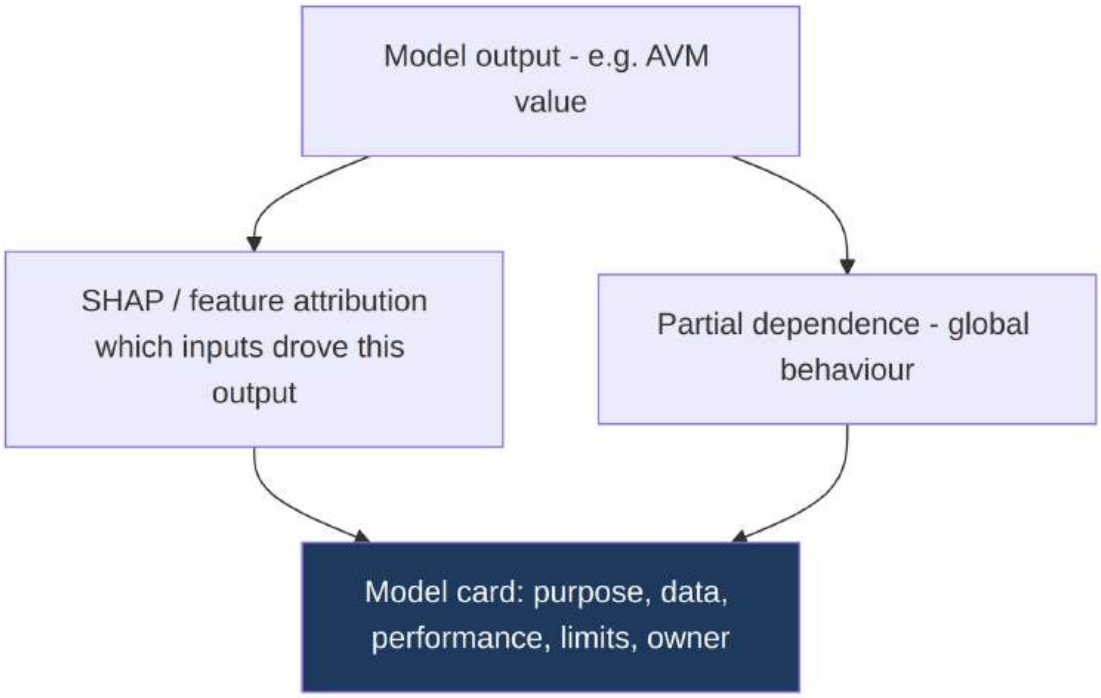
Both the valuation standards (IVS 105 / VPS 5 transparency requirements) and the AI-governance frameworks (§9) require that a model's outputs can be **explained** — to a valuer, an auditor, a regulator, and where appropriate an investor. A number nobody can explain cannot be relied upon, disclosed, or defended. Explainability is therefore a design requirement, not an optional add-on, for every model that informs a valuation, price, or eligibility-relevant decision.

7.2 Techniques

For statistical models, explainability comes from the model form itself (coefficients, elasticities, sensitivities). For ML models, the platform uses **feature-importance and**

attribution techniques such as SHAP (SHapley Additive exPlanations) to show how each input contributed to a given output, plus partial-dependence views for global behaviour. Explanations are produced and stored alongside outputs so that any value can be interrogated after the fact.

Figure 9 — Explainability (SHAP) and model card.



Per-output attribution (SHAP) and global behaviour (partial dependence) feed the model card, so both individual decisions and overall model behaviour are explainable and documented.

7.3 Model cards

Every model — statistical, ML, or an LLM-based component — has a **model card**: a standard document recording what the model is for, the data it was built on, how it performs, its known limitations, and who owns it. Model cards satisfy the documentation expectations of the valuation standards and the transparency expectations of the AI-governance frameworks (including the GPAI/transparency expectations discussed in §9), and they are the artefact a validator or regulator reads first.

Model-card section	Contents
Purpose & scope	What the model does; intended and out-of-scope uses
Data	Training/reference data, sources, quality, lineage, dates
Methodology	Model type, key assumptions, features

Model-card section	Contents
Performance	Accuracy/error metrics; validation results; out-of-time tests
Explainability	How outputs are explained (e.g. SHAP); example attributions
Limitations & risks	Known weaknesses, drift, fairness, failure modes
Governance	Owner, validation status, approval, review date, monitoring

Table 6 — Model-card contents.

CHAPTER 8 — MODEL GOVERNANCE & MODEL-RISK MANAGEMENT

8.1 Models are a managed risk

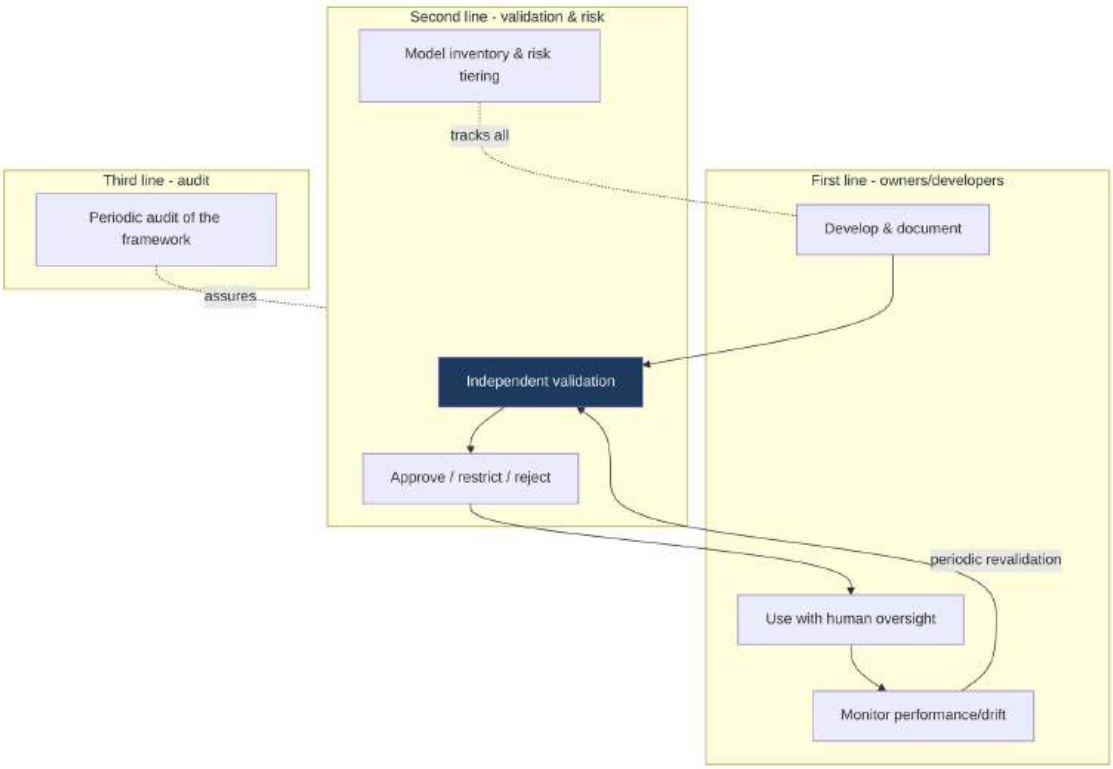
Any model can be wrong, misused, or degrade over time — "model risk." The platform manages it with a **model-risk-management (MRM)** framework in the tradition of established supervisory guidance on model risk (e.g. the principles of the US Federal Reserve/OCC guidance **SR 11-7**), extended to AI/ML via **ISO/IEC 42001** (an AI management system) and the **NIST AI Risk Management Framework** with its **Generative AI Profile** for LLM-specific risks.[195][196] The framework rests on **three lines of defence**: model owners/developers (first line), independent model validation and risk (second line), and internal audit (third line).

8.2 The model lifecycle

Figure 10 — Model lifecycle and three lines of defence.

[195] ISO/IEC 42001:2023 — Artificial intelligence management system (AIMS); certifiable management-system standard complementary to the NIST AI RMF. Cited by identifier.

[196] NIST — AI Risk Management Framework (AI RMF 1.0; Govern/Map/Measure/Manage) and the Generative AI Profile (NIST AI 600-1, released July 2024) identifying LLM-specific risk categories (e.g. confabulation/hallucination, prompt injection, data poisoning, over-reliance). Verified live: https://www.nist.gov/itl/ai-risk-management-framework



Development and use sit in the first line; independent validation, a complete model inventory, and approval sit in the second; audit assures the whole. A model is approved, used under oversight, monitored, and periodically revalidated.

8.3 Controls

Control	Purpose
Model inventory & risk tiering	Know every model; govern proportionately to risk
Independent validation	Challenge conceptual soundness, data, performance before use
Ongoing monitoring & drift detection	Catch performance decay; trigger revalidation/retirement
Documentation & model cards (§7)	Transparency, auditability, reproducibility
Bias & fairness assessment	Detect and mitigate discriminatory outcomes
Change control & versioning	Govern every change; reproducible builds (Vol. II §10)
Human-in-the-loop	No autonomous model decision over money or eligibility
Use limitations & override	Define where a model may/may not be relied on; allow expert override

Table 7 — Model-risk-management controls. The MRM framework applies uniformly to valuation models, risk/Monte Carlo models, ML/AVMs, and LLM-based components —

the governance is model-type-agnostic, while the specific tests differ (e.g. LLM evaluation and hallucination testing for §10).

CHAPTER 9 — AI REGULATORY ALIGNMENT

9.1 Three frameworks, one programme

The platform's AI and model governance is aligned to the three frameworks that now dominate practice: the **EU AI Act (Regulation (EU) 2024/1689)** — the binding, risk-based law; the **NIST AI Risk Management Framework** (Govern–Map–Measure–Manage), with its **2024 Generative AI Profile** for LLM risks — the risk methodology; and **ISO/IEC 42001:2023** — the certifiable AI management system.[197][198][199] They are complementary: ISO 42001 provides the management system, the NIST AI RMF the risk methodology, and the EU AI Act the legal obligations. The platform uses ISO 42001 as the management-system spine, the NIST AI RMF (and GenAI Profile) as the working methodology, and maps both onto the EU AI Act's obligations.

[197] European Commission — EU AI Act (Regulation (EU) 2024/1689): risk-based framework; prohibited practices/AI literacy from 2 Feb 2025; GPAI obligations from 2 Aug 2025; high-risk (Annex III) originally from 2 Aug 2026 and being deferred under the 2026 "Digital Omnibus" simplification (politically agreed May 2026, proceeding through adoption); penalties up to €35m/7% turnover; extraterritorial. Verified live: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

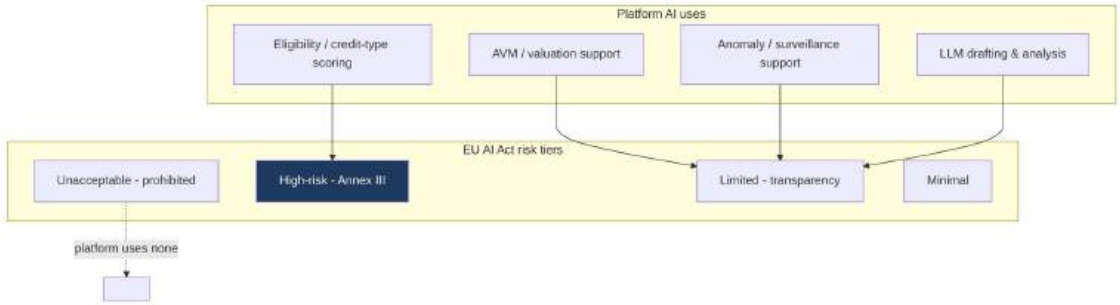
[198] NIST — AI Risk Management Framework (AI RMF 1.0; Govern/Map/Measure/Manage) and the Generative AI Profile (NIST AI 600-1, released July 2024) identifying LLM-specific risk categories (e.g. confabulation/hallucination, prompt injection, data poisoning, over-reliance). Verified live: https://www.nist.gov/itl/ai-risk-management-framework

[199] ISO/IEC 42001:2023 — Artificial intelligence management system (AIMS); certifiable management-system standard complementary to the NIST AI RMF. Cited by identifier.

9.2 Mapping the platform's AI uses to the EU AI Act

The EU AI Act is **risk-based and extraterritorial** (it applies where AI outputs are used in the EU, regardless of where the provider sits), with tiers of unacceptable, high, limited, and minimal risk, and penalties up to €35m or 7% of turnover. Its obligations phase in: **prohibited practices and AI-literacy from 2 February 2025**; **general-purpose-AI (GPAI) model obligations from 2 August 2025**; and the **high-risk (Annex III) obligations** originally from 2 August 2026 — though under the 2026 "Digital Omnibus" simplification (politically agreed in May 2026, then proceeding through adoption) the **high-risk timeline has been deferred** (reported to around December 2027 for Annex III), which the platform tracks as a live, not-yet-final change.[200]

Figure 11 — AI Act risk-tier mapping.



The platform uses no prohibited AI. Any use that scores a person's access to a financial service is treated as potentially high-risk and governed to that standard; valuation-support, surveillance-support and LLM uses are treated at least at the transparency tier, governed conservatively.

Platform AI use	Likely AI Act tier	Key obligations applied
Eligibility / creditworthiness-type scoring of individuals	High-risk (Annex III) if used to decide access	Risk management, data governance, logging, human oversight, conformity assessment, registration
AVM / valuation-support ML	Limited / minimal (decision support, human-decided)	Transparency, documentation, human oversight; governed as a model (§8)
Anomaly / market-surveillance support	Limited	Transparency, human triage, logging

[200] European Commission — EU AI Act (Regulation (EU) 2024/1689): risk-based framework; prohibited practices/AI literacy from 2 Feb 2025; GPAI obligations from 2 Aug 2025; high-risk (Annex III) originally from 2 Aug 2026 and being deferred under the 2026 "Digital Omnibus" simplification (politically agreed May 2026, proceeding through adoption); penalties up to €35m/7% turnover; extraterritorial. Verified live: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

Platform AI use	Likely AI Act tier	Key obligations applied
LLM-assisted drafting & analysis (deployer of GPAI)	Limited (Art. 50 transparency) + GPAI deployer duties	AI-generated-content transparency; use within GPAI provider terms; §10 controls

Table 8 — Platform AI uses → EU AI Act risk tier and obligations. The platform applies the **stricter applicable treatment** where a use could be classified more than one way, and documents the classification per system in the model inventory (§8). Because the high-risk timeline is in flux, the platform builds to the high-risk control set for any borderline use rather than relying on a deferral that may change.

9.3 Why conservative classification

Mis-classifying a high-risk use as low-risk is the expensive error (penalties, remediation, reputational harm). The platform therefore errs toward the stricter tier, especially for anything touching **individual access to a financial product**, and keeps the classification, evidence, and human-oversight design auditable. This is the AI analogue of the substance-over-form principle that runs through Volumes I–III.

CHAPTER 10 — LARGE-LANGUAGE-MODEL USAGE POLICY

10.1 Where LLMs are used — and the bright line

LLMs are used on the platform for **document analysis** (extracting and summarising leases, contracts, reports), **drafting** (first drafts of memos, disclosures, responses — always human-reviewed), **internal Q&A/search** over governed knowledge, and **operational assistance**. The bright line: an **LLM never autonomously makes or executes a financial, valuation, eligibility, or trading decision.** Those decisions rest with qualified humans and governed quantitative models; the LLM assists the humans. This is both a prudential choice and an alignment with the AI-governance frameworks' insistence on human oversight (§8–9).

10.2 Risks and controls

LLMs introduce distinctive risks — captured well by the NIST Generative AI Profile's categories (confabulation/hallucination, prompt injection, data leakage, IP, over-reliance, information integrity).[201] Each is met with a specific control.

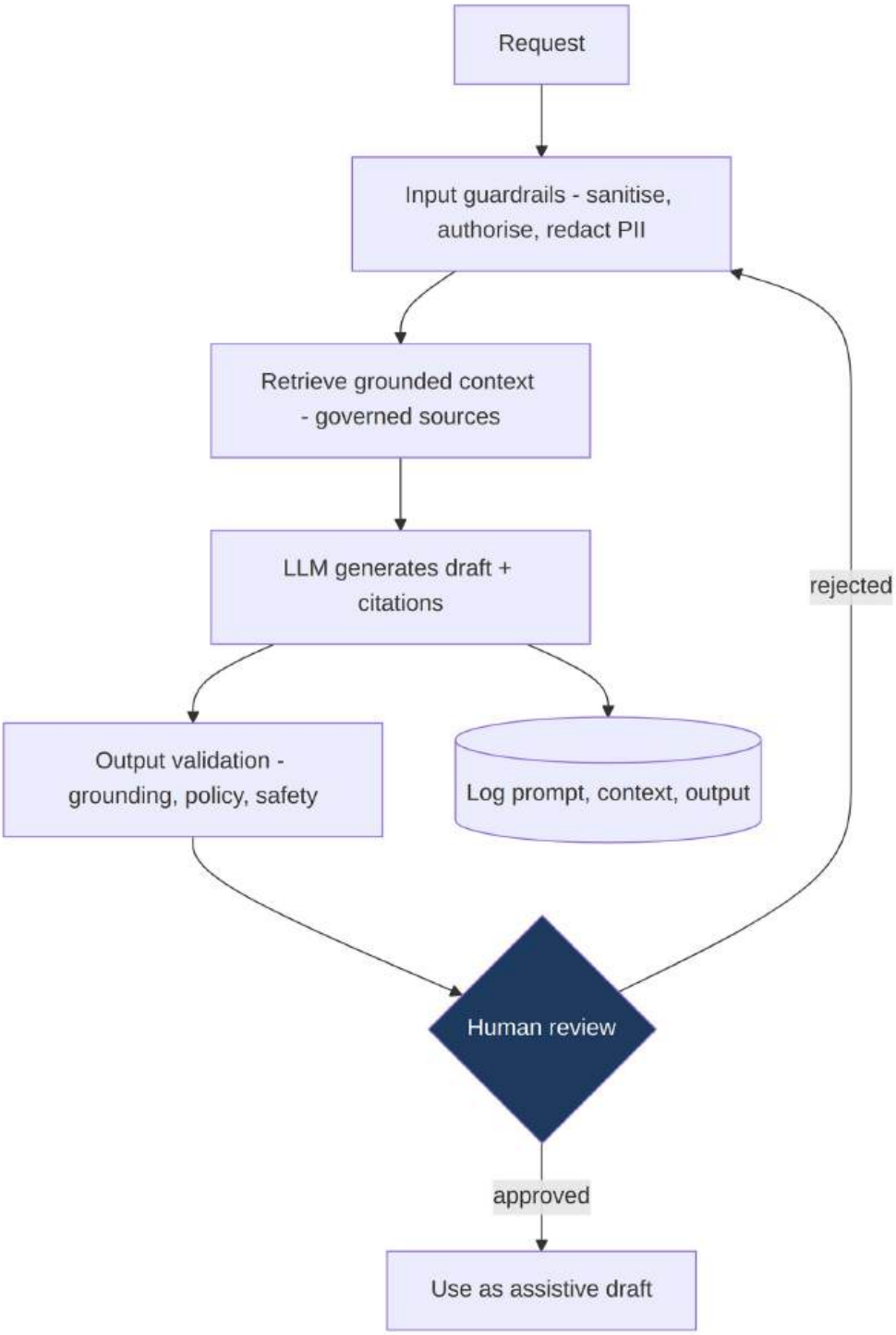
[201] NIST — AI Risk Management Framework (AI RMF 1.0; Govern/Map/Measure/Manage) and the Generative AI Profile (NIST AI 600-1, released July 2024) identifying LLM-specific risk categories (e.g. confabulation/hallucination, prompt injection, data poisoning, over-reliance). Verified live: https://www.nist.gov/itl/ai-risk-management-framework

LLM risk	Control
Hallucination / confabulation	Retrieval-grounding to authoritative sources; cite-or-abstain; human review before any external use
Prompt injection / data poisoning	Input sanitisation; untrusted-content isolation; least-privilege tool access; output validation
Data leakage / privacy	No PII or confidential data into ungoverned models; tenancy/DLP controls; redaction; on-prem/contracted models for sensitive data (Vol. I §9)
Over-reliance / automation bias	Human-in-the-loop; outputs labelled as draft/assistive; no autonomous decisions
IP / copyright	Provenance controls; respect licensing; avoid reproducing protected content
Lack of transparency	AI-generated-content disclosure (Art. 50); logging of prompts/outputs for audit
Non-determinism / inconsistency	Constrained prompts; evaluation suites; versioned model + prompt configuration

Table 9 — LLM risks → controls.

10.3 The LLM control flow

Figure 12 — LLM control flow (retrieval-grounded, human-in-the-loop).



Every LLM interaction is guard-railed on input, grounded in governed sources, validated on output, reviewed by a human, and logged — and never authorised to act on money or eligibility on its own.

10.4 Prohibited and disclosed uses

Prohibited: autonomous financial/eligibility/trading decisions; feeding PII or confidential data to ungoverned models; presenting LLM output as a valuation or as advice; using LLMs to generate content that misleads investors. Disclosed: where investors or counterparties receive materially AI-generated content, it is identified as such, consistent with the transparency obligations of the AI Act (§9). The LLM policy is itself a governed document, reviewed under the model-governance framework (§8).

CHAPTER 11 — DATA ARCHITECTURE FOR INTELLIGENCE

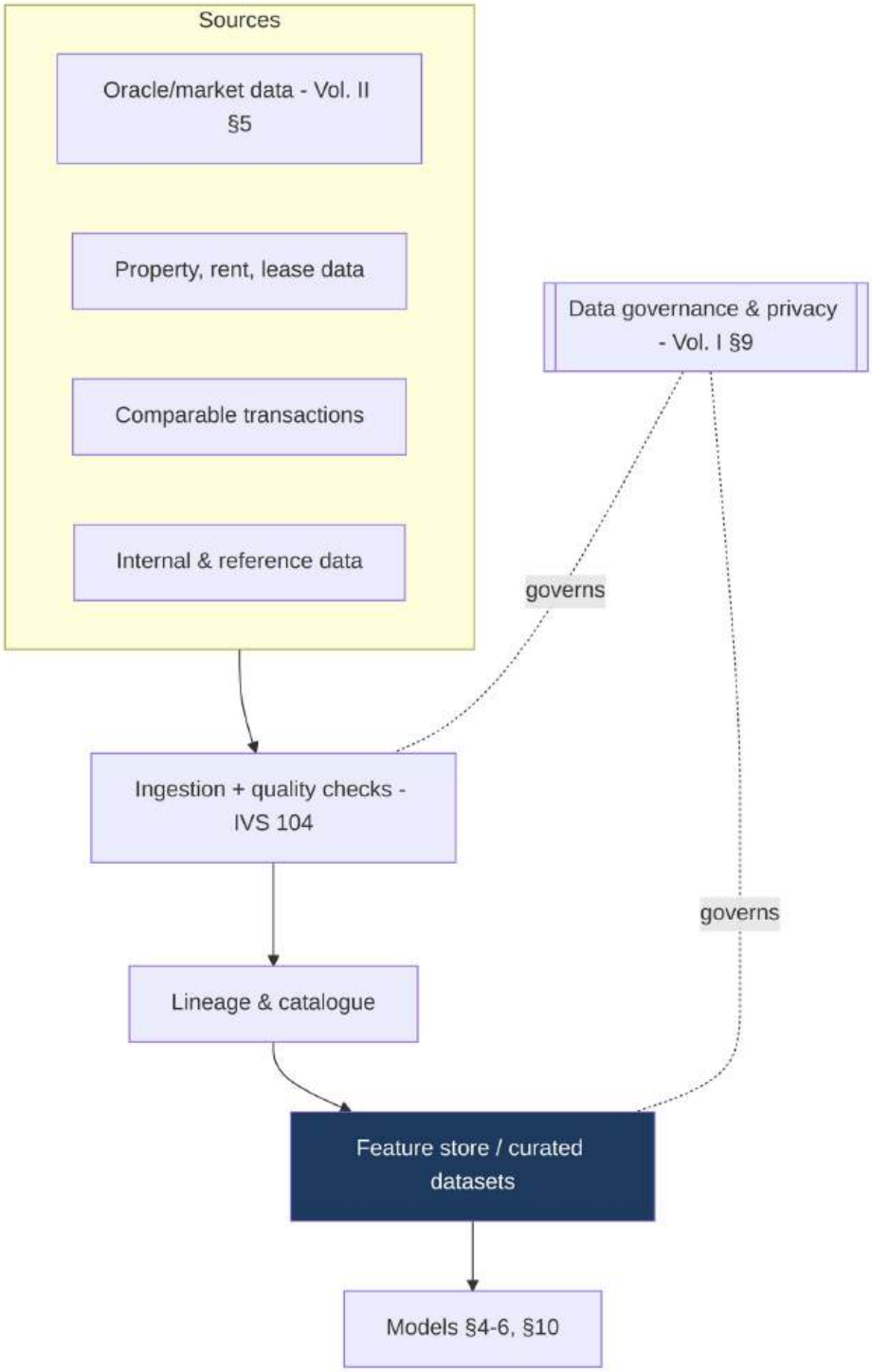
11.1 Data quality is the foundation (IVS 104)

No model is better than its data, and IVS 2025 made data a first-class concern with **IVS 104 (Data & Inputs)** — emphasising data quality, selection, and appropriateness.[202] The platform's data architecture exists to make every model input **traceable, quality-controlled, and appropriate to purpose**, and to keep personal data governed under the data-protection split established in Volume I §9 and Volume II §1.4 (personal data off-chain, never on the ledger).

11.2 The architecture

Figure 13 — Data architecture for intelligence.

[202] IVSC — International Valuation Standards (IVS) 2025 edition; published 31 January 2024, effective 31 January 2025; introduces IVS 104 (Data & Inputs) and IVS 105 (Valuation Models) and expanded ESG content. Verified live 30 Jun 2026: https://ivsc.org/new-edition-of-the-international-valuation-standards-ivs-published/



Data is ingested with quality checks, catalogued with lineage, curated into a feature store, and served to models — all under a governance and privacy layer that keeps personal data off-chain and properly controlled.

11.3 Lineage, reproducibility and privacy

Three properties are mandatory. **Lineage**: every model input can be traced to its source and transformation, so a value can be reconstructed and defended. **Reproducibility**: datasets and features are versioned with the models that use them, so a past valuation or decision can be reproduced exactly. **Privacy**: personal data is minimised, governed, and never placed on-chain or fed to ungoverned models (Vol. I §9; §10 above). Data governance is shared with the security/operations controls of Volume V.

CHAPTER 12 — LIMITATIONS & THREATS REGISTER

12.1 Honest assessment

#	Threat / limitation	Exposure	Mitigation / status
1	Valuation uncertainty / illiquid-asset subjectivity	High	Standards-anchored valuation; sensitivity + Monte Carlo; disclosure (§2, §4–5)
2	Model risk (wrong, misused, decayed)	High	MRM framework; independent validation; monitoring; three lines of defence (§8)
3	NAV error / mispricing	High	NAV policy, independent review, oracle checks, circuit breakers, restatement procedure (§3)
4	Oracle/data-source failure or manipulation	High	Decentralised feeds, thresholds, proof-of-reserve, fallback (§3; Vol. II §5)
5	AVM/ML inaccuracy on heterogeneous assets	Medium-High	Confidence measures; cross-check only; human-decided; disclosed (§6)
6	LLM hallucination / prompt injection / leakage	Medium-High	Grounding, guardrails, human-in-loop, logging; no autonomous decisions (§10)
7	EU AI Act high-risk mis-classification	Medium	Conservative classification; build to high-risk controls for borderline uses (§9)
8	AI Act timeline change (Digital Omnibus)	Medium	Track to final dates; do not rely on deferral (§9.2)

#	Threat / limitation	Exposure	Mitigation / status
9	Data quality / lineage gaps (IVS 104)	Medium	Quality checks, lineage, catalogue, feature store (§11)
10	Bias / unfair outcomes in scoring models	Medium	Fairness assessment; validation; human oversight (§8)
11	Over-reliance / automation bias by staff	Medium	Human-in-the-loop design; assistive labelling; training (§8, §10)
12	Reproducibility failure (cannot reconstruct a number)	Medium	Versioned data/models; lineage; audit trail (§11)
13	False precision in disclosure	Medium	Report ranges/uncertainty, not bare point values (§4–5)

12.2 Honest limitations

This volume specifies an intelligence and governance architecture; it does not itself value any asset, build any model, or validate any system — those are the work of qualified valuers and validators. Valuation of illiquid real estate is inherently uncertain, and no model removes that uncertainty; the platform's contribution is to make the uncertainty explicit and governed, not to eliminate it. AI/ML adds capability and new failure modes in equal measure; the platform's deliberately conservative posture (human-in-the-loop, no autonomous decisions, conservative AI Act classification) trades some automation for trustworthiness. Regulatory timelines — especially the EU AI Act high-risk schedule — are moving and must be re-checked.

INTERIM COMPLIANCE & COMPLETENESS AUDIT — VOLUME IV

Verification performed. Standards, frameworks, and regulatory dates were checked against primary sources on 30 June 2026 and recorded in Appendix A: **IVS 2025** (effective 31 Jan 2025; new IVS 104 Data & Inputs, IVS 105 Valuation Models)[203]; the **RICS Valuation – Global Standards (Red Book) 2025** (effective 31 Jan 2025; new VPS 5 Valuation Models; AI/AVM use with governance and human oversight; VPGA 1

[203] IVSC — International Valuation Standards (IVS) 2025 edition; published 31 January 2024, effective 31 January 2025; introduces IVS 104 (Data & Inputs) and IVS 105 (Valuation Models) and expanded ESG content. Verified live 30 Jun 2026: https://ivsc.org/new-edition-of-the-international-valuation-standards-ivs-published/

referencing IFRS 13)[204]; the **EU AI Act (Reg (EU) 2024/1689)** phasing (prohibited Feb 2025; GPAI Aug 2025; high-risk originally Aug 2026, deferred under the 2026 Digital Omnibus)[205]; the **NIST AI RMF** and its **July 2024 Generative AI Profile (AI 600-1)**[206]; and **ISO/IEC 42001:2023** (cited by identifier). **SR 11-7** (model-risk principles) and **IFRS 13** (fair value) are cited by stable identifier.

No fabricated identifiers. No standard edition, framework name, regulation number, or date has been invented; the in-flux EU AI Act high-risk timeline is flagged as not-yet-final rather than stated as settled.

Open / flagged items for specialist sign-off. 1. EU AI Act high-risk timeline (Digital Omnibus) — confirm final effective dates before relying on any deferral (§9.2). 2. Classification of each AI use against Annex III — confirm with AI-governance counsel; default to stricter tier (§9). 3. NAV policy (basis, frequency, error-correction/restatement) — confirm with administrator, auditor, counsel (§3). 4. Valuer engagement and AVM-use boundaries under VPS 5 / IVS 105 — confirm with RICS-registered valuers (§2, §6). 5. Model inventory, validation cadence, and independence — confirm with model-risk function (§8). 6. LLM provider terms, data residency, and sensitive-data handling — confirm with security and legal (§10–11; Vol. V).

Link policy. Hyperlinks point only to official/primary sources verified live on 30 June 2026 (IVSC, RICS, the European Commission AI Act pages, NIST). ISO/IEC 42001, SR 11-7, IFRS 13, and NIST AI 600-1 are cited by stable identifier.

---

[204] RICS — Valuation – Global Standards (Red Book), 2025 edition, effective 31 January 2025; incorporates IVS; new VPS 5 (Valuation Models); permits governed use of AI/AVMs with human oversight; VPGA 1 references IFRS 13 (fair value). Verified live: https://www.rics.org/profession-standards/rics-standards-and-guidance/sector-standards/valuation-standards/red-book/red-book-global

[205] European Commission — EU AI Act (Regulation (EU) 2024/1689): risk-based framework; prohibited practices/AI literacy from 2 Feb 2025; GPAI obligations from 2 Aug 2025; high-risk (Annex III) originally from 2 Aug 2026 and being deferred under the 2026 “Digital Omnibus” simplification (politically agreed May 2026, proceeding through adoption); penalties up to €35m/7% turnover; extraterritorial. Verified live: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

[206] NIST — AI Risk Management Framework (AI RMF 1.0; Govern/Map/Measure/Manage) and the Generative AI Profile (NIST AI 600-1, released July 2024) identifying LLM-specific risk categories (e.g. confabulation/hallucination, prompt injection, data poisoning, over-reliance). Verified live: https://www.nist.gov/itl/ai-risk-management-framework

FUTURE JURISDICTION & TECHNOLOGY COMPATIBILITY NOTES

Standards & regulatory watch items. (a) **EU AI Act** — track the Digital Omnibus to final adoption and confirm the high-risk effective dates; track GPAI codes of practice and Article 50 transparency guidance. (b) **IVS / RICS** — both update periodically; track future editions and any further AI/AVM and ESG guidance (IVS 104 ESG appendix; RICS AI and AVM material). (c) **NIST** — track new AI RMF profiles (e.g. critical-infrastructure, cyber-AI) and updates to the GenAI Profile. (d) **ISO/IEC** — track AI management-system and AI-risk standards and certification practice. (e) **Sustainability/financial reporting** — IFRS S1/S2 and ESG factors increasingly affect valuation (IVS 104; RICS VPGA), so keep the data architecture (§11) ready to capture ESG inputs.

Technology watch items. Explainability methods and LLM evaluation tooling are advancing quickly; revisit §7 and §10 controls as the state of the art and the regulatory expectations mature. Confidential-compute and privacy-preserving analytics (Vol. II §8) may allow richer modelling on sensitive data without exposing it.

GLOSSARY

Covers terms introduced in this volume; master glossary in Vol. I, technical in Vol. II. Canonical reminder: the instrument is a **ledger-based security** implemented as an **ERC-3643 permissioned token**.

- **AVM (automated valuation model)** — a model that produces an indicative property value from data; used as support/cross-check, not a standalone valuation.
- **Basis of value** — the type of value being assessed (e.g. market value, fair value).
- **DCF (discounted cash flow)** — valuing an asset by discounting its projected net cash flows to present value.
- **EU AI Act** — Regulation (EU) 2024/1689; the EU's risk-based AI law.
- **Expected shortfall (ES)** — the average loss in the tail beyond the value-at-risk threshold.
- **Fair value (IFRS 13)** — a financial-reporting measurement basis.
- **GPAI** — general-purpose AI model (e.g. a foundation model / LLM), regulated separately under the AI Act.
- **Hedonic model** — a regression that prices an asset from its characteristics.
- **ISO/IEC 42001** — the international standard for an AI management system (AIMS).

- **IVS** — International Valuation Standards (2025 edition effective 31 Jan 2025).
- **Model card** — a standard document describing a model's purpose, data, performance, limits, and governance.
- **Model risk / MRM** — the risk that a model is wrong or misused, and the framework to manage it.
- **Monte Carlo simulation** — running a model over many random, correlated scenarios to produce an outcome distribution.
- **NAV (net asset value)** — assets minus liabilities per unit; the value used for pricing, distributions, and (Model A) mint-gating.
- **NIST AI RMF** — the NIST AI Risk Management Framework (Govern–Map–Measure–Manage) and its Generative AI Profile.
- **RICS Red Book** — RICS Valuation – Global Standards (2025 edition effective 31 Jan 2025), incorporating IVS.
- **SHAP** — SHapley Additive exPlanations; a feature-attribution technique for explaining model outputs.
- **Three lines of defence** — owners (1st), independent validation/risk (2nd), audit (3rd).
- **VaR (value-at-risk)** — a loss threshold not expected to be exceeded at a stated confidence level.
- **VPS / VPGA** — RICS Valuation Technical & Performance Standards / Valuation Practice Guidance Applications.

APPENDIX A — STANDARDS & FRAMEWORKS REGISTER

Authoritative register of standards and frameworks relied on. "Verified live 30 Jun 2026" means the official source was retrieved on that date. Hyperlinks only to official sources verified live; other items cited by stable identifier. Re-check before reliance.

#	Standard / framework	Identifier / key facts (30 Jun 2026)	Official source
A1	International Valuation Standards (IVS)	2025 edition; published 31 Jan 2024, effective 31 Jan 2025; new IVS 104 (Data & Inputs), IVS 105 (Valuation Models)	IVSC — https://ivsc.org/new-edition-of-the-international-valuation-standards-ivs-published/
A2	RICS Valuation – Global Standards (Red Book)	2025 edition; effective 31 Jan 2025; incorporates IVS; new VPS 5 (Valuation Models); governed AI/AVM use	RICS — https://www.rics.org/profession-standards/rics-standards-and-guidance/sector-standards/valuation-standards/red-book/red-book-global

#	Standard / framework	Identifier / key facts (30 Jun 2026)	Official source
A3	EU AI Act	Regulation (EU) 2024/1689; risk-based; prohibited Feb 2025; GPAI Aug 2025; high-risk Aug 2026 (deferred via 2026 Digital Omnibus); fines up to €35m/7%	European Commission — https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
A4	NIST AI Risk Management Framework	AI RMF 1.0 (Govern/Map/Measure/Manage); Generative AI Profile NIST AI 600-1 (Jul 2024)	NIST — https://www.nist.gov/itl/ai-risk-management-framework
A5	ISO/IEC 42001	AI management system (AIMS); 2023; certifiable	Cited by identifier (ISO)
A6	Model-risk principles (SR 11-7)	Supervisory model-risk-management principles	Cited by identifier
A7	IFRS 13	Fair value measurement (financial reporting)	Cited by identifier (referenced by RICS VPGA 1)
A8	Oracle/NAV & proof-of-reserve layer	Decentralised oracle delivery of NAV/reserves on-chain	See Vol. II Appendix A

APPENDIX B — MODEL INVENTORY TEMPLATE (INDICATIVE)

Indicative columns for the platform-wide model inventory maintained by the model-risk function (§8).

Field	Example
Model ID / name	VAL-DCF-001 / Income DCF
Type	Statistical / ML / LLM-component
Purpose & scope	Income-asset valuation support
Risk tier (internal + AI Act)	High / Limited
Owner (1st line)	Valuation team lead
Validation status (2nd line)	Validated / restricted / pending
Data & lineage ref	Dataset version + catalogue link
Performance metrics	Error/accuracy; last test date
Monitoring	Drift metric; thresholds; last check

Field	Example
Model card	Link (§7)
Approval & review date	Approver; next review

APPENDIX C — EXAMPLE MODEL CARD (SKELETON)

Skeleton for an AVM model card; completed cards live in the model registry.

Section	Example content
Purpose & scope	Indicative valuation cross-check for residential-type assets; not a standalone valuation
Intended / out-of-scope use	Support to a valuer; not for final material valuation without inspection
Data	Comparable transactions + property attributes; sources; date range; quality notes (IVS 104)
Methodology	Gradient-boosted regression; key features; assumptions
Performance	Error distribution; out-of-time test; confidence measure reported with each output
Explainability	SHAP attributions per output; partial-dependence summaries
Limitations & risks	Sparse comparables for heterogeneous assets; drift in fast-moving markets
Governance	Owner; validation status; AI Act tier; review date; monitoring plan

APPENDIX D — CITATION REGISTER (TABLE — VOLUME IV)

Sources relied on in Volume IV. P = official/primary; S = secondary (paraphrased only).

Ref	Source	Type	Used for	Verification note
ivs	IVSC — International Valuation Standards 2025	P	Valuation standard; IVS 104/105; effective date	Verified live 30 Jun 2026
redbook	RICS — Valuation Global Standards (Red Book) 2025	P	Red Book edition; VPS 5; AI/AVM governance; IFRS	Verified live

Ref	Source	Type	Used for	Verification note
			13 (VPGA 1)	
aiact	European Commission — EU AI Act (Reg (EU) 2024/1689) pages	P	Risk tiers; phasing; GPAI; high-risk deferral	Verified live
nistrmf	NIST — AI Risk Management Framework + Generative AI Profile	P	Risk methodology; LLM risk categories	Verified live
iso42001	ISO/IEC 42001:2023 (AI management system)	P	Management-system spine	Cited by identifier

APPENDIX E — CROSS-REFERENCE INDEX

Topic	This volume	Other volumes
Oracle / NAV delivery on-chain	§3	Vol. II §5
Proof-of-reserve / mint gating	§3	Vol. II §3.3, §5
Valuation / NAV → pricing	§2–3	Vol. III §10
Disclosure / fair value reporting	§2	Vol. I §1.4, §4
Data protection / PII off-chain	§10–11	Vol. I §9; Vol. II §1.4
DevSecOps / reproducible builds	§8, §11	Vol. II §10; Vol. V
Risk outputs → financial model	§5	Vol. VI
AI governance / model risk	§8–10	Vol. V (operations)
Diagrams consolidated	—	Vol. VII

DIAGRAM INVENTORY (Volume IV)

Fig.	Title	Mermaid type	Section
1	Financial-intelligence architecture	flowchart	1.3
2	Valuation approaches	flowchart	2.2

Fig.	Title	Mermaid type	Section
	& bases of value		
3	NAV computation & oracle pipeline	flowchart	3.2
4	DCF model structure	flowchart	4.2
5	Sensitivity / tornado view	flowchart	4.3
6	Monte Carlo simulation flow	flowchart	5.2
7	Risk-metric distribution	flowchart	5.3
8	Machine-learning model pipeline	flowchart	6.2
9	Explainability (SHAP) & model card	flowchart	7.2
10	Model lifecycle & three lines of defence	flowchart	8.2
11	AI Act risk-tier mapping	flowchart	9.2
12	LLM control flow	flowchart	10.3
13	Data architecture for intelligence	flowchart	11.2

Volume VII consolidates all diagrams across volumes.

END OF VOLUME IV (interim draft)

Next: Volume V — Security & Operations (custody depth, key ceremonies, PQC migration, DevSecOps depth, resilience and stress testing). Before final delivery, all seven volumes undergo a single cross-volume Compliance & Completeness Audit; forward references are resolved; registers are re-checked; and the package is compiled to `.docx` on explicit request.

VOLUME V — SECURITY & OPERATIONS

Institutional Digital Real Estate Capital Markets Infrastructure

Multi-Volume Documentation Package — Volume V of VII

TITLE PAGE & DOCUMENT CONTROL

Field	Detail
Document	Volume V — Security & Operations (Custody, Key Ceremonies, PQC Migration, DevSecOps, Resilience)
Package	Institutional Digital Real Estate Capital Markets Infrastructure (7 volumes)
Status	Working draft for internal review and security/operations/resilience sign-off — **not a security policy, key-ceremony script, or audit in this form**
Version	V-0.1 (interim; full cross-volume Compliance & Completeness Audit pending completion of Volume VII)
Date of documentation	30 June 2026
Classification	Confidential — Draft
Companion volumes	Vol. I (legal — segregation/DORA), Vol. II (architecture — custody §7, crypto §8, DevSecOps §10)

Authorship and reliance caveat (read first). This volume is an AI-assisted design document prepared to institutional standards of rigour. Regulatory regimes, supervisory

guidance, cryptographic-standard statuses, and framework versions cited here were checked against official or primary sources **as of 30 June 2026** and footnoted. It remains a draft and **must be reviewed and validated by qualified security engineers, custody/key-management specialists, operational-resilience and legal advisers, and independent auditors before any reliance, key ceremony, migration, or go-live.** Nothing here is a security guarantee, legal advice, or a representation that any control is sufficient for a given threat; security is a continuing programme, not a document.

On "latest releases." Security regulation and cryptographic standards have moved materially in the last 18 months. Every load-bearing regime status, supervisory guidance, and standard version in this volume was re-verified against the regulator or standards body on the date of documentation and recorded in **Appendix A — Standards, Frameworks & Versions Register**; it must be re-checked before reliance.

HOW TO READ THIS VOLUME (CONTROL FILE)

Condensed Control File, reproduced atop every volume after Volume I.

Canonical terms (do not substitute synonyms). The instrument is a **ledger-based security** (Vol. I §4.1) implemented as an **ERC-3643 permissioned token** (Vol. II §3). "Custody" is the safekeeping of crypto-based assets and the keys that control them; "segregation" is the legal/operational separation that keeps client assets out of an insolvency estate. "Key ceremony" is the scripted, witnessed, multi-party process for generating and handling cryptographic keys. "PQC" is post-quantum cryptography. "The platform" denotes the infrastructure as a whole.

Cross-volume reference map.

Volume	Scope	Relationship to this volume
I	Executive & Regulatory	Legal basis for segregation (Art. 37d BA; Art. 242a DEBA) and operational-resilience obligations
II	Technical Architecture	Custody/key (§7), cryptography/PQC (§8), DevSecOps (§10) — this volume deepens all three
III	Marketplace & Trading	Venue operations, settlement-asset stress feed the fund-run testing here
IV	Financial Intelligence	Model/data operations governed by the controls here
V	**Security & Operations (this volume)**	**Custody depth, key ceremonies, PQC migration, DevSecOps, resilience, stress testing**

Volume	Scope	Relationship to this volume
VI	Business & Financial Model	Cost/capacity of the controls here
VII	Architecture Atlas	Consolidates this volume's diagrams

Cross-volume item extended in this volume. Volume I's segregation analysis is extended by **FINMA Guidance 01/2026 (12 January 2026)** on the custody of crypto-based assets, which clarifies the segregation models and bankruptcy treatment under **Art. 37d Banking Act** and **Art. 242a DEBA** (see §2). This is carried to the final cross-volume audit.

Rule set (unchanged). No fabricated facts or citations; regime statuses, guidance, and standard versions verified against primary sources and registered in Appendix A; design options labelled with trade-offs; commentary paraphrased; hyperlinks only to official sources verified live on the date of documentation, all other sources cited by stable identifier.

DETAILED TABLE OF CONTENTS

- Principles & the Security-Operations Model
- Custody Architecture (Depth)
- Key Management & Key Ceremonies
- Post-Quantum Migration Plan
- DevSecOps (Depth)
- Smart-Contract Security Operations
- Threat Detection, SOC & Incident Response
- Operational Resilience & DORA
- Business Continuity, Disaster Recovery & Resilience Testing
- Dev-Phase Fund-Run & Stress Testing
- Vendor & Third-Party Risk
- Limitations & Threats Register

84. Interim Compliance & Completeness Audit (Volume V)
85. Future Jurisdiction & Technology Compatibility Notes
86. Glossary
87. Appendices A–E
88. Diagram Inventory

LIST OF FIGURES

Figure	Title	Section
1	Layered defence-in-depth & security operating model	1.3
2	Custody models & FINMA segregation treatment	2.2
3	Custody & key-control architecture	2.3
4	Key ceremony (M-of-N, witnessed)	3.3
5	Key lifecycle	3.4
6	Post-quantum migration roadmap	4.3
7	DevSecOps secure SDLC with gates	5.2
8	Smart-contract security operations & circuit breaker	6.2
9	Incident-response lifecycle	7.2
10	SOC & detection architecture	7.3
11	DORA five pillars → platform controls	8.2
12	Business continuity & disaster recovery	9.2
13	Dev-phase fund-run stress scenario	10.2
14	Third-party risk & CTPP concentration	11.2

LIST OF TABLES

Table	Title	Section
1	Security principles → mechanisms	1.4
2	Custody models & segregation treatment	2.2
3	Key types & controls	3.1
4	PQC algorithms → platform use → migration phase	4.2
5	DevSecOps controls & gates	5.3
6	Incident severity & reporting	7.4

Table	Title	Section
	matrix	
7	DORA pillar → platform control	8.3
8	Dev-phase stress scenarios	10.3
9	Third-party categories & controls	11.3
10	Security & operations threats register	12.1

EXECUTIVE SUMMARY

The earlier volumes established what the platform is (Vol. I), how it is built (Vol. II), how it trades (Vol. III), and how it values and governs models (Vol. IV). This volume specifies how it is **kept secure and kept running** — the custody and key controls that protect client assets, the migration plan that future-proofs the cryptography, the engineering discipline that keeps the code trustworthy, and the operational resilience that lets the platform withstand and recover from disruption. Its governing idea is the same as the rest of the package: **security and resilience are built in and operated continuously, not asserted once.**

Six decisions frame the volume. **First, custody anchored to current supervisory expectations.** Custody and segregation follow **FINMA Guidance 01/2026** (published 12 January 2026), which clarifies that client crypto-based assets are bankruptcy-remote under **Art. 37d Banking Act** and **Art. 242a DEBA** when held in individual custody, or in collective custody with clearly allocated client shares, with the supervised institution remaining fully responsible even when custody is delegated.[207] **Second, keys protected by multi-party control.** Privileged keys live under **MPC and FIPS 140-3 HSMs**, with **threshold/multisig and timelocks**, generated and handled through scripted, witnessed **key ceremonies** with separation of duties (deepening Vol. II §7). **Third, a real post-quantum migration plan.** The platform is crypto-agile and migrates on a phased roadmap toward the **NIST PQC standards FIPS 203/204/205** (final since 2024), with **HQC** and the **FALCON-based FIPS 206** still on the standards track, on the **CNSA 2.0 (2030)** horizon and against the “harvest-now, decrypt-later” threat.[208][209] **Fourth, DevSecOps in depth** — multiple independent audits, formal verification of

[207] FINMA Guidance 01/2026 (published 12 January 2026) on the custody of crypto-based assets — segregation models (individual; collective with clear shares; non-segregable), bankruptcy treatment under Art. 37d Banking Act and Art. 242a DEBA, private-key-protection and counterparty risks, third-party/foreign-custodian equivalence (prudential supervision + bankruptcy protection), and the principle that the supervised institution retains responsibility when custody is delegated. Cited by identifier (FINMA; published on finma.ch); law-firm summaries paraphrased.

critical invariants, software-supply-chain controls, and multisig-governed deployment. **Fifth, operational resilience to DORA.** For EEA-facing activity the platform maps to the five pillars of **DORA (Regulation (EU) 2022/2554, applicable since 17 January 2025)** — ICT risk management, incident reporting, resilience testing including threat-led penetration testing, third-party risk with the Register of Information, and information sharing — mindful that several of its core cloud and data dependencies are now **designated Critical ICT Third-Party Providers**, creating concentration risk that must be managed.[210] **Sixth, prove it under stress** — including a deliberate **dev-phase "fund-run" stress test** that simulates a mass-redemption/settlement shock before real money is at stake.

The chapters develop the security operating model; custody depth; key management and ceremonies; the PQC migration; DevSecOps; smart-contract security operations; detection, SOC and incident response; DORA-aligned operational resilience; business continuity and disaster recovery; the dev-phase fund-run and stress testing; vendor and third-party risk; and an honest threats register. Open items and limitations are gathered in the Interim Audit and §12.

---

[208] NIST Post-Quantum Cryptography standardisation programme — FIPS 203 (ML-KEM), 204 (ML-DSA), 205 (SLH-DSA) final; HQC selected as a backup KEM (11 Mar 2025), standard in development (~2026–2027); FIPS 206 (FN-DSA, FALCON) in development (Initial Public Draft pending as of late 2025 — NIST reported it "basically written, awaiting approval"; final expected ~late 2026/2027); CNSA 2.0 targets 2030; on-chain PQC depends on chain-level adoption. Verified live: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

[209] NIST — release of the first three finalised PQC standards (FIPS 203/204/205), 13 August 2024. Verified live: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[210] Digital Operational Resilience Act (Regulation (EU) 2022/2554) — applicable since 17 January 2025; five pillars (ICT risk management; incident management and reporting; digital operational resilience testing including TLPT; ICT third-party risk including the Register of Information; information sharing); TLPT regulatory technical standard (Commission Delegated Regulation (EU) 2025/1190, aligned with TIBER-EU); incident-reporting RTS (Commission Delegated Regulation (EU) 2025/301); first list of 19 Critical ICT Third-Party Providers designated by the ESAs on 18 November 2025 (updated annually). Verified live 30 Jun 2026: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en and https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora

CHAPTER 1 — PRINCIPLES & THE SECURITY-OPERATIONS MODEL

1.1 Security is a programme, not a property

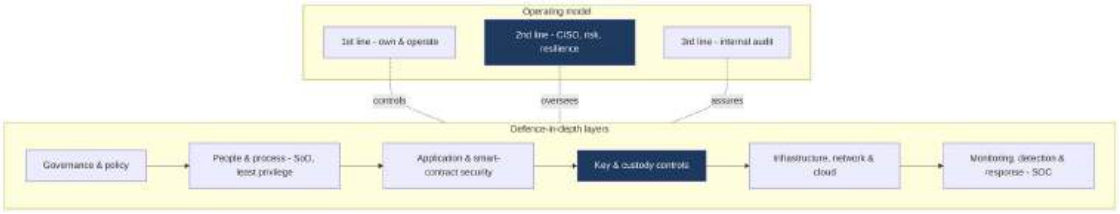
A platform that holds legal title to investors' assets on a public-facing system is a high-value target. Security here is therefore treated as a continuing programme — governed, staffed, tested, and improved — rather than a checklist completed once. The programme rests on a few load-bearing ideas: **defence in depth** (no single control is trusted alone), **least privilege and separation of duties** (no one person or system can act unilaterally on anything that matters), **assume breach** (design so that a compromise is contained and detected, not catastrophic), and **resilience by construction** (the platform is built to withstand and recover from disruption, which is now also a legal obligation under DORA, §8).

1.2 The operating model: three lines and a SOC

Operationally, the programme uses the **three lines of defence** (consistent with the model-risk framework of Vol. IV §8): first line owns and operates controls (engineering, operations, custody); second line sets policy and provides independent security, risk and resilience oversight (a CISO function, security risk, operational resilience); third line is internal audit. A **Security Operations Centre (SOC)** provides continuous monitoring, detection and incident response (§7). Governance sits above, with board-level accountability for security and resilience.

1.3 The layered model

Figure 1 — Layered defence-in-depth & security operating model.



Controls are layered so no single failure is catastrophic; the three lines own, oversee, and assure those layers, with a SOC providing continuous detection and response.

1.4 Principles and mechanisms

Principle	Mechanism	Reference
Defence in depth	Layered controls; no single point of trust	§1.3; all chapters
Least privilege & separation of duties	RBAC; M-of-N for privileged actions; dual control	§3, §5, §6

Principle	Mechanism	Reference
Assume breach	Containment, detection, incident response, recovery	§6–9
Segregation & bankruptcy remoteness	Custody models per FINMA Guidance 01/2026	§2
Crypto-agility & future-proofing	PQC migration; algorithm abstraction	§4
Engineering discipline	Secure SDLC, audits, formal verification, supply-chain	§5
Operational resilience	DORA five pillars; BC/DR; testing	§8–9
Prove under stress	Resilience testing, TLPT, dev-phase fund-run	§9–10
Manage concentration	Third-party/CTPP risk; multi-provider; exit plans	§11

Table 1 — Security principles → mechanisms.

CHAPTER 2 — CUSTODY ARCHITECTURE (DEPTH)

2.1 What custody must achieve

Custody must (a) keep client assets **safe** (protected against theft, loss, and key compromise), (b) keep them **segregated** so they are bankruptcy-remote from the operator and any custodian, and (c) keep the platform's **own privileged keys** under multi-party control. Volume I established the legal basis for segregation; Volume II §7 established the architectural requirement that privileged actions be M-of-N. This chapter deepens both against the most recent Swiss supervisory expectations.

2.2 Segregation models under FINMA Guidance 01/2026

On **12 January 2026 FINMA published Guidance 01/2026** on the custody of crypto-based assets, clarifying when such assets are bankruptcy-remote and what supervised institutions must do.[211] The treatment turns on the **custody model**, and the platform designs to it explicitly.

[211] FINMA Guidance 01/2026 (published 12 January 2026) on the custody of crypto-based assets — segregation models (individual; collective with clear shares; non-segregable), bankruptcy treatment under Art. 37d Banking Act and Art. 242a DEBA, private-key-protection and counterparty risks, third-party/foreign-custodian equivalence (prudential supervision + bankruptcy protection), and the principle that the supervised institution retains responsibility when custody is delegated. Cited by identifier (FINMA; published on finma.ch); law-firm summaries paraphrased.

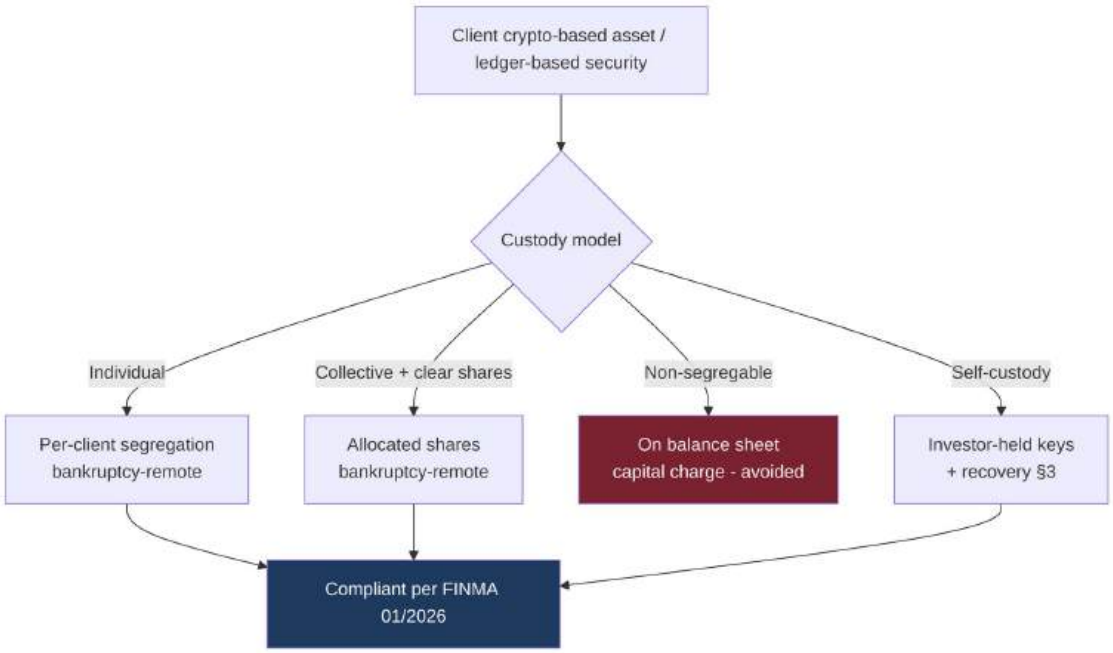
Custody model	Description	Bankruptcy treatment (per FINMA 01/2026)	Platform use
Individual custody	Assets held separately per client, held in readiness at all times	Segregated; excluded from custodian's bankruptcy estate; returned to client; off-balance-sheet, no capital charge	Preferred for client holdings
Collective custody with clear shares	Pooled (e.g. omnibus) but each client's share clearly allocated	Segregated as above, provided shares are unambiguous	Acceptable where individual custody is impractical
Non-segregable custody	Segregation not ensured	On balance sheet; subject to capital requirements; not bankruptcy-remote	Avoided
Self-custody (investor-held)	Investor controls their own keys	Outside the custodian's estate by definition	Supported (with recovery, §3)

Table 2 — Custody models and segregation treatment. Three further points from the guidance shape the design: it stresses **private-key-protection and operational/cyber risk** as primary risks; where custody is **delegated to a third party (especially abroad)** the capital/segregation treatment applies only if the custodian is under **equivalent prudential supervision and equivalent bankruptcy protection exists**; and the **supervised institution remains fully responsible** for compliant custody even when it outsources, requiring documented due diligence and ongoing monitoring.[212] The platform therefore prefers individual (or clearly-shared collective) custody with prudentially supervised custodians, and treats any delegation as a governed, monitored, equivalence-tested arrangement.

2.3 Custody and key-control architecture

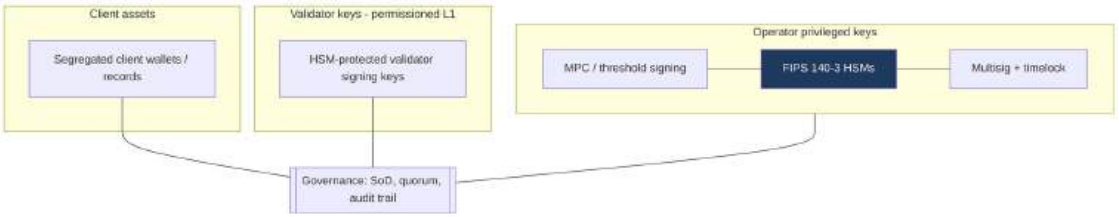
Figure 2 — Custody models & FINMA segregation treatment.

[212] FINMA Guidance 01/2026 (published 12 January 2026) on the custody of crypto-based assets — segregation models (individual; collective with clear shares; non-segregable), bankruptcy treatment under Art. 37d Banking Act and Art. 242a DEBA, private-key-protection and counterparty risks, third-party/foreign-custodian equivalence (prudential supervision + bankruptcy protection), and the principle that the supervised institution retains responsibility when custody is delegated. Cited by identifier (FINMA; published on finma.ch); law-firm summaries paraphrased.



The platform's custody design selects models that FINMA Guidance 01/2026 treats as bankruptcy-remote, and avoids non-segregable custody.

Figure 3 — Custody & key-control architecture.



Client assets are segregated; operator privileged keys are split across MPC and HSMs with multisig and timelocks; validator keys are HSM-protected and segregated from application keys — all under a governance layer enforcing separation of duties and an immutable audit trail.

2.4 Responsibility does not transfer

A recurring theme of the FINMA guidance is that **outsourcing custody does not outsource responsibility.**[213] The platform's operating model reflects this: any third-

[213] FINMA Guidance 01/2026 (published 12 January 2026) on the custody of crypto-based assets — segregation models (individual; collective with clear shares; non-segregable), bankruptcy treatment under Art. 37d Banking Act and Art. 242a DEBA, private-key-protection and counterparty risks, third-party/foreign-custodian equivalence (prudential supervision + bankruptcy protection), and the principle that the supervised institution retains responsibility when custody is delegated. Cited by identifier (FINMA;

party custodian, sub-custodian, or foreign arrangement is subject to due diligence (supervision status, bankruptcy-protection equivalence, technical and operational capability), contractual controls, and ongoing monitoring, with the platform retaining accountability and the ability to exit (§11).

CHAPTER 3 — KEY MANAGEMENT & KEY CEREMONIES

3.1 The keys and what they protect

Three classes of key exist (Vol. II §7), with different blast radii and controls.

Key class	Controls	Compromise impact
Investor wallet keys	Investor-held or custodied; recovery via ERC-3643 / account abstraction	Contained to one holder; must be recoverable (title)
Operator / agent keys (mint, freeze, forced transfer, recovery, upgrade)	MPC + HSM; M-of-N multisig; timelock; SoD	Systemic — strongest controls
Validator signing keys (permissioned L1)	HSM-protected; geographically/organisationally distributed	Network integrity — strong controls, distribution

Table 3 — Key types and controls. The principle throughout: **no single person or device can unilaterally perform a systemic action**, and every privileged action produces an immutable, reviewable audit trail.

3.2 The key-management toolkit

The platform combines **multi-party computation (MPC)** (so a signing key is never reconstructed in one place), **hardware security modules validated to FIPS 140-3** (tamper-resistant generation, storage, and use of keys), **threshold signatures / multisig** (M-of-N approval), and **timelocks** (a delay on the most systemic actions, making them observable and reversible before they take effect). Key-management practice follows recognised guidance (e.g. NIST SP 800-57 for key management; the CryptoCurrency Security Standard for operational controls), cited by identifier in Appendix A.

3.3 Key ceremonies

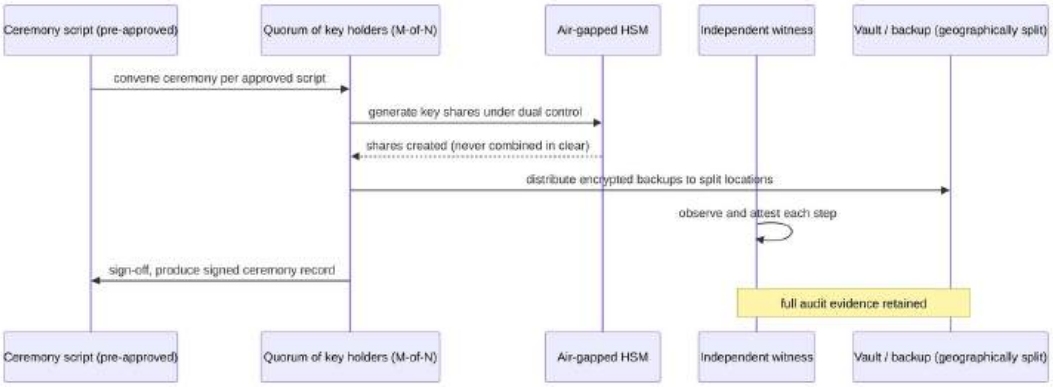
A **key ceremony** is the scripted, witnessed, multi-party process by which the most sensitive keys are generated, backed up, rotated, recovered, or destroyed. It is deliberately formal because the moments when keys are created or recovered are the

---

published on finma.ch); law-firm summaries paraphrased.

moments of greatest exposure. The ceremony is air-gapped where appropriate, performed under dual control with M-of-N quorum, witnessed and recorded, and produces signed evidence.

Figure 4 — Key ceremony (M-of-N, witnessed).



The ceremony is pre-scripted, quorum-controlled, air-gapped, witnessed, and evidenced; key shares are created and split but never combined in the clear.

3.4 The key lifecycle and recovery

Keys are managed across a full lifecycle, each stage governed.

Figure 5 — Key lifecycle.

Every stage — generation, distribution, storage, use, rotation, recovery, destruction — is governed by ceremony, quorum, and audit. Investor-key recovery uses the ERC-3643 recovery function and optional account-abstraction social recovery (Vol. II §7), so a lost key never means a lost legal title.

CHAPTER 4 — POST-QUANTUM MIGRATION PLAN

4.1 The threat and the deadline

A cryptographically relevant quantum computer would break the RSA/elliptic-curve cryptography that secures TLS, signatures, and key exchange. The threat is already live through **"harvest-now, decrypt-later" (HNDL)**: adversaries can capture encrypted long-lived data today and decrypt it once quantum hardware matures, so data with confidentiality requirements beyond ~2030 is already exposed if it crosses networks under classical key exchange. National-security guidance (**NSA CNSA 2.0**) targets migration by **2030**, and a **June 2026 US executive order** set firmer federal PQC-

migration deadlines — both signalling the direction for regulated finance even where not directly binding.[214] The platform therefore treats PQC migration as a present programme, not a future project.

4.2 The standards and where they apply

The platform migrates toward the NIST PQC standards, abstracted behind the crypto-agility layer of Volume II §8 so algorithms are configuration rather than hard-coding.

Standard / algorithm	Function	Platform application	Status (30 Jun 2026)
FIPS 203 — ML-KEM	Key encapsulation	TLS, service channels, data-at-rest key wrapping	Final (Aug 2024); migrate first
FIPS 204 — ML-DSA	Signatures (primary)	Code/document/claim signing; service auth	Final (Aug 2024); enterprise default (e.g. ML-DSA-65)
FIPS 205 — SLH-DSA	Hash-based signatures (conservative)	Root/long-term/code-signing trust anchors	Final (Aug 2024)
FIPS 206 — FN-DSA (FALCON)	Compact signatures	Bandwidth-constrained signing	In development (Initial Public Draft pending as of late 2025 — NIST reports it “basically written, awaiting approval”; final expected ~late 2026/2027)
HQC	Backup KEM (code-based)	Algorithm diversity vs a lattice break	Selected Mar 2025; standard ~2026–2027

Table 4 — PQC algorithms → platform use → migration phase. A constraint repeated from Volume II: **on-chain** signature schemes are fixed by the chain’s protocol, so on-chain PQC depends on chain-level adoption the platform does not control; the platform can act unilaterally **off-chain** (TLS, signing, data-at-rest) and tracks the chain’s PQC roadmap for the on-chain layer.[215]

---

[214] NIST Post-Quantum Cryptography standardisation programme — FIPS 203 (ML-KEM), 204 (ML-DSA), 205 (SLH-DSA) final; HQC selected as a backup KEM (11 Mar 2025), standard in development (~2026–2027); FIPS 206 (FN-DSA, FALCON) in development (Initial Public Draft pending as of late 2025 — NIST reported it “basically written, awaiting approval”; final expected ~late 2026/2027); CNSA 2.0 targets 2030; on-chain PQC depends on chain-level adoption. Verified live: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

[215] NIST Post-Quantum Cryptography standardisation programme — FIPS 203 (ML-KEM), 204 (ML-DSA), 205 (SLH-DSA) final; HQC selected as a backup KEM (11 Mar 2025), standard in development (~2026–2027); FIPS 206 (FN-DSA, FALCON) in development (Initial Public Draft pending as of late 2025 — NIST reported it “basically

4.3 The phased migration roadmap

The platform does not “rip and replace”; it migrates in phases, prioritising long-lived secrets and harvestable channels, using **hybrid** schemes (a classical key exchange *and* ML-KEM together) during transition so the channel is safe if either holds.

Figure 6 — Post-quantum migration roadmap.

written, awaiting approval”; final expected ~late 2026/2027); CNSA 2.0 targets 2030; on-chain PQC depends on chain-level adoption. Verified live: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

Migration begins with a cryptographic inventory and crypto-agility, moves through PKI/TLS/data-at-rest and vendor dependencies, and converges on PQC-everywhere by the CNSA-2.0 horizon — with on-chain PQC adopted as the chain supports it.

4.4 Governance of the migration

The migration is itself a governed programme: a maintained cryptographic inventory (which algorithm protects what, and how long that data must stay confidential), prioritisation by data longevity and exposure, hybrid deployment during transition, vendor/third-party cryptographic requirements written into contracts (§11), and validation/testing of each migrated component under the DevSecOps and resilience controls (§5, §9). Progress is tracked against the roadmap and re-checked as HQC and FIPS 206 finalise.

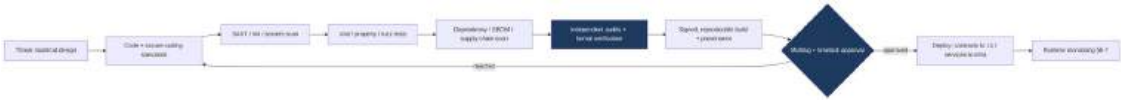
CHAPTER 5 — DEVSECOPS (DEPTH)

5.1 Security is built, not inspected in

The trustworthiness of the platform's code is established before deployment, through a secure software-development lifecycle (SDLC) in which security is a property of the pipeline rather than a final review. This chapter deepens Volume II §10: the principle there was "code is gated by automated checks, human audit, formal proofs, and a governed multisig deployment"; here that is expanded into the concrete control set and the software-supply-chain protections that modern attacks make mandatory.

5.2 The secure SDLC

Figure 7 — DevSecOps secure SDLC with gates.



Every change passes threat modelling, static and dynamic testing, supply-chain scanning, independent audit and formal verification of critical invariants, a signed reproducible build with provenance, and a governed multisig deployment — then is watched at runtime.

5.3 The control set

Control	Purpose
Threat modelling (STRIDE) at design	Find design flaws before code exists
Secure-coding standards + review	Prevent common classes of defect
SAST / linting / secrets scanning	Catch code and credential issues early
Unit / property / fuzz testing	Behavioural and edge-case assurance (esp. contracts)
Dependency scanning + **SBOM**	Know and vet every component (software bill of materials)

Control	Purpose
Software-supply-chain integrity (e.g. SLSA-style provenance; NIST SSDF)	Defend against compromised build/dependencies
Independent audits (more than one) + formal verification	External challenge; mathematical proof of critical invariants (supply integrity, transfer-eligibility, escrow conditions)
Signed, reproducible builds	Tamper-evidence; verifiable artefacts
Secrets management	No secrets in code; vaulted, rotated
Infrastructure-as-code security	Consistent, scanned, reviewable infrastructure
Change control + multisig deployment	No single engineer ships to production; governed, auditable

Table 5 — DevSecOps controls and gates. Two controls are non-negotiable for the on-chain layer: **multiple independent smart-contract audits** and **formal verification** of the invariants whose failure would be catastrophic (you cannot patch a bug an attacker has already exploited on an immutable ledger as easily as a server). Runtime monitoring and the open-source monitoring/relayer tooling that succeeded earlier hosted offerings (Vol. II §10) carry the assurance into operation.

CHAPTER 6 — SMART-CONTRACT SECURITY OPERATIONS

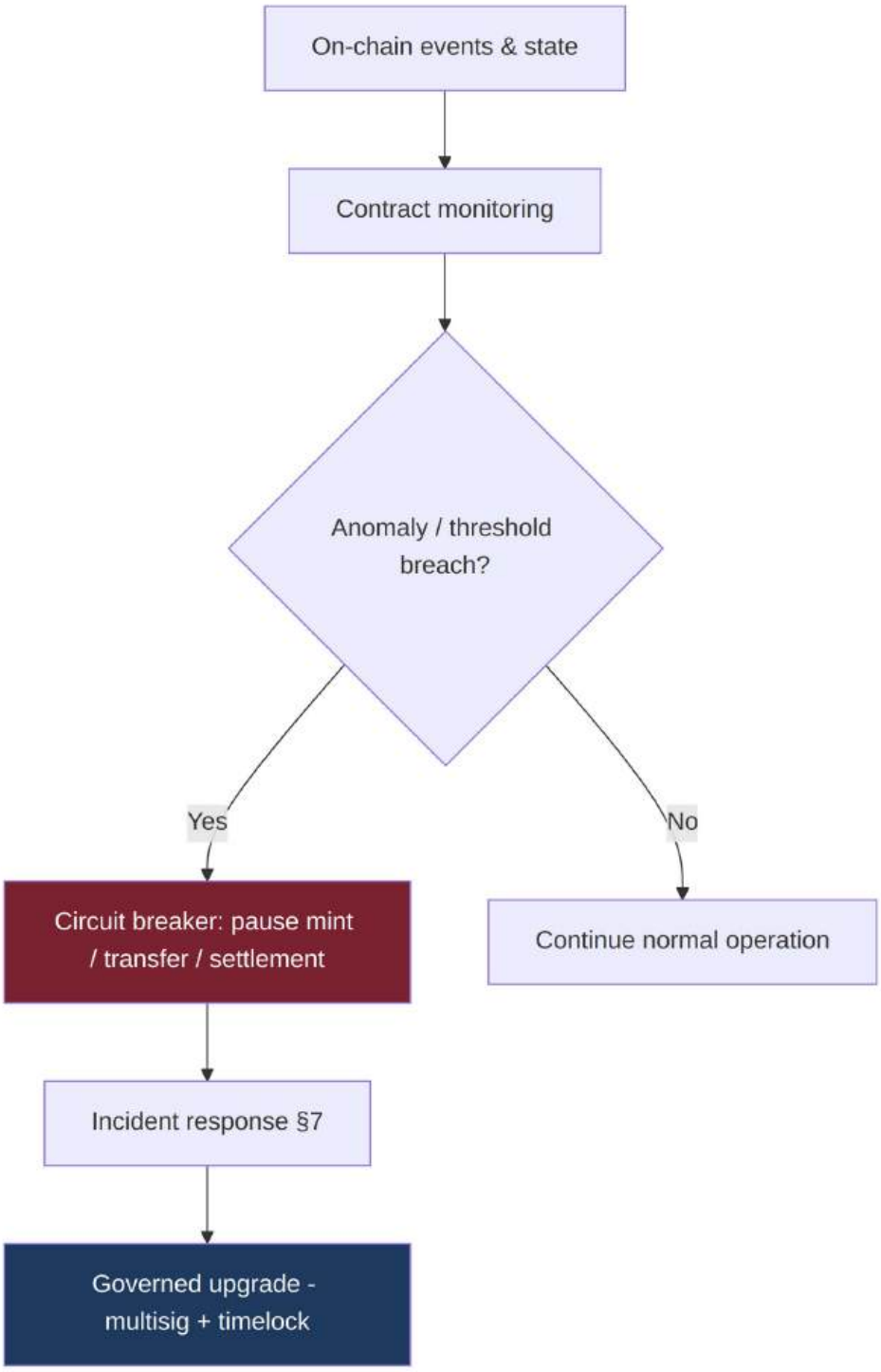
6.1 Operating immutable code safely

Once deployed, smart contracts are largely immutable, high-value, and publicly reachable — a combination that demands its own operational discipline. Smart-contract security operations cover continuous monitoring of contract state and events, the ability to **halt** (pause/freeze) on anomaly, governed **upgrades**, and rehearsed **incident playbooks** for the failure modes that matter most: key compromise, oracle failure/manipulation, and an active exploit.

6.2 Monitoring, circuit breakers and governed upgrades

The platform monitors on-chain events and contract state in real time (balances, mint/burn, transfers, compliance reverts, oracle updates, upgrade events) and wires **circuit breakers** that can pause minting, transfers, or settlement when a threshold or anomaly is detected (e.g. reserve shortfall, NAV staleness, abnormal volume). Upgrades run through the UUPS pattern under **multisig + timelock** (Vol. II §3.4), so any change is observable before it takes effect and reversible if wrong.

Figure 8 — Smart-contract security operations & circuit breaker.



Monitoring feeds anomaly detection; a breach trips a circuit breaker that pauses the affected function and triggers incident response; remediation, if it needs a code change, goes through a governed, timelocked upgrade.

6.3 Incident playbooks and a bug bounty

The platform maintains rehearsed playbooks for the key on-chain incidents — **key/agent-key compromise** (rotate via ceremony, freeze, forced-transfer where lawful), **oracle failure or manipulation** (switch to fallback/quorum, pause dependent functions), **active exploit** (pause, contain, communicate, remediate), and **settlement-asset failure** (halt settlement, invoke fallback rails). A **bug-bounty programme** incentivises responsible disclosure, and on-chain forensics (the immutable ledger is itself evidence) supports post-incident analysis and any regulatory reporting (§7–8).

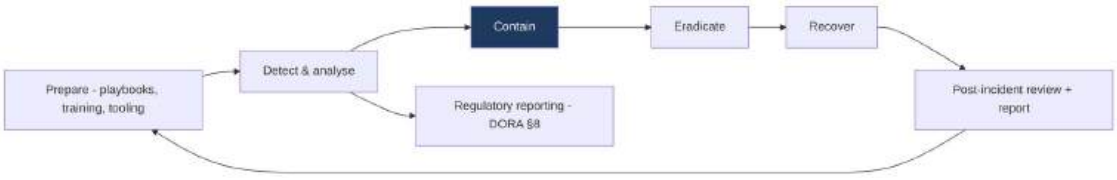
CHAPTER 7 — THREAT DETECTION, SOC & INCIDENT RESPONSE

7.1 Detect and respond, because prevention is never perfect

Assuming breach means investing as much in **detection and response** as in prevention. The platform runs a Security Operations Centre (SOC) with security information and event management (SIEM), aligned to the functions of the **NIST Cybersecurity Framework 2.0** (Govern, Identify, Protect, Detect, Respond, Recover) and the incident-handling lifecycle of recognised guidance (e.g. NIST SP 800-61), and to the incident-reporting obligations of DORA (§8).

7.2 The incident-response lifecycle

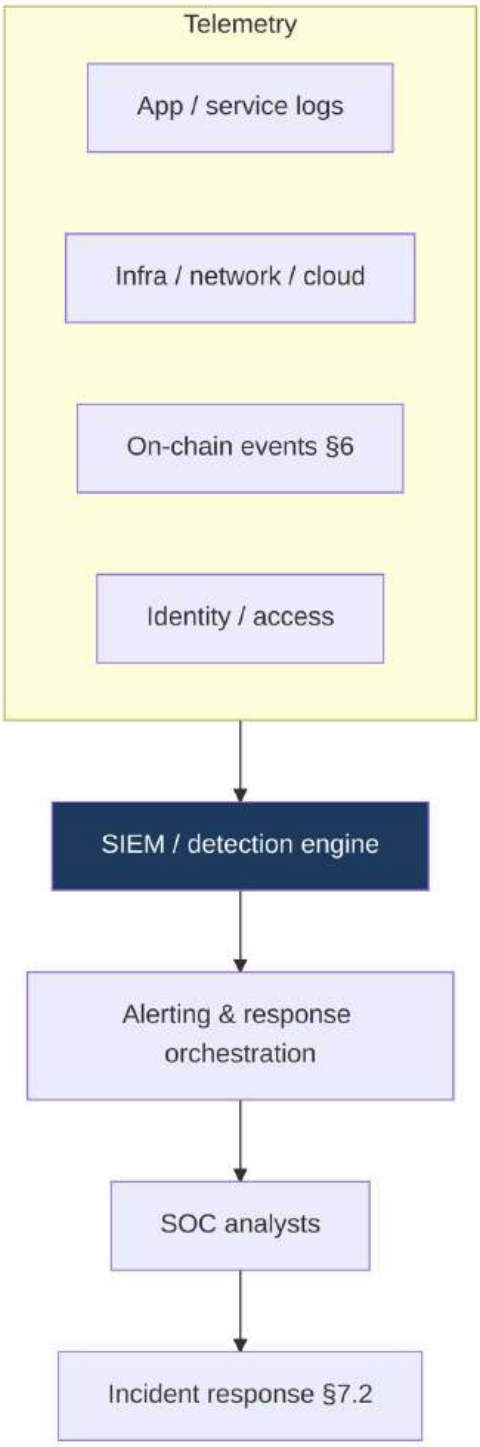
Figure 9 — Incident-response lifecycle.



A continuous loop: prepare, detect/analyse, contain, eradicate, recover, learn — with a parallel path to regulatory reporting where an incident is classified as major.

7.3 SOC and detection architecture

Figure 10 — SOC & detection architecture.



Telemetry from applications, infrastructure, the chain, and identity flows into a SIEM with response orchestration; analysts triage alerts into the incident-response process.

7.4 Incident classification and reporting

Incidents are classified by severity and impact, which drives both internal escalation and external reporting. For EEA-facing activity, **DORA** sets harmonised classification and **major-incident reporting** obligations with defined timelines (initial, intermediate, and final reports), per the relevant Commission Delegated Regulation; Swiss and other regimes have their own notification duties (Vol. I).[216]

Severity	Examples	Action
Critical	Active exploit; key compromise; settlement halt	Immediate containment; exec + board; regulator reporting
High	Oracle failure; significant outage; data incident	Containment; SOC lead; assess reportability
Medium	Contained intrusion attempt; degraded service	SOC handling; monitor; log
Low	Anomalies, near-misses	Triage; trend analysis

Table 6 — Incident severity & reporting matrix. Classification thresholds and reporting templates are fixed with counsel against each applicable regime before go-live.

CHAPTER 8 — OPERATIONAL RESILIENCE & DORA

8.1 Resilience is now a legal obligation

For EEA-facing activity, operational resilience is governed by the **Digital Operational Resilience Act (DORA, Regulation (EU) 2022/2554)**, which has been **applicable since 17 January 2025** and is, in 2026, in active enforcement.[217] DORA harmonises

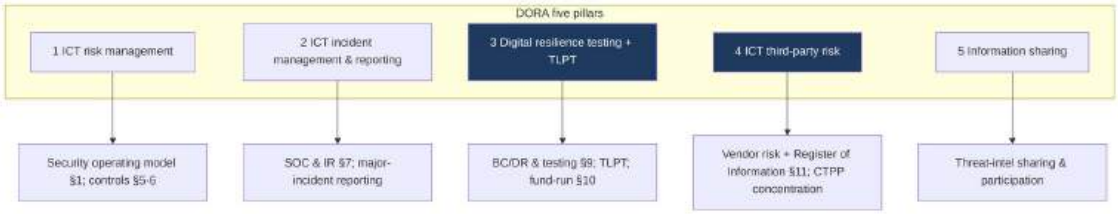
[216] Digital Operational Resilience Act (Regulation (EU) 2022/2554) — applicable since 17 January 2025; five pillars (ICT risk management; incident management and reporting; digital operational resilience testing including TLPT; ICT third-party risk including the Register of Information; information sharing); TLPT regulatory technical standard (Commission Delegated Regulation (EU) 2025/1190, aligned with TIBER-EU); incident-reporting RTS (Commission Delegated Regulation (EU) 2025/301); first list of 19 Critical ICT Third-Party Providers designated by the ESAs on 18 November 2025 (updated annually). Verified live 30 Jun 2026: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en and https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora

[217] Digital Operational Resilience Act (Regulation (EU) 2022/2554) — applicable since 17 January 2025; five pillars (ICT risk management; incident management and

ICT-risk rules across the financial sector around **five pillars**, and the platform maps its security-operations programme directly onto them.

8.2 The five pillars mapped

Figure 11 — DORA five pillars → platform controls.



Each DORA pillar maps to a concrete part of the platform's programme; the testing and third-party pillars (highlighted) are where DLT platforms face the most work.

8.3 Pillar-by-pillar

DORA pillar	Platform control
ICT risk-management framework	Governed security programme; policies; three lines (§1)
ICT-incident management & reporting	SOC, IR lifecycle, classification, major-incident reporting (§7)
Digital operational resilience testing	Vulnerability/scenario testing; **threat-led penetration testing (TLPT)**; dev-phase fund-run (§9–10)
ICT third-party risk	Due diligence, key contractual provisions, **Register of Information**, concentration management (§11)
Information sharing	Participation in threat-intelligence sharing

Table 7 — DORA pillar → platform control. **Threat-led penetration testing** is the most demanding pillar for in-scope entities: the DORA TLPT regulatory technical standard (a Commission Delegated Regulation applicable from mid-2025, aligned with the TIBER-EU framework) requires, for designated entities, advanced red-team testing of live systems at least every three years, with a minimum multi-week active red-team phase, mandatory purple-teaming at closure, and an external threat-intelligence provider.[218]

---

reporting; digital operational resilience testing including TLPT; ICT third-party risk including the Register of Information; information sharing); TLPT regulatory technical standard (Commission Delegated Regulation (EU) 2025/1190, aligned with TIBER-EU); incident-reporting RTS (Commission Delegated Regulation (EU) 2025/301); first list of 19 Critical ICT Third-Party Providers designated by the ESAs on 18 November 2025 (updated annually). Verified live 30 Jun 2026: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en and https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora

The platform builds TLPT capability into its resilience programme (§9) rather than treating it as a one-off.

8.4 Concentration risk and Critical ICT Third-Party Providers

DORA created an EU **oversight framework for Critical ICT Third-Party Providers (CTPPs)**, and on **18 November 2025 the European Supervisory Authorities designated the first list of 19 CTPPs** — which includes the hyperscale cloud, core data, and post-trade infrastructure providers the financial sector (and this platform) depends on.[219] This makes **concentration risk** explicit: if the platform's hosting, data, or oracle infrastructure rests on a small number of designated providers, that dependency must be assessed, documented in the **Register of Information**, and mitigated (multi-provider strategies, exit plans, contractual rights) — see §11. The platform treats CTPP concentration as a first-order operational risk, not a procurement detail.

---

[218] Digital Operational Resilience Act (Regulation (EU) 2022/2554) — applicable since 17 January 2025; five pillars (ICT risk management; incident management and reporting; digital operational resilience testing including TLPT; ICT third-party risk including the Register of Information; information sharing); TLPT regulatory technical standard (Commission Delegated Regulation (EU) 2025/1190, aligned with TIBER-EU); incident-reporting RTS (Commission Delegated Regulation (EU) 2025/301); first list of 19 Critical ICT Third-Party Providers designated by the ESAs on 18 November 2025 (updated annually). Verified live 30 Jun 2026: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en and https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora

[219] Digital Operational Resilience Act (Regulation (EU) 2022/2554) — applicable since 17 January 2025; five pillars (ICT risk management; incident management and reporting; digital operational resilience testing including TLPT; ICT third-party risk including the Register of Information; information sharing); TLPT regulatory technical standard (Commission Delegated Regulation (EU) 2025/1190, aligned with TIBER-EU); incident-reporting RTS (Commission Delegated Regulation (EU) 2025/301); first list of 19 Critical ICT Third-Party Providers designated by the ESAs on 18 November 2025 (updated annually). Verified live 30 Jun 2026: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en and https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora

CHAPTER 9 — BUSINESS CONTINUITY, DISASTER RECOVERY & RESILIENCE TESTING

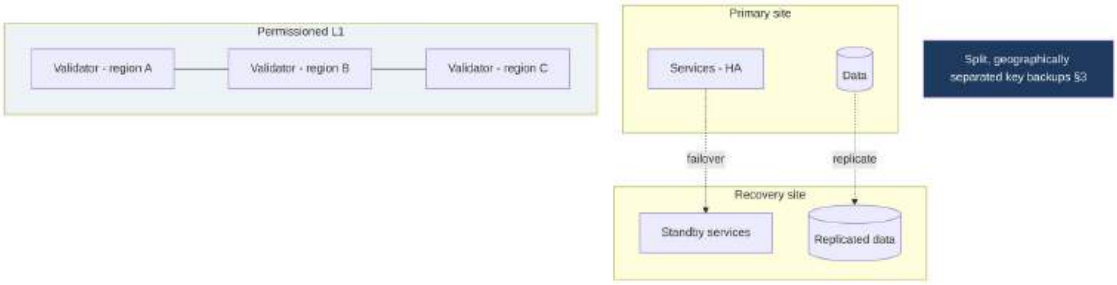
9.1 Withstand, respond, recover

Operational resilience means the platform can keep delivering its critical functions through disruption and recover quickly when it cannot. This rests on classic business-continuity and disaster-recovery (BC/DR) discipline — recovery objectives, redundancy, backups, and tested restoration — adapted for the blockchain-specific concerns of finality and validator availability (Vol. II §11), and proven through testing rather than assumed.

9.2 BC/DR architecture

The platform defines **recovery objectives** (recovery-time and recovery-point objectives, RTO/RPO) per critical function; deploys services **highly available** across zones with automated failover; backs up data and keys (the latter via split, geographically separated backups, §3); and ensures the permissioned L1's **validator set is geographically and organisationally distributed** so no single site failure halts the chain. On-chain state is, by design, replicated across validators; off-chain state follows standard multi-site backup-and-restore with tested recovery.

Figure 12 — Business continuity & disaster recovery.



Services fail over to a recovery site, data is replicated, the validator set spans regions/operators, and keys are recoverable from geographically separated backups — with recovery objectives defined and tested per critical function.

9.3 Resilience testing

Resilience is proven by testing across a spectrum: vulnerability assessments and scenario-based tests (all in-scope entities under DORA), **threat-led penetration testing** for designated entities (§8.3), **disaster-recovery drills** (failover and restore against RTO/RPO), and **game-days / chaos exercises** that deliberately inject failures (a region outage, an oracle stall, a validator loss) to confirm the platform degrades gracefully and recovers. The most platform-specific of these — a simulated mass-redemption "fund-run" — is important enough to treat on its own (§10).

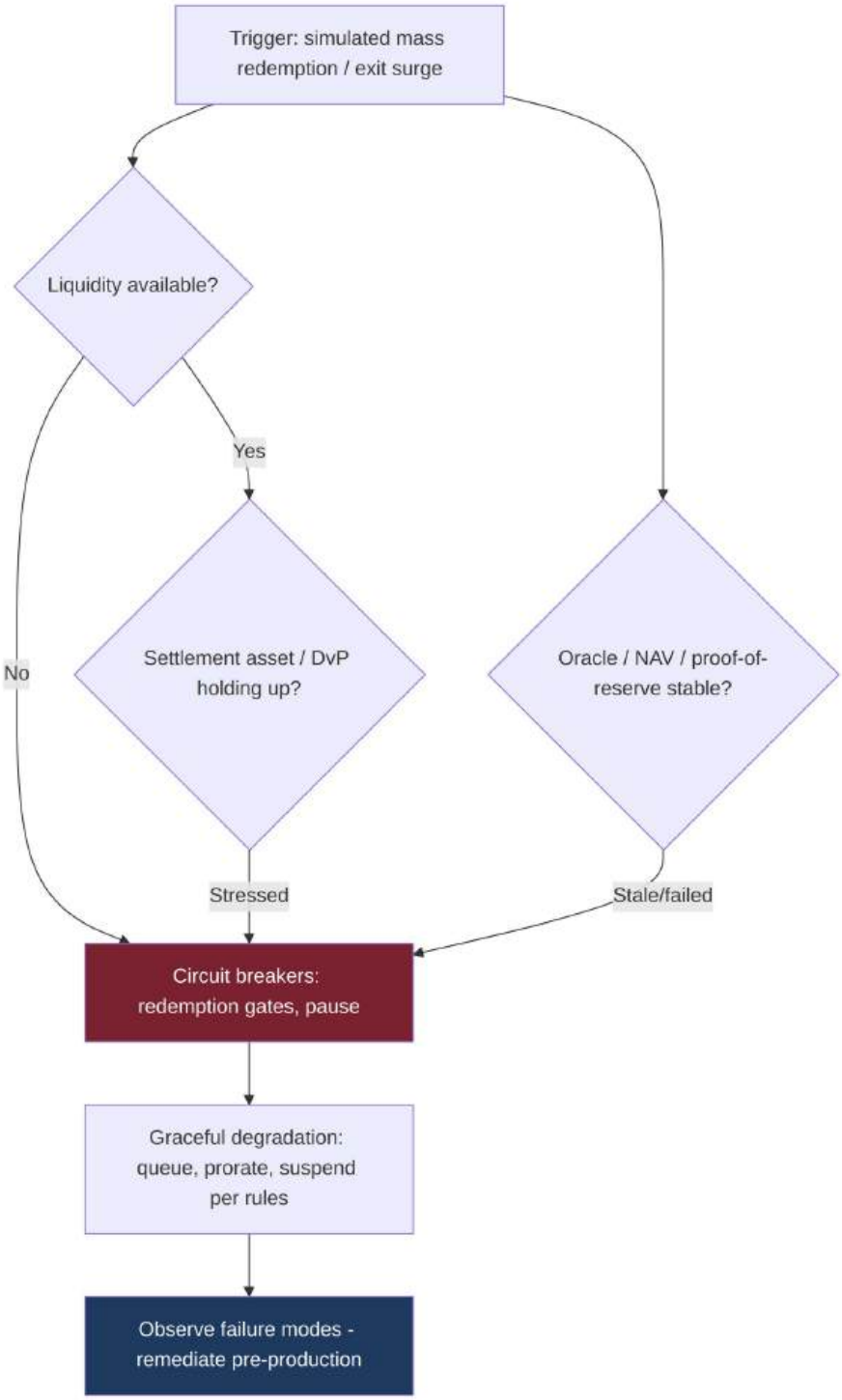
CHAPTER 10 — DEV-PHASE FUND-RUN & STRESS TESTING

10.1 Why simulate a run before real money is at stake

The most dangerous scenario for any asset-holding platform is a **run**: many holders trying to exit at once. For a tokenised real-estate vehicle this is doubly hard because the underlying assets are illiquid (Vol. III §6) while the token can be transferred instantly. The platform therefore conducts a deliberate **dev-phase fund-run stress test** — simulating a mass-redemption/exit shock in a controlled pre-production environment — so that the failure modes are discovered and remediated **before** real investors and real money are exposed. This is both prudent engineering and a concrete instance of DORA scenario testing (§8).

10.2 The fund-run scenario

Figure 13 — Dev-phase fund-run stress scenario.



The test drives a redemption surge and observes whether liquidity, the settlement asset/DvP, and the oracle/NAV layer hold — and whether the designed circuit breakers, redemption gates, and graceful-degradation rules behave as intended.

10.3 What is tested

Scenario	Stresses	What “passing” looks like
Mass redemption surge	Liquidity (§Vol. III §6); redemption mechanics	Gates/queues/proration engage per disclosed rules; no disorderly failure
Settlement-asset stress	Cash leg / stablecoin / DvP (Vol. II §9)	DvP halts safely; fallback rails; no principal loss
Oracle / NAV outage	Pricing, mint-gate, distributions (Vol. IV §3)	Circuit breakers pause dependent functions; stale data rejected
Validator / chain disruption	Finality, availability (§9)	Chain continues or fails safe; no double-settlement
Combined shock	All of the above together	Containment, clear precedence of controls, recoverability

Table 8 — Dev-phase stress scenarios. Two honesty caveats: a dev-phase test cannot perfectly reproduce real human behaviour or real market liquidity, and passing it is necessary but not sufficient. Its value is to surface and fix the controllable failure modes — and to validate that the product-level liquidity features (redemption windows, gates, proration; Vol. I Ch. 3, Vol. IV §6) and the technical circuit breakers actually work together under pressure.

CHAPTER 11 — VENDOR & THIRD-PARTY RISK

11.1 The platform is only as resilient as its dependencies

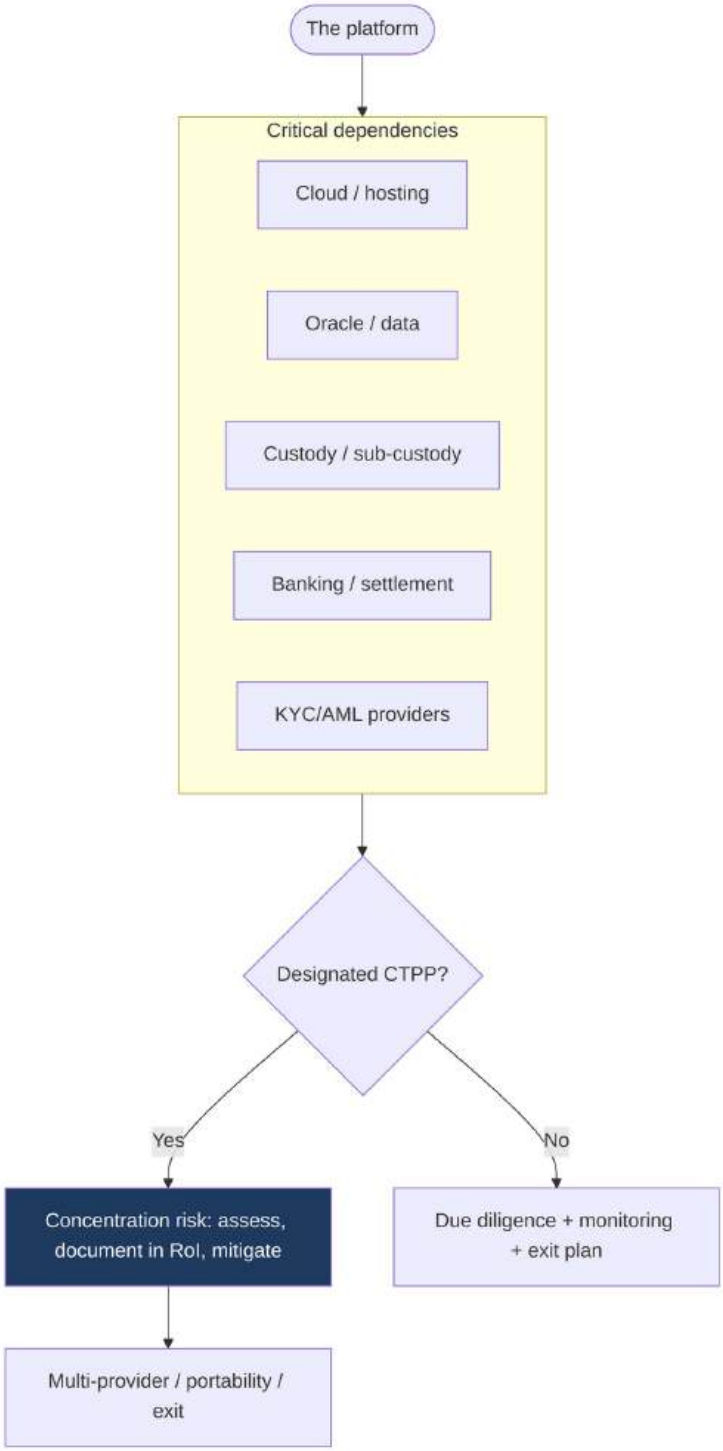
The platform depends on third parties for hosting/cloud, data and oracles, custody, KYC/AML, banking/settlement, and validator operations. Each is a managed risk, not a solved one (a theme from every volume’s threats register). DORA’s third-party pillar makes this explicit and binding for EEA-facing activity: maintain a **Register of Information** of all ICT third-party arrangements, include **key contractual provisions** (audit rights, exit strategies, security and resilience requirements, sub-contracting controls), and manage **concentration risk**.[220]

[220] Digital Operational Resilience Act (Regulation (EU) 2022/2554) — applicable since 17 January 2025; five pillars (ICT risk management; incident management and reporting; digital operational resilience testing including TLPT; ICT third-party risk including the Register of Information; information sharing); TLPT regulatory technical standard (Commission Delegated Regulation (EU) 2025/1190, aligned with TIBER-EU); incident-reporting RTS (Commission Delegated Regulation (EU) 2025/301); first list of 19 Critical ICT Third-Party Providers designated by the ESAs on 18 November 2025 (updated annually). Verified live 30 Jun 2026: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en and

11.2 Concentration and the CTPP dimension

Figure 14 — Third-party risk & CTPP concentration.

https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora



Critical dependencies are assessed for concentration; where a provider is a designated Critical ICT Third-Party Provider, the dependency is documented and mitigated through multi-provider strategies, portability, and exit planning.

11.3 Vendor categories and controls

Vendor category	Key risks	Controls
Cloud / hosting (often a CTPP)	Concentration, outage, lock-in	Multi-AZ/region; exit/portability; RoI; DORA clauses
Oracle / data	Manipulation, staleness, concentration	Decentralised feeds, fallback quorum (Vol. II §5); monitoring
Custody / sub-custody	Segregation, insolvency, key compromise	FINMA-aligned equivalence test; due diligence; responsibility retained (§2)
Banking / settlement	Settlement-asset failure, access	DvP, fallback rails, diversified partners (Vol. II §9)
KYC/AML / claim issuers	Data protection, reliability	Vetting; data-protection controls (Vol. I §9)
Validator operators	Collusion, availability	Vetting, distribution, HSM keys, PoA→PoS (Vol. II §2.3)

Table 9 — Third-party categories and controls. The governing rule, reinforced by FINMA Guidance 01/2026 for custody specifically, is that **outsourcing never outsources accountability** (§2.4): the platform remains responsible, must be able to oversee and exit, and designs against single points of dependence.

CHAPTER 12 — LIMITATIONS & THREATS REGISTER

12.1 Honest assessment

#	Threat / limitation	Exposure	Mitigation / status
1	Operator/agent-key compromise	High	MPC + FIPS 140-3 HSM; M-of-N; timelock; ceremonies (§2–3)
2	Custody/segregation failure (esp. delegated/foreign)	High	FINMA-aligned models; equivalence test; responsibility retained (§2)
3	Smart-contract exploit	High	Multiple audits, formal verification, monitoring, circuit breakers, bug bounty (§5–6)
4	Oracle/settlement-asset failure	High	Decentralised feeds, fallback, circuit breakers, DvP (§6; Vol. II §5, §9)
5	Run / mass redemption on illiquid assets	High	Redemption gates/features; circuit breakers; dev-phase fund-run test (§10)

#	Threat / limitation	Exposure	Mitigation / status
6	Third-party / CTPP concentration	Medium-High	RoI, multi-provider, exit plans, DORA clauses (§11)
7	Quantum threat to classical crypto (HNDL)	Medium (rising)	Crypto-agility; phased PQC migration; hybrid (§4)
8	DORA non-compliance / enforcement	Medium-High	Five-pillar mapping; TLPT; RoI; reporting (§7–8)
9	Validator-set compromise/availability	Medium	Vetted, distributed, HSM-protected; PoA→PoS (§9; Vol. II §2.3)
10	Insider threat / privilege abuse	Medium	SoD, least privilege, M-of-N, audit trails, monitoring (§1, §3, §7)
11	Supply-chain compromise (build/deps)	Medium	SBOM, provenance, signed reproducible builds (§5)
12	DR/BC failure (cannot recover in objective)	Medium	RTO/RPO, replication, tested restore, drills (§9)
13	Incident-detection gap / slow response	Medium	SOC, SIEM, IR lifecycle, game-days (§7)
14	On-chain PQC dependence on chain roadmap	Medium	Off-chain PQC unilaterally; track chain support (§4)
15	Over-reliance on a single custodian/provider	Medium	Diversification, portability, exit (§2, §11)

12.2 Honest limitations

This volume specifies a security-and-operations architecture and programme; it does not itself secure anything — only implementation, continuous operation, independent testing, and audit do. Several controls are deliberately conservative (M-of-N everywhere, timelocks, list-first venue strategy from Vol. III) and trade speed for safety. The platform cannot eliminate its dependence on oracles, custodians, validators, settlement assets, and cloud/CTPP providers; it can only manage that dependence. The dev-phase fund-run is a model of a run, not a run; real liquidity and real human behaviour will differ. And the PQC migration depends on standards (HQC, FIPS 206) and chain support that are not yet all final. Security is a programme that must be funded and operated continuously (Vol. VI), not a state achieved by this document.

INTERIM COMPLIANCE & COMPLETENESS AUDIT — VOLUME V

Verification performed. Regimes, guidance, and standard statuses were checked against primary sources on 30 June 2026 and recorded in Appendix A: **FINMA Guidance 01/2026** (12 Jan 2026) on custody of crypto-based assets, including segregation models and bankruptcy treatment under **Art. 37d Banking Act** and **Art. 242a DEBA**[221]; **DORA (Reg (EU) 2022/2554)**, applicable since 17 Jan 2025, its five pillars, the TLPT regulatory technical standard, the Register of Information, and the 18 November 2025 first designation of 19 Critical ICT Third-Party Providers[222]; and the **NIST PQC** programme — FIPS 203/204/205 final (Aug 2024), HQC selected (Mar 2025, standard ~2026–2027), and FIPS 206/FN-DSA in development (Initial Public Draft pending as of late 2025 — NIST reported it "basically written, awaiting approval"; final expected ~late 2026/2027)[223][224]. **FIPS 140-3**, **NIST CSF 2.0**, **NIST SP 800-57 / 800-61 /**

[221] FINMA Guidance 01/2026 (published 12 January 2026) on the custody of crypto-based assets — segregation models (individual; collective with clear shares; non-segregable), bankruptcy treatment under Art. 37d Banking Act and Art. 242a DEBA, private-key-protection and counterparty risks, third-party/foreign-custodian equivalence (prudential supervision + bankruptcy protection), and the principle that the supervised institution retains responsibility when custody is delegated. Cited by identifier (FINMA; published on finma.ch); law-firm summaries paraphrased.

[222] Digital Operational Resilience Act (Regulation (EU) 2022/2554) — applicable since 17 January 2025; five pillars (ICT risk management; incident management and reporting; digital operational resilience testing including TLPT; ICT third-party risk including the Register of Information; information sharing); TLPT regulatory technical standard (Commission Delegated Regulation (EU) 2025/1190, aligned with TIBER-EU); incident-reporting RTS (Commission Delegated Regulation (EU) 2025/301); first list of 19 Critical ICT Third-Party Providers designated by the ESAs on 18 November 2025 (updated annually). Verified live 30 Jun 2026: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en and https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora

[223] NIST Post-Quantum Cryptography standardisation programme — FIPS 203 (ML-KEM), 204 (ML-DSA), 205 (SLH-DSA) final; HQC selected as a backup KEM (11 Mar 2025), standard in development (~2026–2027); FIPS 206 (FN-DSA, FALCON) in development (Initial Public Draft pending as of late 2025 — NIST reported it "basically written, awaiting approval"; final expected ~late 2026/2027); CNSA 2.0 targets 2030; on-chain PQC depends on chain-level adoption. Verified live: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

800-218, **ISO/IEC 27001:2022**, **CNSA 2.0**, and the **CryptoCurrency Security Standard** are cited by stable identifier.

Cross-volume item extended. Volume I's segregation analysis is extended here by FINMA Guidance 01/2026 and the specific provisions (Art. 37d BA; Art. 242a DEBA); carried to the final cross-volume audit.

No fabricated identifiers. No regime, guidance, standard, or date has been invented; the not-yet-final items (HQC and FIPS 206 standards; DORA enforcement specifics) are flagged as such rather than stated as settled.

Open / flagged items for specialist sign-off. 1. Custody-model selection and any delegation/foreign-custodian equivalence — confirm with counsel and custodian due diligence against FINMA 01/2026 (§2). 2. Key-ceremony scripts, quorum composition, and HSM models — confirm with custody/key specialists before any ceremony (§3). 3. PQC migration scope, hybrid choices, and timeline — confirm and track HQC/FIPS 206 finalisation; on-chain PQC depends on chain roadmap (§4). 4. DORA in-scope classification, TLPT applicability, and Register-of-Information completeness — confirm with operational-resilience counsel (§8, §11). 5. Incident classification thresholds and reporting templates per regime — confirm with counsel (§7). 6. Dev-phase fund-run scenario design and acceptance criteria — confirm with risk and treasury (§10).

Link policy. Hyperlinks point only to official/primary sources verified live on 30 June 2026 (EIOPA/ESMA for DORA; NIST for PQC). FINMA Guidance 01/2026, the DORA delegated regulations, FIPS standards, NIST SPs, ISO standards, and Swiss statutory provisions are cited by stable identifier.

FUTURE JURISDICTION & TECHNOLOGY COMPATIBILITY NOTES

Regulatory watch items. (a) **DORA** — 2026 is the enforcement phase ("interventionist supervision"); track CTPP designations (updated annually), TLPT notification waves, and Register-of-Information data-quality expectations. (b) **FINMA** — track further guidance and the Swiss FINIG/crypto-regulation reforms under consultation; custody expectations may tighten. (c) **PQC mandates** — track CNSA 2.0 (2030), the 2026 US executive order on PQC, and any EEA/Swiss PQC expectations for finance. (d) **NIST** — track HQC and FIPS 206 finalisation, and new CSF/AI-security profiles.

[224] NIST — release of the first three finalised PQC standards (FIPS 203/204/205), 13 August 2024. Verified live: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

Technology watch items. Confidential-compute and MPC custody tooling, account-abstraction recovery (Vol. II §7), and post-quantum-ready HSMs are advancing; revisit the custody and key chapters as they mature. On-chain PQC remains dependent on chain-level adoption (§4). Supply-chain integrity tooling (provenance, SBOM ecosystems) continues to evolve and should be tracked for the DevSecOps pipeline (§5).

GLOSSARY

Covers terms introduced in this volume; master glossary in Vol. I, technical in Vol. II. Canonical reminder: the instrument is a **ledger-based security** implemented as an **ERC-3643 permissioned token**.

- **BC/DR** — business continuity / disaster recovery.
- **CCSS** — CryptoCurrency Security Standard (operational security controls for crypto systems).
- **Circuit breaker** — an automated control that pauses a function (mint, transfer, settlement, redemption) on anomaly.
- **CNSA 2.0** — the NSA's Commercial National Security Algorithm Suite 2.0, targeting PQC migration by 2030.
- **CTPP** — Critical ICT Third-Party Provider, designated by the EU's ESAs for direct oversight under DORA.
- **DORA** — Digital Operational Resilience Act (Regulation (EU) 2022/2554).
- **FIPS 140-3** — the standard for validating cryptographic modules / HSMs.
- **HNDL** — "harvest now, decrypt later": capturing ciphertext today to decrypt once quantum computers exist.
- **HSM** — hardware security module: tamper-resistant device for key generation/storage/use.
- **Key ceremony** — a scripted, witnessed, multi-party process for handling sensitive keys.
- **MPC** — multi-party computation; splits a signing key so it is never reconstructed in one place.
- **PQC** — post-quantum cryptography; NIST standards FIPS 203/204/205 (and forthcoming HQC, FIPS 206).
- **Register of Information (RoI)** — DORA's mandated register of all ICT third-party arrangements.
- **RTO / RPO** — recovery-time objective / recovery-point objective.
- **SBOM** — software bill of materials.
- **SIEM / SOC** — security information and event management / security operations centre.

- **SLSA / SSDF** — supply-chain integrity framework / NIST Secure Software Development Framework.
- **Threat-led penetration testing (TLPT)** — DORA's advanced red-team testing of live systems (aligned with TIBER-EU).
- **Three lines of defence** — own/operate (1st), oversee (2nd), audit (3rd).
- **Timelock** — a delay on a sensitive action so it is observable and reversible before it takes effect.

APPENDIX A — STANDARDS, FRAMEWORKS & VERSIONS REGISTER

Authoritative register relied on. "Verified live 30 Jun 2026" means the official source was retrieved on that date. Hyperlinks only to official sources verified live; other items cited by stable identifier. Re-check before reliance.

#	Standard / framework / regime	Identifier / key facts (30 Jun 2026)	Official source
A1	DORA	Regulation (EU) 2022/2554; applicable 17 Jan 2025; 5 pillars; TLPT RTS (Commission Delegated Reg (EU) 2025/1190); incident-reporting RTS (Reg (EU) 2025/301); first 19 CTPPs designated 18 Nov 2025	EIOPA — https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en ; ESMA — https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora
A2	FINMA Guidance 01/2026	Custody of crypto-based assets (12 Jan 2026); segregation models; Art. 37d BA; Art. 242a DEBA; institution retains responsibility	Cited by identifier (FINMA; published on finma.ch)
A3	NIST PQC programme	FIPS 203/204/205 final (13 Aug 2024); HQC selected (11 Mar 2025, standard ~2026–2027); FIPS 206/FN-DSA in development (IPD pending late 2025)	NIST CSRC — https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization
A4	NIST FIPS 203/204/205 release	Published 13 Aug 2024	NIST — https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

#	Standard / framework / regime	Identifier / key facts (30 Jun 2026)	Official source
A5	FIPS 140-3	Cryptographic-module / HSM validation	Cited by identifier (NIST CMVP)
A6	NIST CSF 2.0	Cybersecurity Framework 2.0 (Govern/Identify/Protect/Detect/Respond/Recover)	Cited by identifier
A7	NIST SP 800-57 / 800-61 / 800-218	Key management / incident handling / secure software development (SSDF)	Cited by identifier
A8	ISO/IEC 27001:2022	Information security management system	Cited by identifier
A9	CNSA 2.0	NSA PQC migration suite; 2030 horizon	Cited by identifier
A10	CryptoCurrency Security Standard (CCSS)	Operational crypto security controls	Cited by identifier
A11	Swiss segregation provisions	Art. 37d Banking Act; Art. 242a DEBA	See Vol. I / Vol. III registers

APPENDIX B — KEY-CEREMONY CHECKLIST (INDICATIVE)

Indicative; the actual ceremony script is approved and controlled by the custody/security function (§3).

Stage	Checklist item
Pre-ceremony	Approved script; quorum (M-of-N) confirmed; roles assigned; witness present; environment air-gapped/clean
Generation	Keys/shares generated in HSM under dual control; never combined in clear
Backup	Encrypted shares distributed to geographically separated, access-controlled vaults
Verification	Test signing / recovery dry-run; integrity checks
Evidence	Each step observed, recorded, attested; signed ceremony record retained
Post-ceremony	Inventory updated; access reviewed; audit trail filed; debrief

APPENDIX C — INCIDENT SEVERITY & REPORTING MATRIX (INDICATIVE)

Indicative mapping; thresholds and templates fixed with counsel per regime (§7.4).

Severity	Internal escalation	External reporting (indicative)
Critical	Exec + board; SOC lead; legal	DORA major-incident report (where in scope); other regulators per Vol. I; affected parties
High	SOC lead; CISO; assess reportability	Report if classification thresholds met
Medium	SOC handling	Log; monitor; assess
Low	Triage	Trend analysis only

APPENDIX D — CITATION REGISTER (TABLE — VOLUME V)

Sources relied on in Volume V. P = official/primary; S = secondary (paraphrased only).

Ref	Source	Type	Used for	Verification note
dora	EIOPA / ESMA — DORA (Reg (EU) 2022/2554) pages	P	Five pillars; applicability; TLPT; RoI; CTPP designation	Verified live 30 Jun 2026
finma	FINMA Guidance 01/2026 (custody of crypto-based assets)	P	Segregation models; Art. 37d BA / Art. 242a DEBA; outsourcing responsibility	Cited by identifier (FINMA); summaries paraphrased
nistpqc	NIST CSRC — PQC standardisation programme	P	FIPS 203/204/205; HQC; FIPS 206 status; migration	Verified live
nistfips	NIST — FIPS 203/204/205 release	P	13 Aug 2024 publication	Verified live

APPENDIX E — CROSS-REFERENCE INDEX

Topic	This volume	Other volumes
Custody / key architecture (baseline)	§2–3	Vol. II §7
Cryptography / PQC (baseline)	§4	Vol. II §8

Topic	This volume	Other volumes
DevSecOps (baseline)	§5–6	Vol. II §10
Resilience / finality	§9	Vol. II §11
Segregation (legal basis)	§2	Vol. I §4.6
DORA (legal basis)	§8	Vol. I §1.5, §10
Settlement-asset / DvP stress	§10	Vol. II §9; Vol. III §5
Liquidity / redemption (run)	§10	Vol. III §6; Vol. I Ch. 3
Oracle/NAV operations	§6, §10	Vol. II §5; Vol. IV §3
Cost/capacity of controls	§1, §12	Vol. VI
Diagrams consolidated	—	Vol. VII

DIAGRAM INVENTORY (Volume V)

Fig.	Title	Mermaid type	Section
1	Layered defence-in-depth & operating model	flowchart	1.3
2	Custody models & FINMA segregation	flowchart	2.2
3	Custody & key-control architecture	flowchart	2.3
4	Key ceremony (M-of-N, witnessed)	sequenceDiagram	3.3
5	Key lifecycle	flowchart	3.4
6	Post-quantum migration roadmap	flowchart	4.3
7	DevSecOps secure SDLC with gates	flowchart	5.2
8	Smart-contract security operations & circuit breaker	flowchart	6.2
9	Incident-response lifecycle	flowchart	7.2
10	SOC & detection architecture	flowchart	7.3
11	DORA five pillars → platform controls	flowchart	8.2
12	Business continuity & disaster recovery	flowchart	9.2

Fig.	Title	Mermaid type	Section
13	Dev-phase fund-run stress scenario	flowchart	10.2
14	Third-party risk & CTPP concentration	flowchart	11.2

Volume VII consolidates all diagrams across volumes.

END OF VOLUME V (interim draft)

Next: Volume VI — Business & Financial Model (TAM/SAM/SOM, tokenomics, roadmap, cost and capacity — including the cost of the controls specified here). Before final delivery, all seven volumes undergo a single cross-volume Compliance & Completeness Audit; forward references are resolved; registers are re-checked; and the package is compiled to `.docx` on explicit request.

VOLUME VI — BUSINESS & FINANCIAL MODEL

Institutional Digital Real Estate Capital Markets Infrastructure

Multi-Volume Documentation Package — Volume VI of VII

TITLE PAGE & DOCUMENT CONTROL

Field	Detail
Document	Volume VI — Business & Financial Model (Market, Revenue, Tokenomics, Costs, Roadmap)
Package	Institutional Digital Real Estate Capital Markets Infrastructure (7 volumes)
Status	Working draft for internal review and commercial/finance sign-off — **not a financial forecast, offering document, or investment solicitation in this form**
Version	VI-0.1 (interim; full cross-volume Compliance & Completeness Audit pending completion of Volume VII)

Field	Detail
Date of documentation	30 June 2026
Classification	Confidential — Draft
Companion volumes	Vol. IV (valuation/NAV, risk), Vol. V (security/operations cost drivers), Vol. I (regulatory)

Authorship and reliance caveat (read first). This volume is an AI-assisted design document. Third-party **market-size data and current on-chain figures** cited here were checked against public sources **as of 30 June 2026** and footnoted; they are external estimates, not the platform's own results. All **financial projections, unit economics, and scenarios in this volume are illustrative assumptions, not forecasts, promises, or guarantees** of any outcome, and are provided to structure planning — not to value the business or solicit investment. This draft **must be reviewed and validated by qualified finance, commercial, tax, and legal advisers, and all figures replaced with the platform's own validated data, before any reliance, fundraising, or decision.** Nothing here is investment advice or an offer of securities.

On "latest releases." Market-size forecasts and on-chain adoption figures move fast and vary widely by source and methodology. Every external figure was re-verified on the date of documentation and recorded in **Appendix A — Market Data & Sources Register**, with its source and framing; all must be re-checked before reliance.

HOW TO READ THIS VOLUME (CONTROL FILE)

Condensed Control File, reproduced atop every volume after Volume I.

Canonical terms (do not substitute synonyms). The instrument is a **ledger-based security** (Vol. I §4.1) implemented as an **ERC-3643 permissioned token** (Vol. II §3). "TAM/SAM/SOM" = total / serviceable / obtainable market. "AUM" = assets under management/administration on the platform. "Take rate" = platform revenue as a share of value transacted or administered. "The platform" denotes the infrastructure as a whole. A "platform token," if any, is discussed as a design option in §4 and is distinct from the asset tokens.

Cross-volume reference map.

Volume	Scope	Relationship to this volume
I	Executive & Regulatory	Licensing, jurisdictions, and constraints that shape the model
II	Technical Architecture	The build whose cost this volume plans
III	Marketplace & Trading	The venue whose liquidity drives

Volume	Scope	Relationship to this volume
		trading revenue
IV	Financial Intelligence	Valuation/NAV and risk discipline consumed by the financial model
V	Security & Operations	The operating cost base (security, custody, resilience)
VI	**Business & Financial Model (this volume)**	**Market, revenue, tokenomics, unit economics, costs, funding, roadmap**
VII	Architecture Atlas	Consolidates this volume's diagrams

Rule set (unchanged). No fabricated facts or citations; external figures verified against sources and registered in Appendix A with framing; the platform's own projections labelled illustrative; design options labelled with trade-offs; commentary paraphrased; hyperlinks only to official/primary sources verified live on the date of documentation, all other sources cited by stable identifier.

DETAILED TABLE OF CONTENTS

- Principles & the Business-Model Frame
- Market Opportunity (TAM / SAM / SOM)
- Value Proposition & Competitive Position
- Revenue Model & Tokenomics
- Unit Economics
- Financial Model & Scenarios
- Cost & Capacity Planning
- Funding & Capital Requirements
- Roadmap & Phasing
- Key Risks to the Business Model
- KPIs & Model Governance
- Limitations & Threats Register

109. Interim Compliance & Completeness Audit (Volume VI)
110. Future Jurisdiction & Technology Compatibility Notes
111. Glossary
112. Appendices A–E
113. Diagram Inventory

LIST OF FIGURES

Figure	Title	Section
1	Business-model frame & value flow	1.3
2	TAM / SAM / SOM funnel	2.3
3	The forecast-vs-reality gap	2.4
4	Value proposition by participant	3.2
5	Revenue streams	4.2
6	Platform-token decision tree	4.4
7	Unit economics of an issuance	5.2
8	Scenario ranges (illustrative)	6.3
9	Cost structure (build vs run)	7.2
10	Funding stages & capital	8.2
11	Phased roadmap	9.2
12	KPI tree	11.2

LIST OF TABLES

Table	Title	Section
1	Business-model principles → mechanisms	1.4
2	External tokenization market-size estimates (attributed)	2.2
3	Revenue streams & drivers	4.2
4	Illustrative issuance unit economics	5.2
5	Financial-model drivers & scenarios	6.2
6	Cost categories (build vs run)	7.2
7	Roadmap phases & gates	9.2
8	Business-model risks	10.1
9	Business-model threats/limitations register	12.1

EXECUTIVE SUMMARY

The preceding volumes design an institution-grade infrastructure for tokenised real-estate securities. This volume asks the commercial questions: who pays, for what, how much, at what cost, and on what path — and it answers them with deliberate honesty about a market that is simultaneously enormous in projection and tiny in reality.

Five decisions frame the volume. **First, honesty over hype.** External forecasts for tokenised real-world assets (RWAs) span an order of magnitude — from McKinsey's roughly $2 trillion by 2030 (base case, excluding stablecoins) to Boston Consulting Group's $16 trillion and Standard Chartered's ~$30 trillion by 2034 — because they measure different things (asset value vs business opportunity vs demand, with or without the "money layer").[225][226] Against those projections, the **current on-chain reality is about $40 billion of tokenised RWAs (excluding stablecoins) as of mid-2026**, dominated by Treasuries and private credit, with **tokenised real estate still nascent** — the best-known retail platforms remain under $100 million on-chain.[227] The platform's business model is built for that gap, not for the headline. **Second, a two-sided value proposition.** The platform serves asset owners/issuers (access to capital, efficient structuring, distribution) and investors (access, fractional exposure, transparency, compliant settlement), and its economics depend on serving both. **Third, diversified, mostly usage-based revenue** — issuance/structuring, venue/trading, servicing/administration, custody, and data — rather than reliance on a single stream or on speculative token economics; any platform token is examined as a design option with heavy caveats, not assumed. **Fourth, a cost base dominated by trust** —

---

[225] McKinsey & Company, "The tides of tokenization" — base-case tokenised-asset value of roughly $2tn by 2030 (range ~$1–4tn), ~$3.0tn including cash and deposits, excluding stablecoins/CBDCs and native crypto. Verified live: https://www.mckinsey.com/featured-insights/week-in-charts/the-tides-of-tokenization

[226] Third-party tokenisation market-size forecasts, cited by named source and year, with wide methodology-driven variance: Boston Consulting Group + ADDX (2022) ~$16tn by 2030 ("business opportunity" framing; best case up to ~$68tn; ~10% of global GDP); BCG + Ripple (2025) ~$9.4tn by 2030 and ~$18.9tn by 2033 (including the "money layer" of deposits/stablecoins; ~$6.4tn non-currency by 2030); Standard Chartered (with Synpulse) ~$30tn by 2034 (broad, demand-led); Citi and Bernstein ~$5tn (2030 / 2028). These are external estimates measuring different things, not guarantees; cited by identifier.

[227] rwa.xyz — analytics on tokenised real-world assets. As of 30 June 2026, on-chain tokenised RWAs total roughly $40bn in distributed value excluding stablecoins, led by tokenised US Treasuries and private credit, with 6+ asset classes each above $1bn; tokenised real estate remains nascent (best-known retail platforms under $100m on-chain). Figures for illiquid assets are best-available estimates. Verified live: https://app.rwa.xyz/

security, custody, audits, oracle and resilience (Vol. V), compliance, and people — that must be funded continuously and scales sub-linearly with volume. **Fifth, a phased roadmap** anchored in Switzerland first (Vol. I), gated on the technical, market, and operational readiness of the prior volumes, with liquidity — the sector's central unsolved problem — treated as the make-or-break risk.

The chapters develop the model frame; the market (TAM/SAM/SOM with a candid forecast-vs-reality section); the value proposition and competitive position; the revenue model and tokenomics; unit economics; an illustrative financial model with scenario ranges; cost and capacity planning; funding and capital requirements; the phased roadmap; business-model risks; KPIs and governance; and an honest limitations register. Every forward-looking number is an illustrative assumption to be replaced with validated data.

CHAPTER 1 — PRINCIPLES & THE BUSINESS-MODEL FRAME

1.1 What this volume is — and is not

This volume frames how the infrastructure becomes a viable business. It is **not** a forecast of results, a valuation of the enterprise, or an offer of securities; every forward-looking figure is an **illustrative assumption** meant to structure thinking and be replaced by the platform's own validated data. That discipline is not a disclaimer of convenience — it is the same truthfulness standard applied to the legal and technical volumes, extended to commercial claims, where over-optimistic projection is the characteristic failure mode of the sector.

1.2 The value the platform captures — and the value it must first create

A capital-markets infrastructure earns by **reducing friction** in the issuance, distribution, servicing, custody, and trading of securities. But in tokenised real estate the platform must first *create* value that does not yet reliably exist — chiefly **liquidity and trust** — before it can capture a share of it. The model therefore couples revenue to activities that genuinely lower cost or unlock access (structuring, compliant distribution, atomic settlement, transparent servicing), and treats the creation of a credible, liquid, well-governed venue as the precondition for revenue, not a by-product.

1.3 The business-model frame

Figure 1 — Business-model frame and value flow.

Asset owners bring assets and pay to issue and distribute; investors bring capital and pay to access and trade; the platform sits between, earning across issuance, venue, servicing, and custody while delivering capital access to one side and compliant, transparent exposure to the other.

1.4 Principles and mechanisms

Principle	Mechanism	Reference
Honesty over hype	Illustrative projections; attributed external data; candid gap analysis	§2, §6
Serve both sides	Value proposition for issuers and investors	§3
Diversified, usage-based revenue	Multiple fee streams; token only as an option	§4
Liquidity is the product	Venue depth (Vol. III) as precondition for revenue	§2.4, §3, §10
Trust is the cost base	Security/custody/audit/compliance funded continuously	§7
Phased, gated growth	Switzerland first; readiness gates; jurisdiction sequencing	§9
Manage the real risks	Liquidity, adoption, regulatory, concentration	§10

Table 1 — Business-model principles → mechanisms.

CHAPTER 2 — MARKET OPPORTUNITY (TAM / SAM / SOM)

2.1 A market defined by a gap

The tokenised-asset opportunity is genuinely large in the underlying market and genuinely small in current realisation. Global real estate is one of the largest asset classes on earth (measured in the hundreds of trillions of dollars), yet only tens of billions of dollars of *all* real-world assets are tokenised on-chain today. The honest way to size this market is to state both the ceiling and the floor, and to be explicit about the assumptions that would move the platform from floor toward ceiling.

2.2 The ceiling: external forecasts (attributed, with variance)

Third-party forecasts for the tokenised-RWA market vary by more than an order of magnitude, chiefly because they measure different things.

Source (year)	Figure	Timeframe	What it measures
McKinsey	~$2T base (range $1–4T); ~$3.0T incl. cash/deposits	2030	Tokenised assets excl. stablecoins/CBDCs[228]
BCG + ADDX	~$16T (best case up to ~$68T)	2030	“Business opportunity” framing; ~10% of global GDP[229]
BCG + Ripple	~$9.4T; ~$18.9T	2030; 2033	Incl. “money layer”; ~$6.4T non-currency by 2030[230]
Standard Chartered	~$30T	2034	Broad, demand-led (trade-

[228] McKinsey & Company, “The tides of tokenization” — base-case tokenised-asset value of roughly $2tn by 2030 (range ~$1–4tn), ~$3.0tn including cash and deposits, excluding stablecoins/CBDCs and native crypto. Verified live: https://www.mckinsey.com/featured-insights/week-in-charts/the-tides-of-tokenization

[229] Third-party tokenisation market-size forecasts, cited by named source and year, with wide methodology-driven variance: Boston Consulting Group + ADDX (2022) ~$16tn by 2030 (“business opportunity” framing; best case up to ~$68tn; ~10% of global GDP); BCG + Ripple (2025) ~$9.4tn by 2030 and ~$18.9tn by 2033 (including the “money layer” of deposits/stablecoins; ~$6.4tn non-currency by 2030); Standard Chartered (with Synpulse) ~$30tn by 2034 (broad, demand-led); Citi and Bernstein ~$5tn (2030 / 2028). These are external estimates measuring different things, not guarantees; cited by identifier.

[230] Third-party tokenisation market-size forecasts, cited by named source and year, with wide methodology-driven variance: Boston Consulting Group + ADDX (2022) ~$16tn by 2030 (“business opportunity” framing; best case up to ~$68tn; ~10% of global GDP); BCG + Ripple (2025) ~$9.4tn by 2030 and ~$18.9tn by 2033 (including the “money layer” of deposits/stablecoins; ~$6.4tn non-currency by 2030); Standard Chartered (with Synpulse) ~$30tn by 2034 (broad, demand-led); Citi and Bernstein ~$5tn (2030 / 2028). These are external estimates measuring different things, not guarantees; cited by identifier.

Source (year)	Figure	Timeframe	What it measures
			finance heavy)[231]
Citi / Bernstein	~$5T	2030 / 2028	Tokenised assets[232]

Table 2 — External tokenization market-size estimates (attributed). These are **external estimates, not guarantees**, and the spread itself is the message: the conservative, assets-only view is low-single-digit trillions; the largest numbers appear when a report counts broader categories or the money layer. The platform plans against the **conservative** end and treats the upside as optionality.

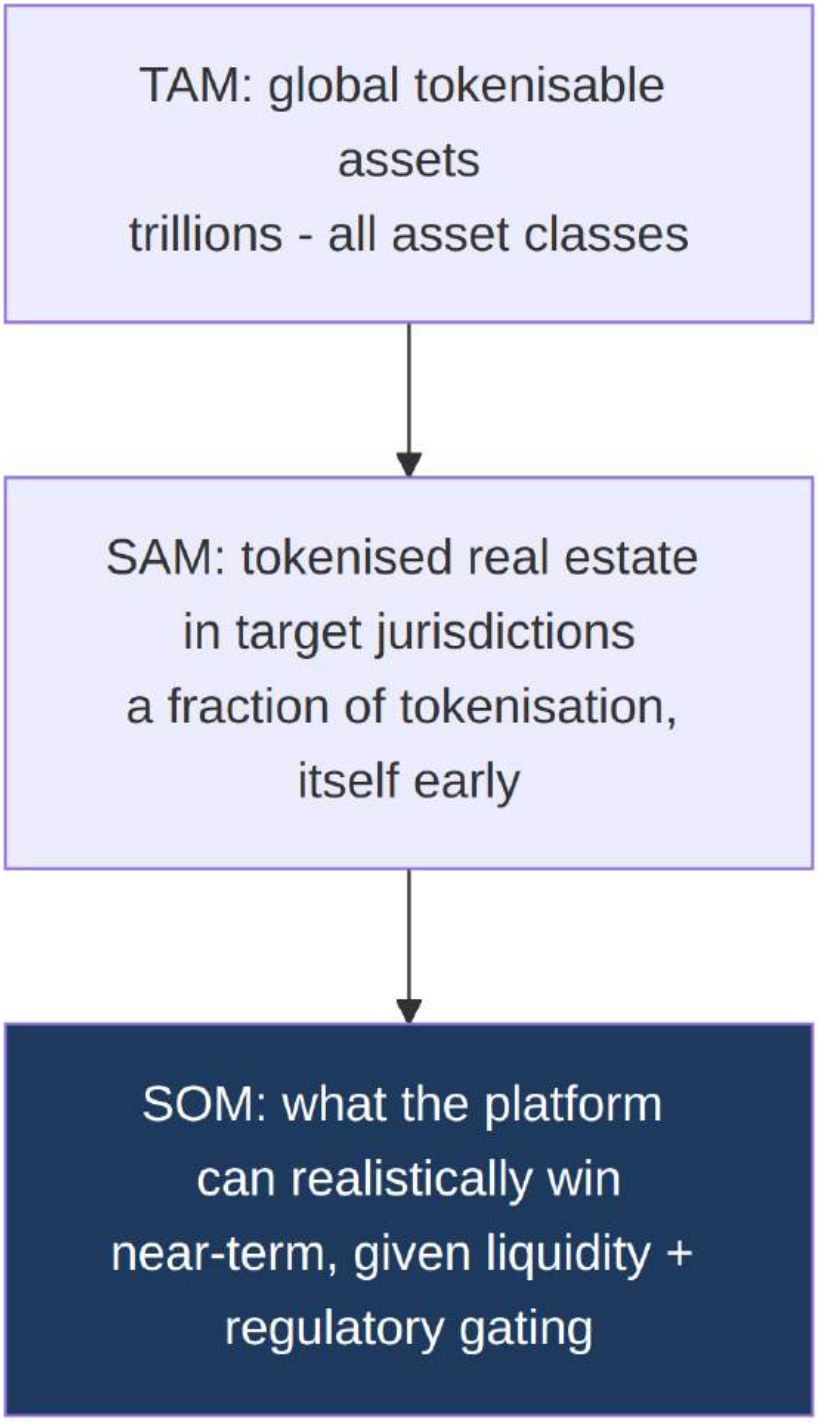
2.3 From TAM to SOM

The platform's addressable market narrows sharply from the headline.

Figure 2 — TAM / SAM / SOM funnel.

[231] Third-party tokenisation market-size forecasts, cited by named source and year, with wide methodology-driven variance: Boston Consulting Group + ADDX (2022) ~$16tn by 2030 ("business opportunity" framing; best case up to ~$68tn; ~10% of global GDP); BCG + Ripple (2025) ~$9.4tn by 2030 and ~$18.9tn by 2033 (including the "money layer" of deposits/stablecoins; ~$6.4tn non-currency by 2030); Standard Chartered (with Synpulse) ~$30tn by 2034 (broad, demand-led); Citi and Bernstein ~$5tn (2030 / 2028). These are external estimates measuring different things, not guarantees; cited by identifier.

[232] Third-party tokenisation market-size forecasts, cited by named source and year, with wide methodology-driven variance: Boston Consulting Group + ADDX (2022) ~$16tn by 2030 ("business opportunity" framing; best case up to ~$68tn; ~10% of global GDP); BCG + Ripple (2025) ~$9.4tn by 2030 and ~$18.9tn by 2033 (including the "money layer" of deposits/stablecoins; ~$6.4tn non-currency by 2030); Standard Chartered (with Synpulse) ~$30tn by 2034 (broad, demand-led); Citi and Bernstein ~$5tn (2030 / 2028). These are external estimates measuring different things, not guarantees; cited by identifier.



Total tokenisable assets narrow to tokenised real estate in the platform's licensed jurisdictions (a small, early slice), and narrow again to what a single compliant venue can realistically capture in the near term. The obtainable market is small in absolute terms today and depends on solving liquidity.

- **TAM** — all tokenisable assets (the trillions above), the outer bound only.
- **SAM** — tokenised real-estate securities in the platform's target jurisdictions (Switzerland first, then selected EEA/UAE/Asia per Vol. I). Real estate is projected to be a large tokenised category over time, but is one of the least-developed today.
- **SOM** — the share a single, compliant, well-governed venue can realistically obtain in the near term: modest, concentrated in a few high-quality issuances, and constrained by liquidity, distribution reach, and regulatory gating.

2.4 The floor: forecast versus reality

Honesty requires stating today's reality next to the forecasts. As of mid-2026, on-chain tokenised RWAs total roughly **$40 billion excluding stablecoins**, dominated by tokenised US Treasuries and private credit; six-plus asset classes have each passed $1 billion, but **tokenised real estate remains nascent** — the best-known retail real-estate platforms remain **under $100 million** on-chain, a rounding error against the multi-trillion physical market.[233] The reasons are structural and must be respected by any credible plan: real estate's legal complexity does not vanish when a token is issued (most jurisdictions still require conventional title transfer for legal ownership change — Vol. I), and, above all, **tokenisation does not by itself create liquidity** — most tokenised RWAs show low trading volumes, long holding periods, and thin secondary markets.

Figure 3 — The forecast-vs-reality gap.

The distance between today's ~$40bn and the multi-trillion forecasts is both the opportunity and the risk; it is bridged only by solving liquidity, trust, regulatory clarity, and distribution — not by tokenisation alone. The platform's strategy (Vols. II–V) targets exactly these bridges.

[233] rwa.xyz — analytics on tokenised real-world assets. As of 30 June 2026, on-chain tokenised RWAs total roughly $40bn in distributed value excluding stablecoins, led by tokenised US Treasuries and private credit, with 6+ asset classes each above $1bn; tokenised real estate remains nascent (best-known retail platforms under $100m on-chain). Figures for illiquid assets are best-available estimates. Verified live: https://app.rwa.xyz/

The commercial implication: the platform must **not** underwrite its plan on the headline forecasts. It should target a modest, defensible SOM, win on quality and compliance, and treat liquidity as the metric that determines whether the market — and the business — actually materialises (§10, §11).

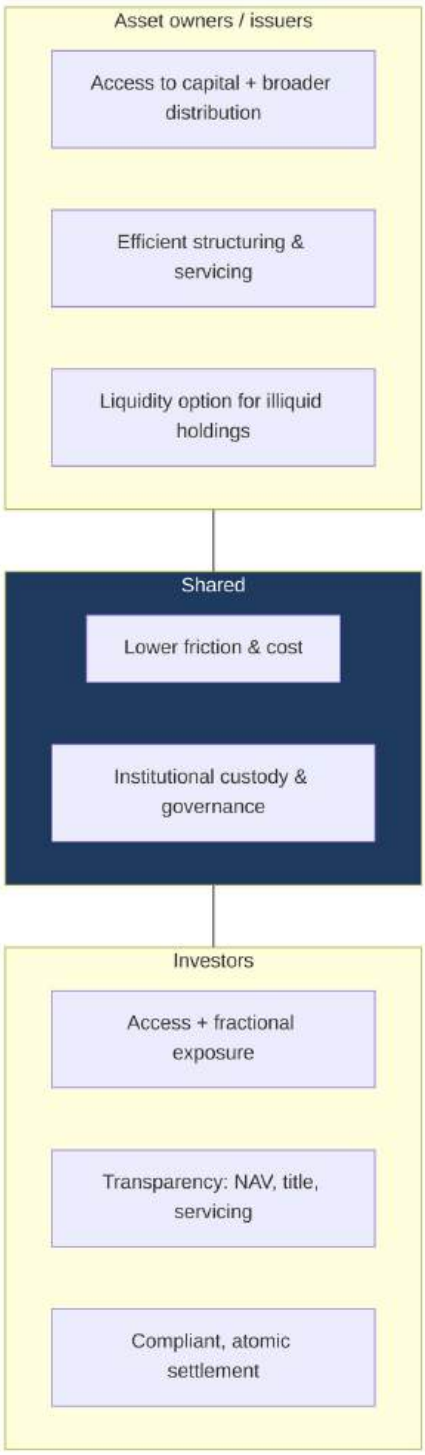
CHAPTER 3 — VALUE PROPOSITION & COMPETITIVE POSITION

3.1 Problems solved, and for whom

The platform's value proposition rests on frictions that are real in real-estate capital markets: **access** (high minimums and closed distribution exclude most investors and lock up issuer capital), **settlement** (slow, intermediated, reconciliation-heavy), **transparency** (opaque ownership, valuation, and servicing), and **compliance** (costly, manual, jurisdiction-by-jurisdiction). The platform addresses these with fractionalisation, atomic DvP settlement (Vol. III), on-chain transparency with off-chain privacy (Vols. I–II), and compliance-by-construction (ERC-3643 — Vol. II §3). Crucially, it does so for **institutional** standards of custody, valuation, and resilience, which is where crypto-native real-estate efforts have generally been weakest.

3.2 Value by participant

Figure 4 — Value proposition by participant.



Issuers gain capital access, efficiency, and an optional liquidity path; investors gain access, transparency, and compliant settlement; both gain lower friction and institutional-grade custody and governance — the differentiator against less-regulated alternatives.

3.3 Competitive position and honest threats

The platform competes on three fronts (developed in Vol. I): **incumbent capital-markets infrastructure** (CSDs, exchanges, fund administrators) that is trusted but not yet tokenised and may itself tokenise; **regulated tokenisation venues and DLT market infrastructures** (e.g. Swiss DLT trading facilities, the EU DLT Pilot Regime, and bank-led efforts) that share the platform's compliance posture; and **crypto-native real-estate platforms** that reach retail but often lack institutional custody, valuation, and legal robustness. The platform's chosen ground is **institutional trust plus genuine compliance-by-construction** — but this is contested ground, and the honest threats are that incumbents tokenise faster, that a better-capitalised regulated venue wins the liquidity network effect first, or that the whole real-estate-tokenisation thesis under-delivers on liquidity (§10). The platform's defensibility rests on execution quality, regulatory standing, and being early to a *credible* (not merely a *cheap*) venue.

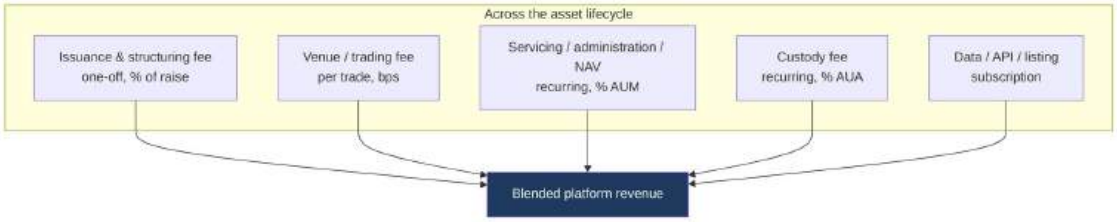
CHAPTER 4 — REVENUE MODEL & TOKENOMICS

4.1 Diversified, mostly usage-based

The platform earns across the lifecycle of a tokenised security rather than from a single event, and prefers **usage-based** fees (tied to value issued, administered, or traded) over speculative or one-off economics. Diversification matters because any single stream is fragile in an early market: issuance is lumpy, trading is thin until liquidity builds, and servicing revenue accrues slowly. A blended model smooths this and aligns platform revenue with genuine activity.

4.2 Revenue streams

Figure 5 — Revenue streams.



Revenue accrues at issuance, on trading, and recurringly on assets under administration and custody, plus data/listing — so the platform is not dependent on any single event or on trading volumes that take time to build.

Stream	Basis	Character	Notes (illustrative)
Issuance / structuring	% of amount raised	One-off, lumpy	Higher touch for first

Stream	Basis	Character	Notes (illustrative)
			issuances; scales with reuse
Venue / trading	bps per trade	Usage; thin early	Grows only as liquidity builds (§10)
Servicing / administration / NAV	% of AUM p.a.	Recurring	The compounding, stable core over time
Custody	% of assets under administration p.a.	Recurring	Tied to Vol. V custody offering
Data / API / listing	Subscription / fee	Recurring	Transparency and integrations as a product

Table 3 — Revenue streams and drivers. All fee levels are **illustrative** and must be set against market benchmarks and cost-to-serve; the platform's stance is to price for trust and reliability, not to undercut, given its institutional positioning (§3).

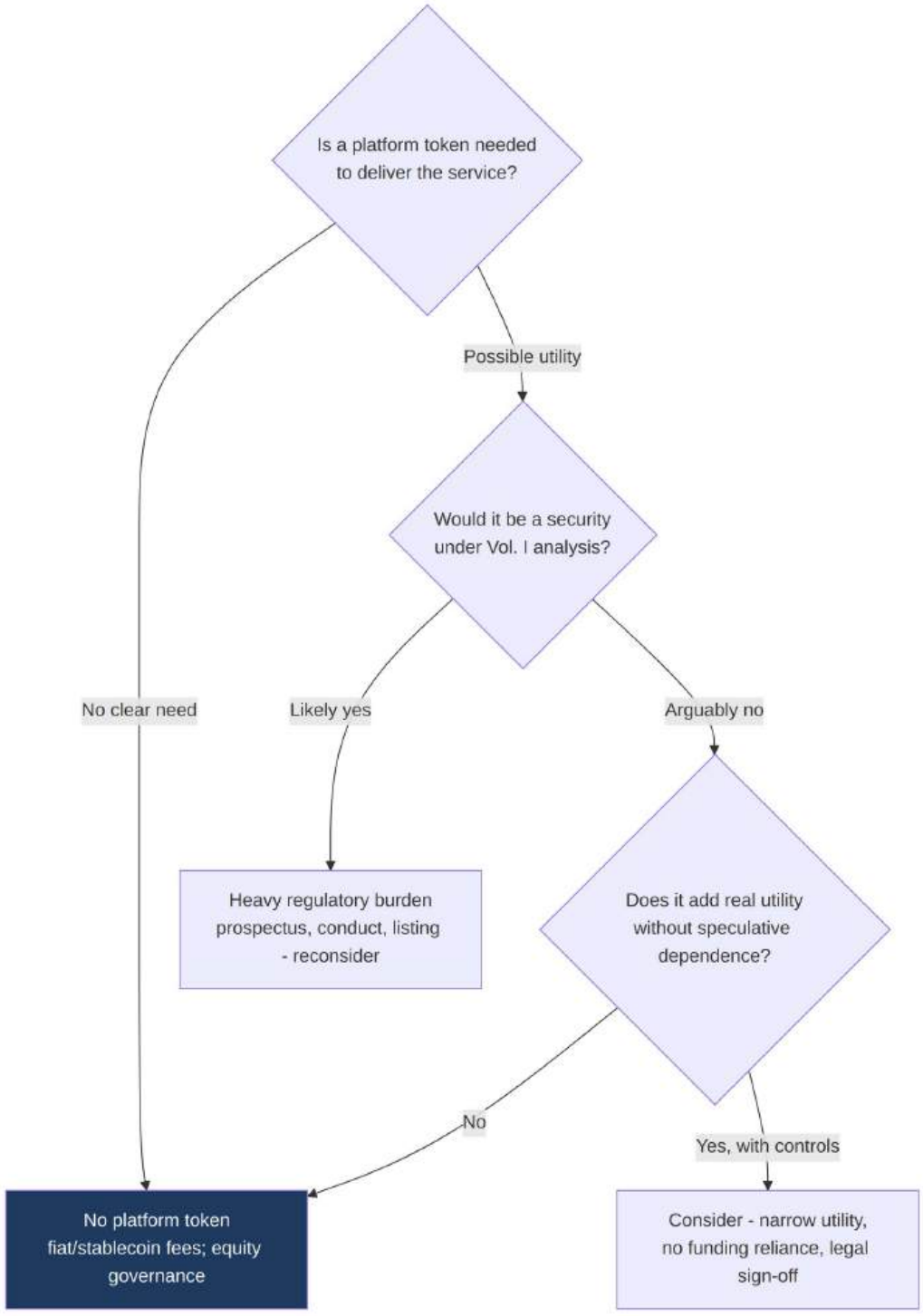
4.3 Alignment and honesty in pricing

Fees are disclosed transparently (consistent with Vol. I conduct rules) and structured to align the platform with client outcomes — recurring revenue rewards keeping assets well-administered and liquid, not merely issuing them. The platform avoids fee structures that depend on churn, opacity, or investor detriment.

4.4 Tokenomics: a platform token is an option, not an assumption

A recurring question is whether the platform should issue its own **platform token** (for access, fees, governance, or incentives). This is treated as a **design decision with serious trade-offs**, not a default. The asset tokens (the securities themselves) are unaffected by this question; the issue is purely whether a *separate* platform/utility token adds value.

Figure 6 — Platform-token decision tree.



The default is no platform token: fees are paid in fiat or regulated stablecoins and governance sits with the corporate entity. A token is considered only if it adds genuine, non-speculative utility and survives the securities analysis of Volume I — and never as a funding mechanism that would import speculative risk into a regulated capital-markets business.

The recommended posture is **no platform token at launch**: it avoids a large regulatory surface (a token that is itself a security triggers the full Vol. I regime), avoids tying the business to crypto-market sentiment, and keeps incentives clean. Any future token would require explicit legal clearance and a real utility case.

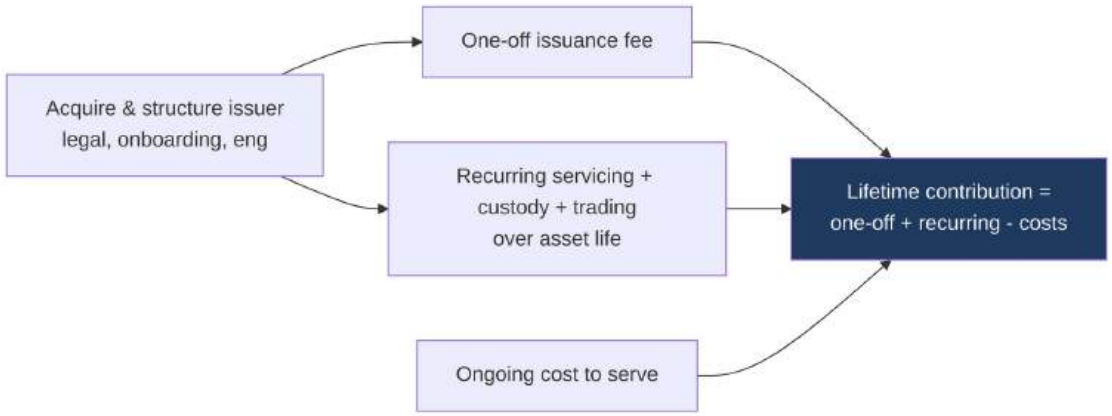
CHAPTER 5 — UNIT ECONOMICS

5.1 The unit is an issuance (and the assets it carries)

The platform's economics are best understood per **issuance** (an asset or portfolio brought on-platform) and per **unit of AUM** it generates over time. The first issuances are expensive (bespoke structuring, legal, onboarding, first-of-kind engineering); the marginal issuance is far cheaper as templates, integrations, and processes are reused. Recurring servicing/custody revenue then compounds on the resulting AUM. The model only works if **lifetime revenue per issuance exceeds fully-loaded cost to acquire and serve it** — the standard test, applied honestly.

5.2 Illustrative unit economics

Figure 7 — Unit economics of an issuance.



Each issuance carries an acquisition/structuring cost, earns a one-off fee plus recurring revenue over the asset's life, and nets to a lifetime contribution only if recurring economics outweigh the ongoing cost to serve. Early issuances may run at a loss by design; the model must show the crossover.

Line (illustrative, per issuance)	Direction	Comment
Amount raised / asset value	driver	Sets fee base
One-off issuance/structuring fee	+ revenue	Lumpy; higher for first-of-kind
Recurring servicing/NAV (% AUM	+ revenue	Compounds over asset life

Line (illustrative, per issuance)	Direction	Comment
p.a.)		
Recurring custody (% AUA p.a.)	+ revenue	Tied to custody offering
Trading fees	+ revenue	Only if liquidity builds
Acquisition + structuring cost	− cost	High early, falls with reuse
Ongoing cost to serve	− cost	Servicing, custody, compliance, support
Lifetime contribution	**=**	**Must be positive at steady state**

Table 4 — Illustrative issuance unit economics. All values are **illustrative placeholders**; the platform must populate them with its own validated data and market benchmarks before any reliance. The purpose here is the *structure* of the economics, not any specific number.

5.3 What has to be true

Three things must hold for the unit economics to work: **reuse** (structuring and engineering cost per issuance must fall sharply after the first few), **retention** (assets must stay on-platform long enough for recurring revenue to compound), and **liquidity** (trading revenue and issuer willingness both depend on a functioning secondary market). If liquidity fails to develop, the model must still stand on issuance plus recurring servicing/custody alone — a deliberately conservative test the plan should pass.

CHAPTER 6 — FINANCIAL MODEL & SCENARIOS

6.1 A driver-based model, not a point forecast

The financial model is built from **drivers**, not a single predicted trajectory: the number and size of issuances, resulting AUM, blended take rate, trading turnover, and the cost base. Because the market is early and uncertain (§2), the responsible output is a **range of scenarios** with explicit assumptions — not a confident forecast. This mirrors the risk discipline of Volume IV: show the distribution and the sensitivities, not a false-precision single line.

6.2 Drivers and scenarios

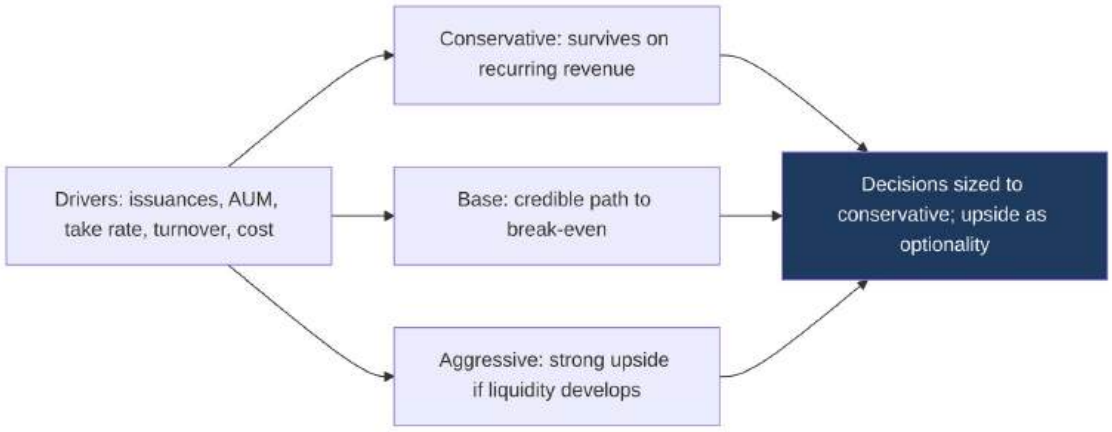
Driver	Conservative	Base	Aggressive
Issuances onboarded (per period)	few	moderate	many
Average issuance size	smaller	mid	larger

Driver	Conservative	Base	Aggressive
Cumulative AUM	low	moderate	high
Blended take rate	compressed	mid	firm
Trading turnover (liquidity)	minimal	building	active
Cost base	lean	scaling	scaling faster
Outcome	slow path to break-even	credible path	strong path (if liquidity comes)

Table 5 — Financial-model drivers and scenarios (illustrative). The scenarios are **planning aids, not predictions**; the conservative case deliberately assumes liquidity stays thin, so the business must survive on issuance and recurring revenue.

6.3 Reading the scenarios honestly

Figure 8 — Scenario ranges (illustrative).



The same drivers produce a range; the platform sizes commitments (hiring, capital, runway) to the conservative case and treats the base and aggressive cases as upside — the opposite of underwriting the plan on the headline forecasts.

The single most important sensitivity is **liquidity/turnover**, followed by **issuance volume** and **retention**; the model should show break-even under the conservative case and quantify how much faster the base and aggressive cases reach it. No scenario is presented as promised.

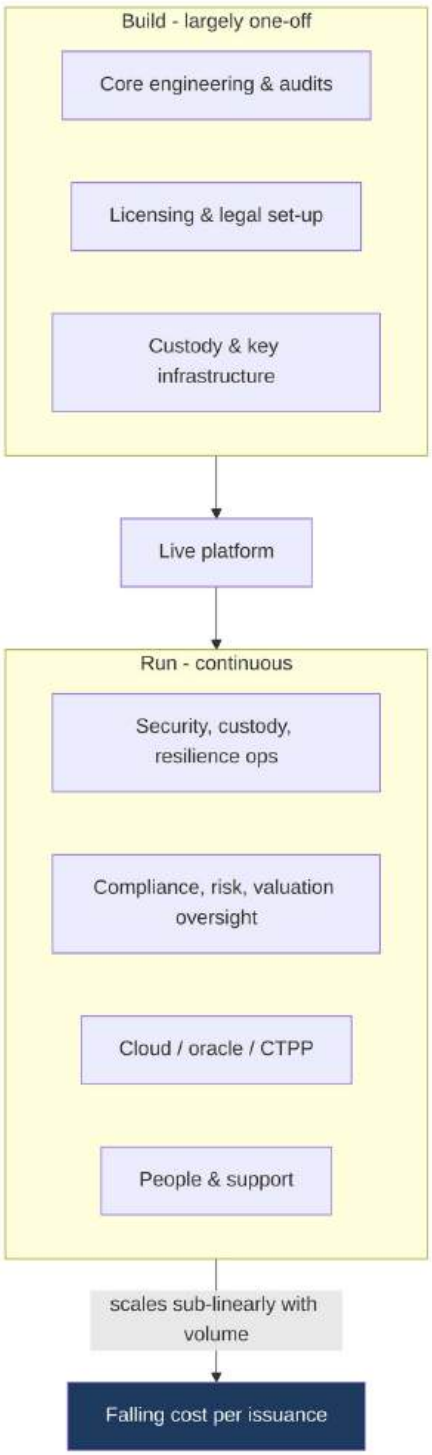
CHAPTER 7 — COST & CAPACITY PLANNING

7.1 A cost base dominated by trust

Unlike a typical software business, this platform's cost base is dominated by the things that make it trustworthy: **security and custody** (HSMs, key ceremonies, MPC — Vol. V), **audits and formal verification** (Vol. V §5–6), **oracle and infrastructure** (Vol. II §5, cloud/CTPP — Vol. V §11), **compliance and legal** (Vol. I), **operational resilience** (Vol. V §7–9), and **people** (engineering, risk, compliance, operations, valuation oversight). These are largely **fixed and continuous** — they must be funded whether or not volume arrives — which is why the plan is phased and cost-disciplined.

7.2 Build versus run

Figure 9 — Cost structure (build vs run).



Build costs are largely one-off (engineering, licensing, custody set-up); run costs are continuous (security, compliance, infrastructure, people). Because run costs scale sub-linearly with volume, cost per issuance falls as the platform grows — the source of operating leverage.

Category	Build / Run	Scales with volume?	Reference
Core engineering & audits	Build (+ ongoing)	Weakly	Vol. II, V
Licensing & legal set-up	Build	No	Vol. I
Custody & key infrastructure	Build + Run	Weakly	Vol. V §2–3
Security / resilience operations	Run	Weakly	Vol. V
Compliance / risk / valuation oversight	Run	Partly	Vol. I, IV
Cloud / oracle / CTPP	Run	Partly (usage)	Vol. II §5, V §11
People & support	Run	Partly	—

Table 6 — Cost categories (build vs run).

7.3 Capacity

Capacity is set by the scarcest resources: **skilled people** (security, compliance, valuation, engineering), **audit/validation throughput**, and **operational controls** (key ceremonies, onboarding). The plan scales capacity ahead of volume in controlled steps, avoiding both over-building (burning runway) and under-building (breaching the conservative controls that are the platform's whole value proposition). Third-party concentration (CTPP dependence — Vol. V §11) is a capacity and resilience constraint, not just a cost.

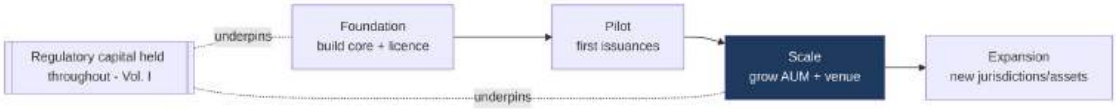
CHAPTER 8 — FUNDING & CAPITAL REQUIREMENTS

8.1 Two distinct capital needs

The platform needs capital for two different purposes: **development and runway** (building the infrastructure and funding operations to break-even) and **regulatory capital** (the own-funds a licensed entity must hold — Vol. I). These are not interchangeable, and regulatory capital in particular is a function of the licences held and the activities performed; the custody design deliberately keeps properly segregated client assets **off-balance-sheet** (Vol. V §2), which limits — but does not eliminate — capital requirements.

8.2 Funding stages and options

Figure 10 — Funding stages and capital.



Funding is staged to readiness gates (§9): foundation and licensing, pilot issuances, scaling AUM and the venue, then expansion — with regulatory capital held throughout, independent of growth funding.

Funding options carry the usual trade-offs: **equity** (aligned, patient, dilutive; suited to a trust-heavy, longer-horizon build), **strategic investment/partnership** (capital plus distribution or credibility; potential conflicts and dependence), and **debt** (non-dilutive but ill-suited to a pre-break-even, capital-regulated business). The plan favours patient equity and selective strategic partners, and explicitly **avoids funding models that would import speculative or crypto-market risk** into a regulated capital-markets business (consistent with the no-platform-token posture of §4.4).

8.3 Runway discipline

Because the cost base is largely fixed and revenue is back-loaded (recurring revenue compounds slowly; trading revenue waits on liquidity), **runway discipline** is existential: the platform must hold enough runway to reach the conservative-case milestones without assuming the base or aggressive case. Capital plans are sized to the conservative scenario (§6), with upside funding raised from strength, not necessity.

CHAPTER 9 — ROADMAP & PHASING

9.1 Gated, jurisdiction-sequenced growth

The roadmap is **phased and gated**: each phase must clear readiness gates (technical, regulatory, operational, commercial) before the next begins, and geographic expansion follows the licensing sequence of Volume I — **Switzerland first**, then selected EEA (via the DLT Pilot Regime / national regimes), the UAE, and Asia as licences and demand allow. This sequencing is deliberate: it concentrates early effort where the legal basis is clearest (Swiss DLT Act; ledger-based securities) and avoids spreading a trust-heavy build across regimes before the core is proven.

9.2 The phases

Figure 11 — Phased roadmap.

Each arrow is a gate: the platform does not move to pilot until it is audited, licensed, and custody is live; not to scale until issuance is repeatable and controls are proven; not to expansion until liquidity and unit economics stand up. Gates protect the conservative plan from optimism.

Phase	Focus	Exit gate	Depends on
0 — Foundation	Build core; audits; Swiss licence; custody	Audited, licensed, custody live	Vols. I, II, V
1 — Pilot	First issuances; limited investor base	Issuance repeatable; controls proven; TLPT-ready	Vols. III, IV, V
2 — Scale	Grow AUM; build venue liquidity	Liquidity building; unit economics positive	Vol. III §; §5–6
3 — Expand	New jurisdictions & asset types	Sustained metrics; capital in place	Vol. I; §8

Table 7 — Roadmap phases and gates.

9.3 Dependencies and sequencing risk

The roadmap consumes the whole package: the legal basis (Vol. I), the built infrastructure (Vol. II), the venue (Vol. III), valuation/NAV and risk (Vol. IV), and security/operations (Vol. V). The principal sequencing risk is **moving to scale before liquidity exists**; the gates are designed to prevent exactly that. A secondary risk is **over-expanding geographically** before the core jurisdiction is proven — hence Switzerland-first.

CHAPTER 10 — KEY RISKS TO THE BUSINESS MODEL

10.1 The risks that decide the outcome

#	Risk	Why it matters	Mitigation
1	**Liquidity fails to develop**	The sector's central unsolved problem; kills trading revenue and issuer appetite	Plan survives on issuance + recurring revenue (§5.3, §6); venue design (Vol. III); honest sizing
2	Slow adoption / long sales cycles	Institutional onboarding is slow; issuances lumpy	Conservative plan; diversified revenue; reuse to cut cost
3	Regulatory change / friction	Licensing, cross-border, tokenisation rules evolve	Switzerland-first; compliance-by-

#	Risk	Why it matters	Mitigation
			construction; watch items (Vol. I)
4	Competitive pre-emption	Incumbent or better-funded venue wins liquidity first	Early to a *credible* venue; execution and trust as moat (§3)
5	Cost overrun / runway	Fixed trust-heavy cost base; back-loaded revenue	Runway sized to conservative case; gated spend (§8)
6	Third-party / CTPP concentration	Dependence on few cloud/oracle providers	Multi-provider; exit plans (Vol. V §11)
7	Execution / key-person	Trust-heavy build needs scarce expertise	Phased capacity; governance; three lines (Vol. V)
8	Reputational / security event	One custody or security failure is existential	Vol. V controls; conservative posture; transparency
9	Over-optimism in planning	Underwriting on headline forecasts	This volume's core discipline: plan to the floor (§2, §6)

Table 8 — Business-model risks.

10.2 The one to watch

If a single risk determines success, it is **liquidity**. The platform can control its costs, its compliance, and its build quality; it cannot unilaterally manufacture a deep secondary market. The strategy therefore treats liquidity as the primary KPI (§11), designs the venue to encourage it (Vol. III), and — crucially — builds a business that is viable even if liquidity remains modest. That is the honest test of the model.

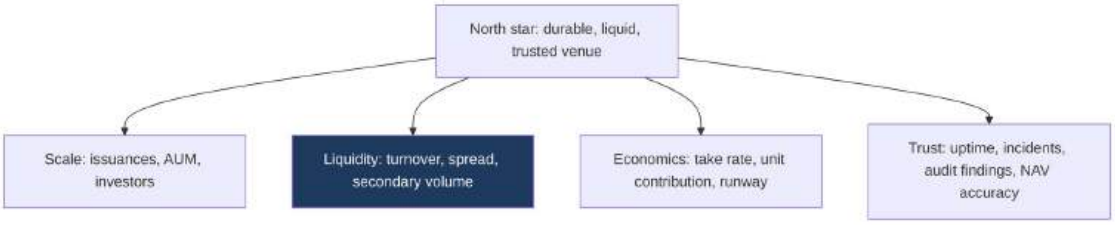
CHAPTER 11 — KPIs & MODEL GOVERNANCE

11.1 Measure what matters

The platform governs the business model with a small set of honest KPIs, led by the metrics that actually predict viability rather than vanity numbers. Assets tokenised and AUM measure scale; **liquidity/turnover** measures whether the market is real; unit economics measure whether growth is profitable; and operational/trust metrics (uptime, incident count, audit findings) measure whether the value proposition holds.

11.2 The KPI tree

Figure 12 — KPI tree.



The north star is a durable, liquid, trusted venue; beneath it sit scale, liquidity, economics, and trust metrics. Liquidity is highlighted because it is both the hardest to achieve and the most predictive of success.

11.3 Governing the model

The financial model is a **living, governed artefact**: assumptions are documented, dated, and owned; actuals are tracked against the illustrative scenarios; and the model is re-forecast on a regular cadence with variance analysis (the same discipline as Vol. IV model governance). Material assumption changes go to the board. The model is never presented internally or externally as a forecast of certain outcomes.

CHAPTER 12 — LIMITATIONS & THREATS REGISTER

12.1 Honest assessment

#	Threat / limitation	Exposure	Mitigation / status
1	Liquidity may never develop at scale	High	Business viable on issuance + recurring revenue; liquidity as primary KPI (§5.3, §6, §11)
2	Market forecasts are uncertain and varied	High	Plan to conservative floor; treat forecasts as external estimates (§2)
3	All projections are illustrative, not forecasts	High	Explicitly labelled; replace with validated data before reliance
4	Adoption slower than assumed	Medium-High	Conservative scenario; diversified revenue; reuse
5	Regulatory/licensing change	Medium-High	Switzerland-first; watch items (Vol. I)
6	Competitive pre-emption	Medium-High	Execution, trust, early-to-

#	Threat / limitation	Exposure	Mitigation / status
			credible-venue (§3)
7	Cost/runway risk	Medium-High	Gated spend; runway to conservative case (§8)
8	CTPP / third-party concentration	Medium	Multi-provider; exit plans (Vol. V §11)
9	Security/custody event	High (if realised)	Vol. V controls; conservative posture
10	Platform-token temptation	Medium	No token at launch; option gated by legal analysis (§4.4)

12.2 Honest limitations

This volume frames a business; it does not prove one. Every forward-looking figure is an illustrative assumption, and the most important external inputs (market size, adoption, liquidity) are uncertain and, in the case of tokenised real estate, currently very small. The model's defining virtue is that it is built to be **viable at the conservative floor** and to treat the large forecasts as upside rather than as the plan. Whether the market materialises is outside the platform's control; whether the platform is well-run, well-capitalised, trusted, and honest about its numbers is within it — and that is where this volume concentrates.

INTERIM COMPLIANCE & COMPLETENESS AUDIT — VOLUME VI

Verification performed. External market data was checked against public sources on 30 June 2026 and recorded in Appendix A: **current on-chain tokenised-RWA value (~$40bn excluding stablecoins; tokenised real estate nascent, leading retail platforms under $100m)** per rwa.xyz[234]; and **forecast ranges** — McKinsey ~$2tn base (range $1–4tn) by 2030[235]; BCG + ADDX ~$16tn (best case ~$68tn) by 2030; BCG +

[234] rwa.xyz — analytics on tokenised real-world assets. As of 30 June 2026, on-chain tokenised RWAs total roughly $40bn in distributed value excluding stablecoins, led by tokenised US Treasuries and private credit, with 6+ asset classes each above $1bn; tokenised real estate remains nascent (best-known retail platforms under $100m on-chain). Figures for illiquid assets are best-available estimates. Verified live: https://app.rwa.xyz/

[235] McKinsey & Company, "The tides of tokenization" — base-case tokenised-asset value of roughly $2tn by 2030 (range ~$1–4tn), ~$3.0tn including cash and deposits,

Ripple ~$9.4tn (2030) and ~$18.9tn (2033); Standard Chartered ~$30tn by 2034; Citi/Bernstein ~$5tn[236]. These are **third-party estimates with wide, methodology-driven variance**, presented as such.

No fabricated figures. No market figure has been invented; every external number is attributed to a named source with its framing, and **all of the platform's own projections, unit economics, and scenarios are explicitly labelled illustrative** — not forecasts, valuations, or offers.

Open / flagged items for specialist sign-off. 1. All financial figures, fee levels, unit economics, and scenarios — replace with the platform's validated data and market benchmarks; finance/commercial sign-off (§4–6). 2. Regulatory-capital requirements — confirm with counsel against the specific licences held (§8; Vol. I). 3. Platform-token decision — legal clearance required before any consideration (§4.4; Vol. I). 4. Market-size assumptions — re-verify sources and framing before any external use (§2). 5. Fee/tax treatment of each revenue stream — confirm with tax and legal advisers (§4).

Link policy. Hyperlinks point only to sources verified live on 30 June 2026 (rwa.xyz for current on-chain data; McKinsey for its forecast). Other forecasts (BCG, Ripple, Standard Chartered, Citi, Bernstein) are cited by named source and year without hyperlink.

FUTURE JURISDICTION & TECHNOLOGY COMPATIBILITY NOTES

Market watch items. (a) **On-chain adoption** — track rwa.xyz and equivalent trackers; the tokenised-real-estate figure is the single most informative number for this platform's SAM. (b) **Forecast revisions** — the major houses revise frequently; re-verify before planning. (c) **Liquidity venues** — watch regulated secondary venues (Vol. III) whose success or failure is the leading indicator for this business. (d) **Stablecoin/settlement**

---

excluding stablecoins/CBDCs and native crypto. Verified live: https://www.mckinsey.com/featured-insights/week-in-charts/the-tides-of-tokenization

[236] Third-party tokenisation market-size forecasts, cited by named source and year, with wide methodology-driven variance: Boston Consulting Group + ADDX (2022) ~$16tn by 2030 ("business opportunity" framing; best case up to ~$68tn; ~10% of global GDP); BCG + Ripple (2025) ~$9.4tn by 2030 and ~$18.9tn by 2033 (including the "money layer" of deposits/stablecoins; ~$6.4tn non-currency by 2030); Standard Chartered (with Synpulse) ~$30tn by 2034 (broad, demand-led); Citi and Bernstein ~$5tn (2030 / 2028). These are external estimates measuring different things, not guarantees; cited by identifier.

rails — regulated settlement-asset developments materially affect trading economics (Vols. III, V).

Model watch items. Keep the financial model driver-based and re-forecast on cadence; as real data accrues, replace illustrative assumptions and narrow the scenario ranges. Revisit the platform-token decision only if a genuine, legally-cleared utility case emerges.

GLOSSARY

Covers terms introduced in this volume; master glossary in Vol. I. Canonical reminder: the instrument is a **ledger-based security** implemented as an **ERC-3643 permissioned token**; a "platform token," if ever used, is a separate design option (§4.4).

- **AUA / AUM** — assets under administration / management on the platform.
- **Base / conservative / aggressive case** — illustrative planning scenarios, not forecasts.
- **Blended take rate** — total platform revenue as a share of value transacted/administered.
- **CTPP** — Critical ICT Third-Party Provider (Vol. V §11); a concentration risk.
- **Lifetime contribution** — one-off plus recurring revenue less cost to serve, per issuance.
- **Liquidity / turnover** — the degree of active secondary trading; the platform's primary KPI.
- **Platform token** — an optional, separate token for the platform (not the asset tokens); default is none (§4.4).
- **SAM** — serviceable available market: tokenised real estate in target jurisdictions.
- **SOM** — serviceable obtainable market: what the platform can realistically win near-term.
- **TAM** — total addressable market: all tokenisable assets (outer bound only).
- **Unit economics** — the per-issuance revenue-versus-cost structure (§5).

APPENDIX A — MARKET DATA & SOURCES REGISTER

Authoritative register of external market data relied on, with framing. "Verified live 30 Jun 2026" means the source was retrieved on that date. Hyperlinks only to sources verified live; other sources cited by named source and year. All figures are external estimates; re-check before reliance.

#	Item	Figure & framing (as at 30 Jun 2026)	Source
A1	Current on-chain tokenised RWA value	~$40bn distributed value, excl. stablecoins; 6+ asset classes >$1bn; Treasuries/credit-led	rwa.xyz — https://app.rwa.xyz/ (verified live)
A2	Tokenised real estate today	Nascent; leading retail platforms under $100m on-chain; legal/liquidity constraints	rwa.xyz + industry reporting (verified live / cited)
A3	McKinsey forecast	~$2tn base (range $1–4tn) by 2030; ~$3.0tn incl. cash/deposits; excl. stablecoins/CBDCs	McKinsey, “The tides of tokenization” — https://www.mckinsey.com/featured-insights/week-in-charts/the-tides-of-tokenization (verified live)
A4	BCG + ADDX forecast	~$16tn by 2030 (business-opportunity framing); best case up to ~$68tn	BCG + ADDX (2022), cited by identifier
A5	BCG + Ripple forecast	~$9.4tn (2030); ~$18.9tn (2033); incl. money layer; ~$6.4tn non-currency by 2030	BCG + Ripple (2025), cited by identifier
A6	Standard Chartered forecast	~$30tn by 2034; broad, demand-led (trade-finance heavy)	Standard Chartered + Synpulse, cited by identifier
A7	Citi / Bernstein forecasts	~$5tn (2030 / 2028)	Citi; Bernstein, cited by identifier
A8	Global real estate context	Real estate among the largest global asset classes (hundreds of trillions)	General; confirm with primary data before reliance

APPENDIX B — ILLUSTRATIVE ASSUMPTION SET (TEMPLATE)

Structure only. All values to be populated with the platform’s validated data — none are provided here as figures, to avoid implying a forecast.

Assumption	Unit	Conservative	Base	Aggressive
Issuances per period	count	—	—	—

Assumption	Unit	Conservative	Base	Aggressive
Average issuance size	currency	—	—	—
Cumulative AUM	currency	—	—	—
Issuance fee	% of raise	—	—	—
Servicing/NAV fee	% AUM p.a.	—	—	—
Custody fee	% AUA p.a.	—	—	—
Trading fee	bps	—	—	—
Annual turnover (liquidity)	% AUM	—	—	—
Fixed run cost	currency p.a.	—	—	—
Break-even period	periods	—	—	—

APPENDIX C — KPI DEFINITIONS (INDICATIVE)

KPI	Definition	Why it matters
Assets tokenised / AUM	Value issued / administered	Scale
Secondary turnover	Traded value ÷ AUM	Liquidity — primary KPI (§11)
Blended take rate	Revenue ÷ value transacted/administered	Monetisation
Unit contribution	Lifetime revenue − cost to serve, per issuance	Profitability of growth
Runway	Months of operation funded	Survival
Uptime / incidents	Availability; security/ops events	Trust (Vol. V)
NAV accuracy	Valuation/oracle error rate	Trust (Vol. IV)

APPENDIX D — CITATION REGISTER (TABLE — VOLUME VI)

Sources relied on in Volume VI. P = primary/official; S = secondary (paraphrased only).

Ref	Source	Type	Used for	Verification note
rwaxyz	rwa.xyz — tokenised-RWA analytics	P	Current on-chain value; real-estate reality	Verified live 30 Jun 2026

Ref	Source	Type	Used for	Verification note
mckinsey	McKinsey — “The tides of tokenization”	P	Conservative forecast (~$2tn by 2030)	Verified live
forecasts	BCG+ADDX, BCG+Ripple, Standard Chartered, Citi, Bernstein	S	Forecast range & variance	Cited by named source and year

APPENDIX E — CROSS-REFERENCE INDEX

Topic	This volume	Other volumes
Regulatory basis / licensing / capital	§8, §9	Vol. I
Built infrastructure (cost of)	§7	Vol. II
Venue / trading / liquidity	§2.4, §3, §10	Vol. III
Valuation / NAV / risk discipline	§6, §11	Vol. IV
Security / custody / ops cost base	§7	Vol. V
Third-party / CTPP concentration	§7, §10	Vol. V §11
Diagrams consolidated	—	Vol. VII

DIAGRAM INVENTORY (Volume VI)

Fig.	Title	Mermaid type	Section
1	Business-model frame & value flow	flowchart	1.3
2	TAM / SAM / SOM funnel	flowchart	2.3
3	The forecast-vs-reality gap	flowchart	2.4
4	Value proposition by participant	flowchart	3.2
5	Revenue streams	flowchart	4.2
6	Platform-token decision tree	flowchart	4.4
7	Unit economics of an	flowchart	5.2

Fig.	Title	Mermaid type	Section
	issuance		
8	Scenario ranges (illustrative)	flowchart	6.3
9	Cost structure (build vs run)	flowchart	7.2
10	Funding stages & capital	flowchart	8.2
11	Phased roadmap	flowchart	9.2
12	KPI tree	flowchart	11.2

Volume VII consolidates all diagrams across volumes.

END OF VOLUME VI (interim draft)

Next: Volume VII — Architecture Atlas (an all-diagram consolidation of every figure across Volumes I–VI, with added C4 component/code and ER/class views). After Volume VII, a single cross-volume Compliance & Completeness Audit is applied across all seven volumes, forward references are resolved, registers are re-checked, and — on explicit request — the full package is compiled.

VOLUME VII — ARCHITECTURE ATLAS

Institutional Digital Real Estate Capital Markets Infrastructure

Multi-Volume Documentation Package — Volume VII of VII

TITLE PAGE & DOCUMENT CONTROL

Field	Detail
Document	Volume VII — Architecture Atlas (Consolidated Diagrams, C4, Data & Contract Models)
Package	Institutional Digital Real Estate Capital Markets Infrastructure (7 volumes)
Status	Working draft — a **visual reference** consolidating and extending the diagrams of Volumes I–VI; not a standalone specification
Version	VII-0.1 (interim; the cross-volume Compliance & Completeness Audit follows this volume)
Date of documentation	30 June 2026
Classification	Confidential — Draft
Companion volumes	All (I–VI); this volume is their visual index and synthesis

Authorship and reliance caveat (read first). This volume is an AI-assisted visual synthesis of Volumes I–VI. It introduces **no new external facts**: every architectural, legal, and quantitative statement traces to the verified Standards/Versions and Citation registers of the preceding volumes, which were checked against primary sources on their documentation dates. The atlas adds *notation* (C4 model views, entity-relationship, class, state, and sequence diagrams) and *consolidation*, not new claims. It remains a draft and **must be read together with Volumes I–VI and reviewed by the relevant specialists before reliance.** Diagrams are simplified for clarity and are not implementation-complete.

On "latest releases." Because this volume adds no new external facts, its currency is inherited from Volumes I–VI. The authoritative version and citation records live in those volumes' Appendix A registers and must be re-checked there before reliance.

HOW TO READ THIS ATLAS (CONTROL FILE)

Condensed Control File, reproduced atop every volume after Volume I.

Canonical terms (do not substitute synonyms). The instrument is a **ledger-based security** (Vol. I §4.1) implemented as an **ERC-3643 permissioned token** (Vol. II §3) on a **permissioned Avalanche L1** (Vol. II §2). Identity uses **ONCHAINID** (Vol. II §4); value/NAV arrives via the **decentralised oracle layer** (Vol. II §5); keys are protected by **MPC and FIPS 140-3 HSMs** (Vol. V). "The platform" denotes the infrastructure as a whole.

How this atlas is organised. Five parts: (1) the **C4 model** (context → container → component); (2) the **contract and data models** (code-level class diagram; entity-

relationship model; domain model); (3) **lifecycle, state and interactions** (the security's state machine and the core sequences); (4) **cross-cutting consolidated views** (end-to-end reference architecture, security/key, governance/assurance, trust boundaries); and (5) the **master diagram index** cataloguing all 86 figures across Volumes I–VI.

Notation legend. Flowcharts show structure and flow; **C4** views show software architecture at increasing zoom (Context/Container/Component/Code); **class** diagrams show contracts/types and their relationships; **ER** diagrams show data entities and cardinality; **state** diagrams show lifecycle; **sequence** diagrams show ordered interactions. Navy-filled nodes mark the most systemic elements.

Rule set (unchanged). No fabricated facts or citations; this volume introduces none, deriving all content from Volumes I–VI; diagrams are simplified; design options and their trade-offs are documented in the source volumes.

DETAILED TABLE OF CONTENTS

- The C4 Model — Context, Container, Component
- Contract & Data Models — Code, Entity-Relationship, Domain
- Lifecycle, State & Interactions
- Cross-Cutting Consolidated Views
- Master Diagram Index (Volumes I–VI)

128. Interim Note & Handover to the Cross-Volume Audit
129. Glossary (pointer)
130. Appendices A–B
131. Diagram Inventory (Volume VII)

LIST OF FIGURES (VOLUME VII)

Figure	Title	Section
1	C4 L1 — System context	1.1
2	C4 L2 — Container view	1.2
3	C4 L3 — Component: on-chain compliance & token suite	1.3
4	C4 L3 — Component: off-chain services & oracle	1.4
5	Code/Class — ERC-3643 contract model	2.1
6	Entity-relationship — platform data model	2.2

Figure	Title	Section
7	Domain class model — platform services	2.3
8	State — ledger-based security lifecycle	3.1
9	Sequence — primary issuance & compliant subscription	3.2
10	Sequence — secondary trade with atomic DvP	3.3
11	Sequence — NAV update & proof-of-reserve gating	3.4
12	End-to-end reference architecture	4.1
13	Security & key architecture (consolidated)	4.2
14	Governance & assurance (consolidated)	4.3
15	Trust boundaries & data classification	4.4

EXECUTIVE SUMMARY

Six volumes have established the legal basis, the technical architecture, the marketplace, the financial intelligence, the security and operations, and the business model of an institutional infrastructure for tokenised real-estate securities. This seventh volume is their **atlas**: a single, navigable visual reference that consolidates all 86 diagrams from Volumes I–VI and adds the higher-fidelity architectural notation the package had not yet shown in one place — the full **C4 model** down to component level, a **code-level class diagram** of the ERC-3643 contract suite, an **entity-relationship** model of the platform's data, a consolidated **state machine** for the security's lifecycle, and the core **interaction sequences** (issuance, atomic DvP trade, and NAV/oracle update).

The atlas introduces **no new facts**. Its purpose is synthesis and navigation: to let a reader see the whole system at a glance, zoom from context to component to code, understand the data and contract models precisely, follow the critical flows end-to-end, and locate any diagram in the package via the master index. It also serves as the visual input to the **cross-volume Compliance & Completeness Audit** that follows, by making cross-references, boundaries, and dependencies explicit in one place.

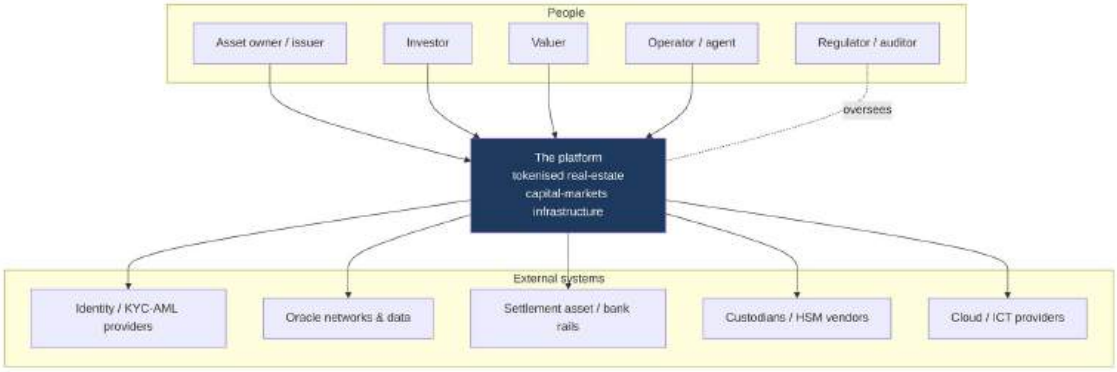
Read this volume last and alongside the others: each diagram is a compression of material specified and sourced in Volumes I–VI, simplified for clarity. The canonical facts, options, trade-offs, and citations remain in those volumes' registers.

CHAPTER 1 — THE C4 MODEL (CONTEXT → CONTAINER → COMPONENT)

The C4 model describes software architecture at four levels of zoom — **Context** (the system and its environment), **Container** (the major deployable/runtime pieces), **Component** (the parts inside a container), and **Code** (classes; §2.1). Volume II introduced Levels 1–2; this atlas consolidates them and adds the component level.

1.1 Level 1 — System context

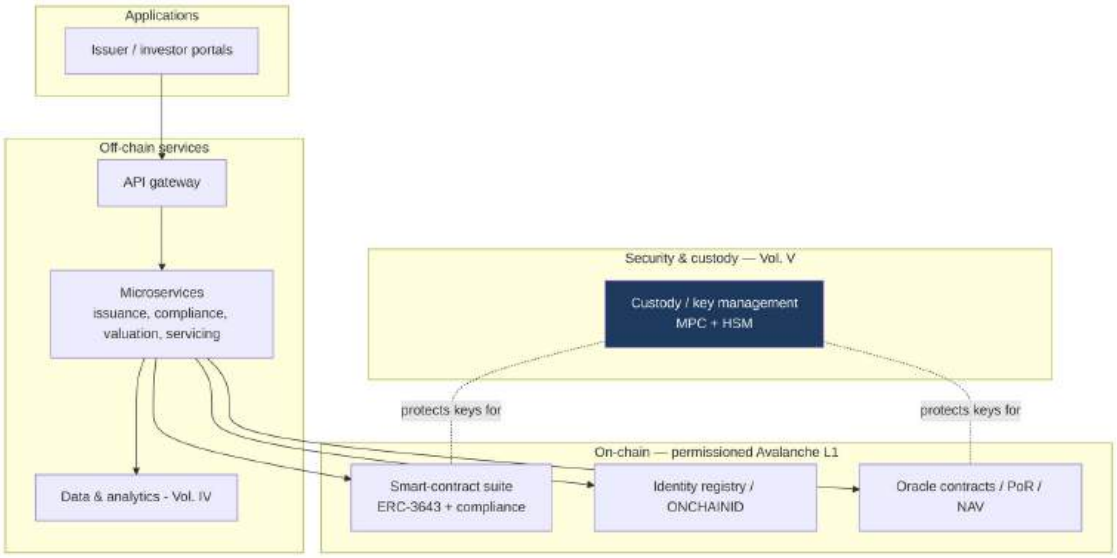
Figure 1 — C4 L1: System context.



The platform sits between the people who use it (issuers, investors, valuers, operators, overseen by regulators) and the external systems it depends on (identity, oracles, settlement, custody, cloud). Source: Vol. II Fig. 1.

1.2 Level 2 — Container view

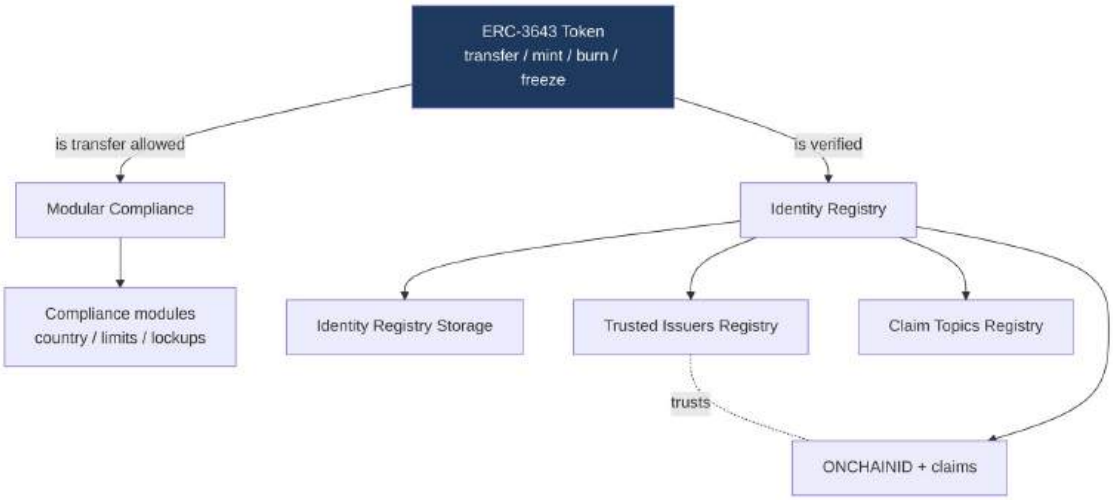
Figure 2 — C4 L2: Container view.



The major containers: the on-chain suite (contracts, identity, oracle) on the permissioned L1; off-chain services, API and data; the custody/key-management layer; and the applications. Source: Vol. II Figs. 2, 13.

1.3 Level 3 — Component: on-chain compliance & token suite

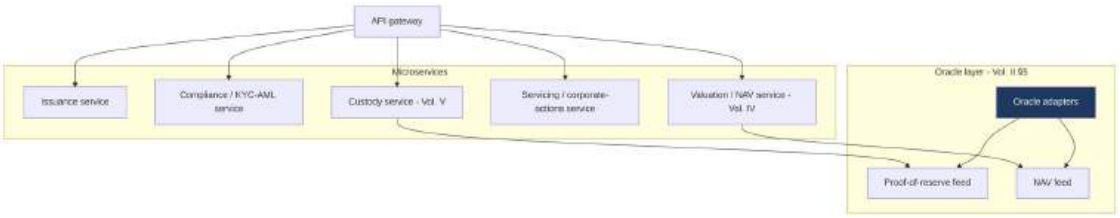
Figure 3 — C4 L3: Component — on-chain compliance & token suite.



Inside the contract container: every transfer asks the Identity Registry "is the party verified?" and Modular Compliance "is this transfer allowed?"; identity resolves through ONCHAINID claims, trusted issuers, and claim topics. Source: Vol. II Fig. 6.

1.4 Level 3 — Component: off-chain services & oracle

Figure 4 — C4 L3: Component — off-chain services & oracle.



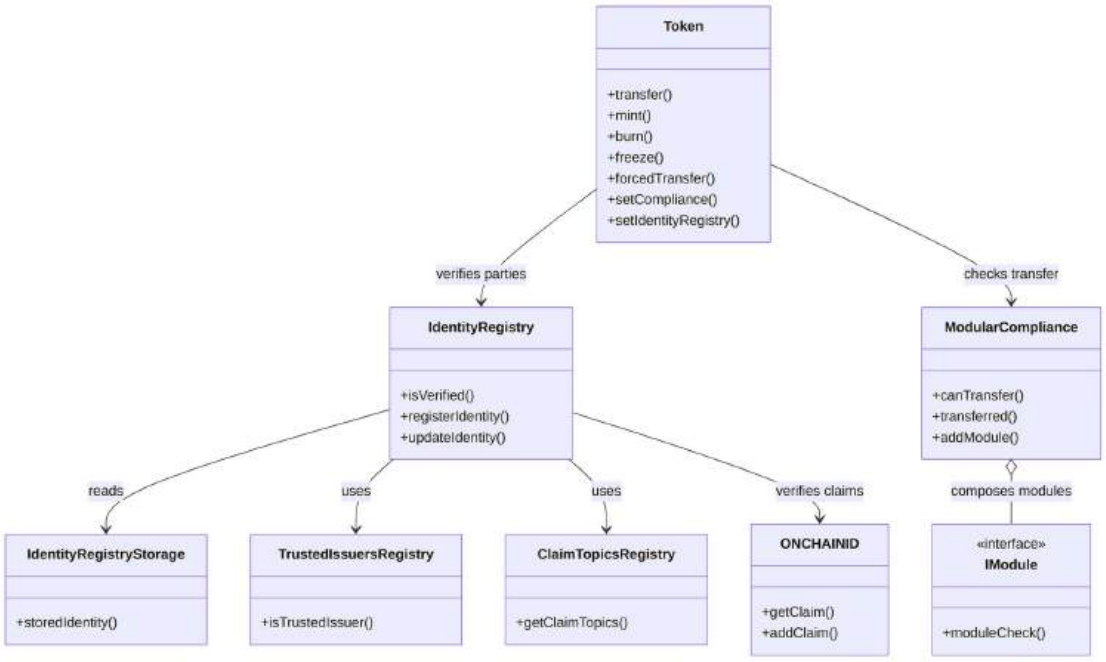
Inside the off-chain container: discrete services for issuance, compliance, valuation/NAV, servicing and custody, with the oracle layer bridging off-chain facts (reserves, NAV) to the chain. Source: Vol. II Figs. 12, 13.

CHAPTER 2 — CONTRACT & DATA MODELS (CODE · ENTITY-RELATIONSHIP · DOMAIN)

This chapter reaches the deepest C4 level (Code) and adds the data and domain models that the flow-oriented diagrams of Volumes I–VI implied but did not draw explicitly.

2.1 Code — the ERC-3643 contract model

Figure 5 — Code/Class: ERC-3643 contract model.

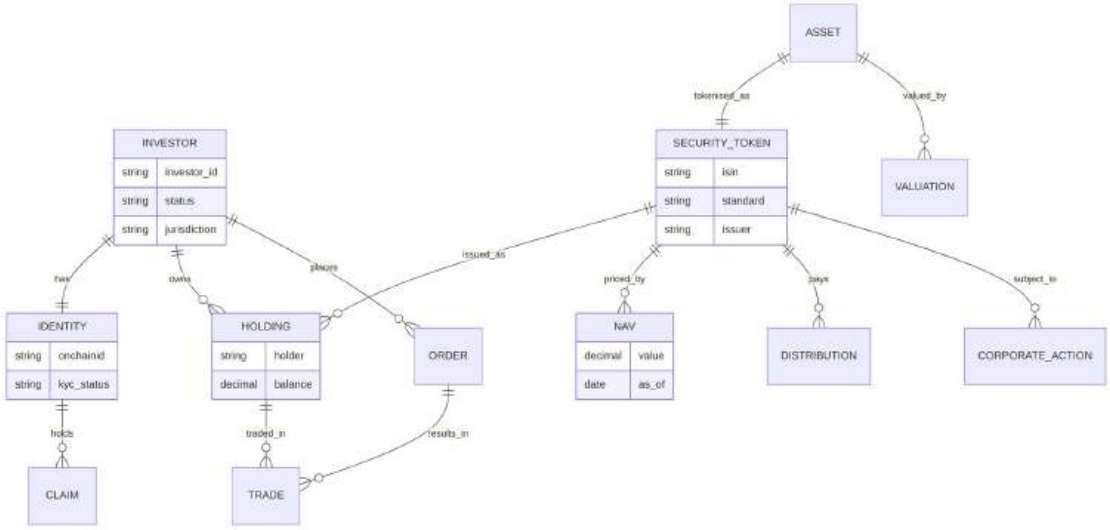


The ERC-3643 suite as classes: the Token delegates verification to the Identity Registry and permissioning to Modular Compliance (a composition of pluggable modules); identity is

proven by ONCHAINID claims validated against trusted issuers and claim topics. Source: Vol. II Fig. 6.

2.2 Entity-relationship — the platform data model

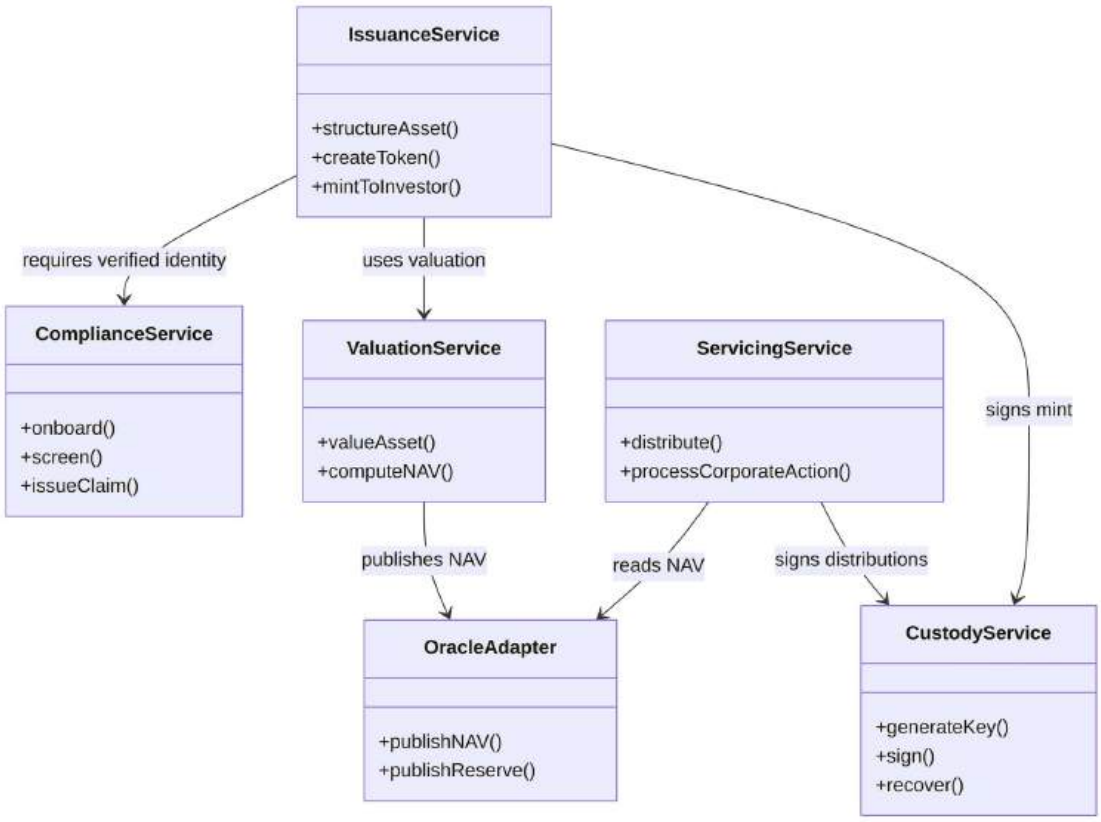
Figure 6 — Entity-relationship: platform data model.



The data model: investors hold verified identities (with claims) and own holdings of security tokens; each token tokenises an asset that is valued, produces NAV, pays distributions, and is subject to corporate actions; orders result in trades that move holdings. Personal data (identity, KYC) is held off-chain (Vol. I §9; Vol. II §1.4). Source: synthesis of Vols. I–IV.

2.3 Domain class model — platform services

Figure 7 — Domain class model: platform services.



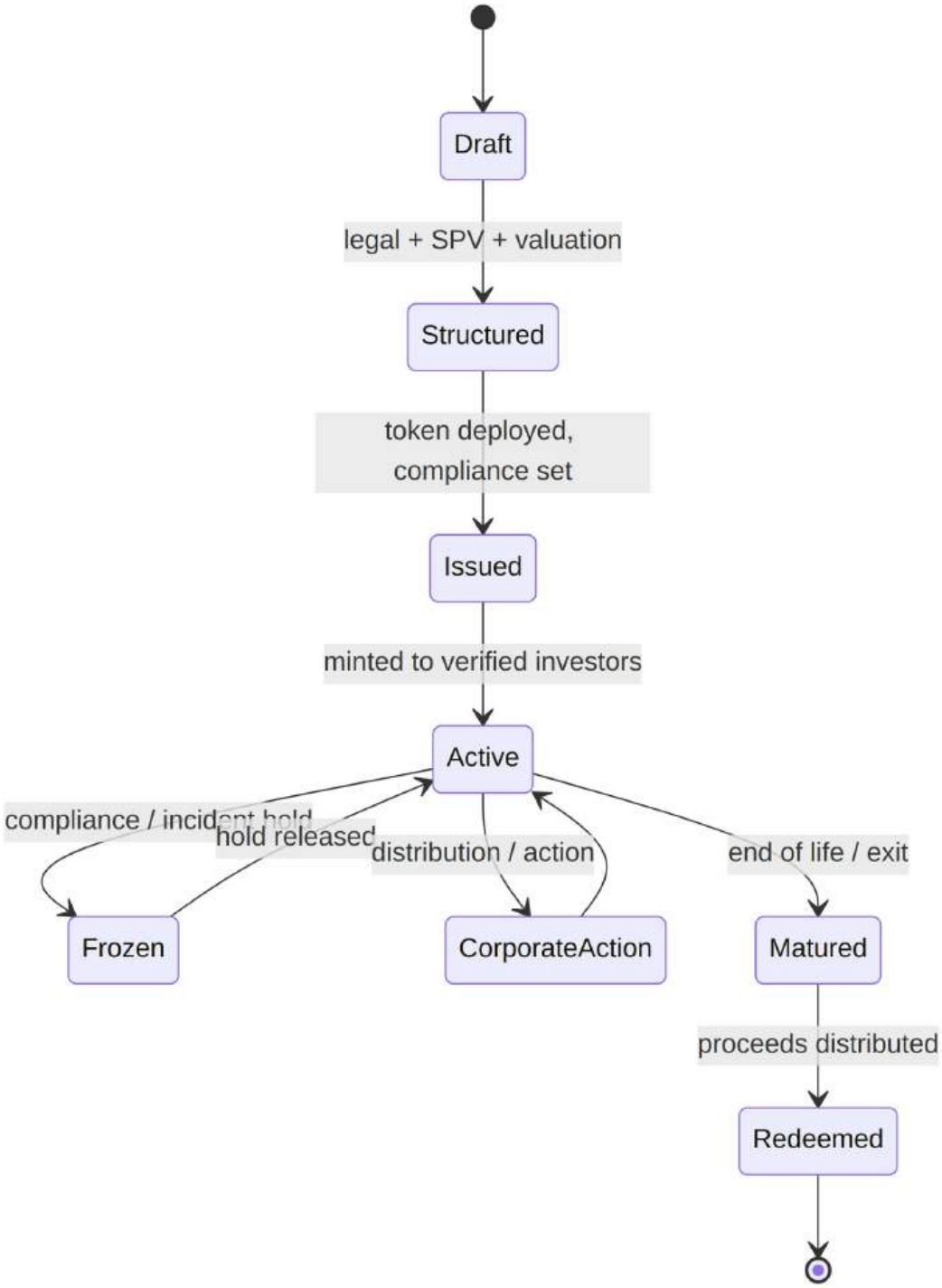
The off-chain services as a domain model: issuance depends on compliance and valuation; valuation publishes NAV through the oracle adapter; servicing reads NAV and executes distributions; custody signs the privileged operations. Source: Vol. II Fig. 13; Vol. IV; Vol. V.

CHAPTER 3 — LIFECYCLE, STATE & INTERACTIONS

This chapter renders the security's lifecycle as an explicit state machine and draws the three interactions that matter most: primary issuance, a secondary trade with atomic delivery-versus-payment, and a NAV update gated by proof-of-reserve.

3.1 The ledger-based security lifecycle

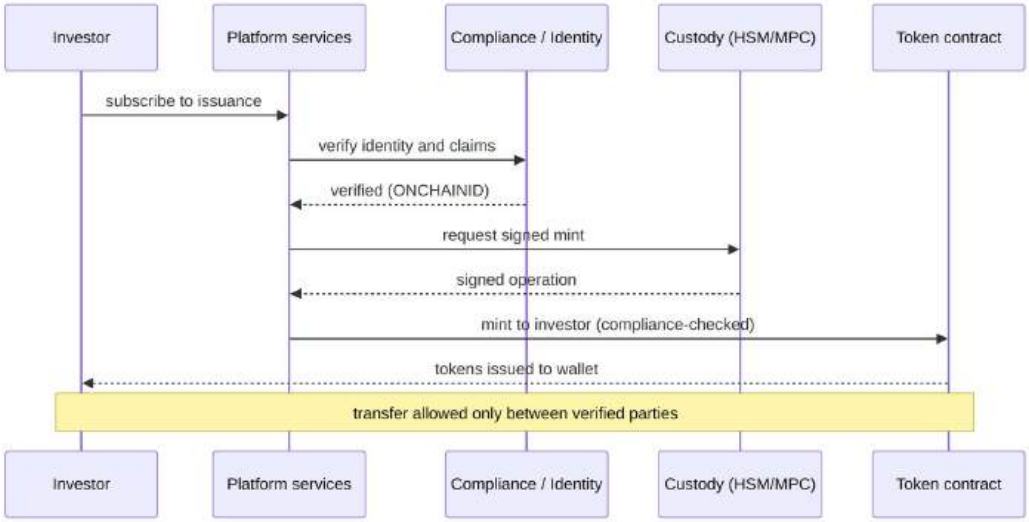
Figure 8 — State: ledger-based security lifecycle.



The security moves from draft through structuring and issuance to an active life (during which it may be frozen for compliance or undergo corporate actions), then to maturity and redemption. Aligns with the CO 973d–973i lifecycle. Source: Vol. I Fig. 8; Vol. III Fig. 1.

3.2 Primary issuance & compliant subscription

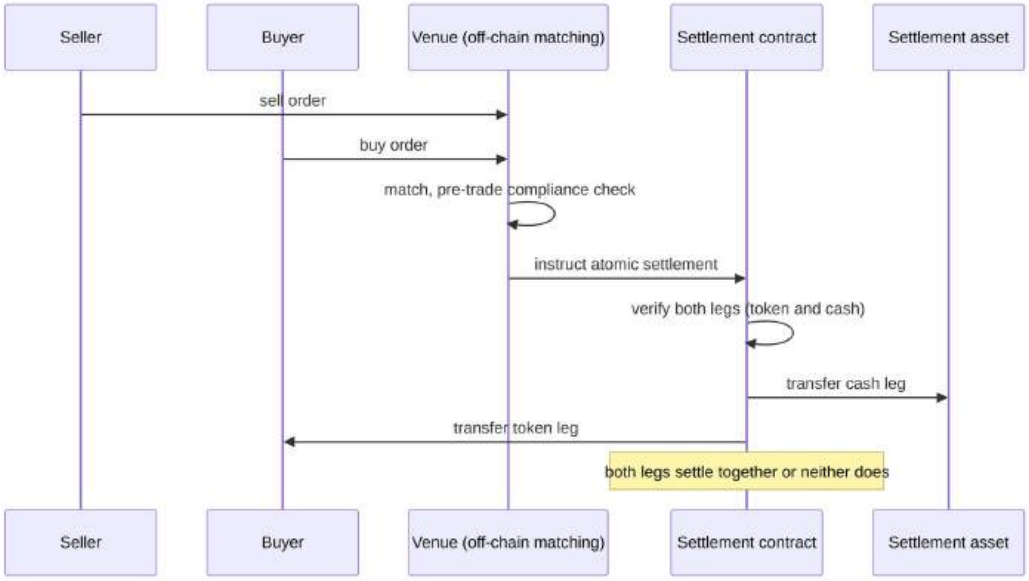
Figure 9 — Sequence: primary issuance & compliant subscription.



Subscription requires identity verification before any mint; the mint is signed under custody controls and executed by the token contract, which enforces that only verified parties may hold tokens. Source: Vol. I Fig. 10; Vol. II Fig. 14.

3.3 Secondary trade with atomic DvP

Figure 10 — Sequence: secondary trade with atomic DvP.

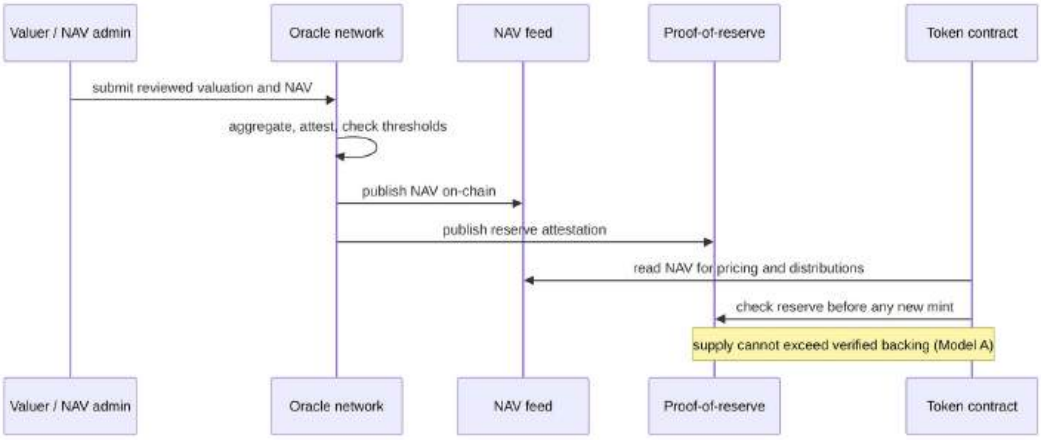


Orders match off-chain with pre-trade compliance; settlement is atomic on-chain

delivery-versus-payment — the token and cash legs move together or not at all, removing settlement risk. Source: Vol. III Figs. 6, 9; Vol. II Fig. 16.

3.4 NAV update & proof-of-reserve gating

Figure 11 — Sequence: NAV update & proof-of-reserve gating.



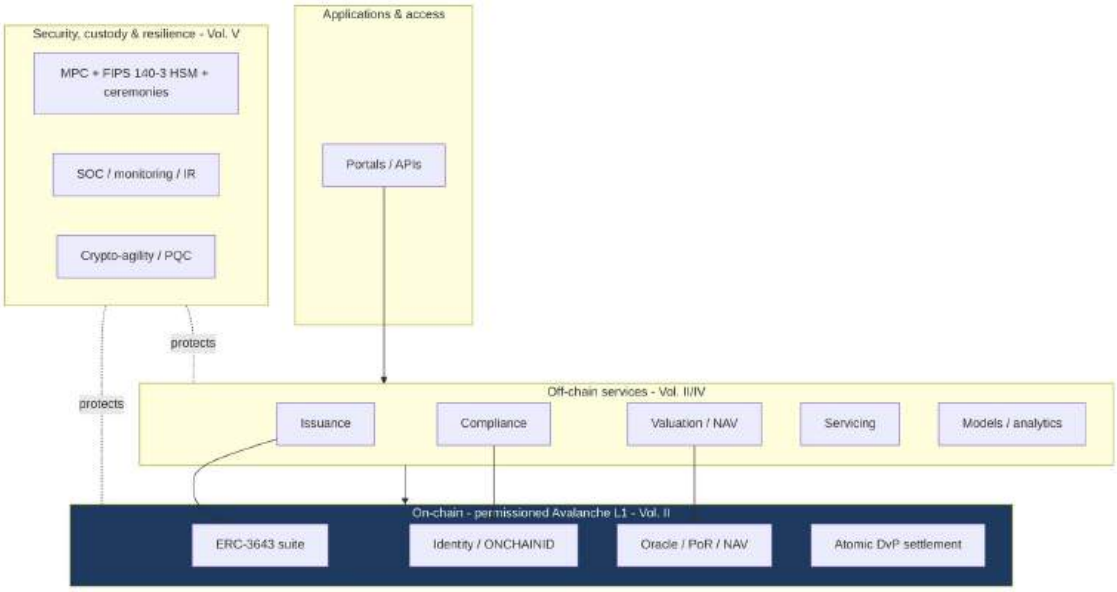
Reviewed valuations reach the chain only through the decentralised oracle network, which attests and publishes NAV and proof-of-reserve; the token reads NAV for pricing and checks reserves before minting, so supply cannot exceed verified backing. Source: Vol. II Fig. 12; Vol. IV Fig. 3.

CHAPTER 4 — CROSS-CUTTING CONSOLIDATED VIEWS

These four views compress the whole package into single pictures: the end-to-end architecture, the security/key architecture, the governance/assurance model, and the trust boundaries.

4.1 End-to-end reference architecture

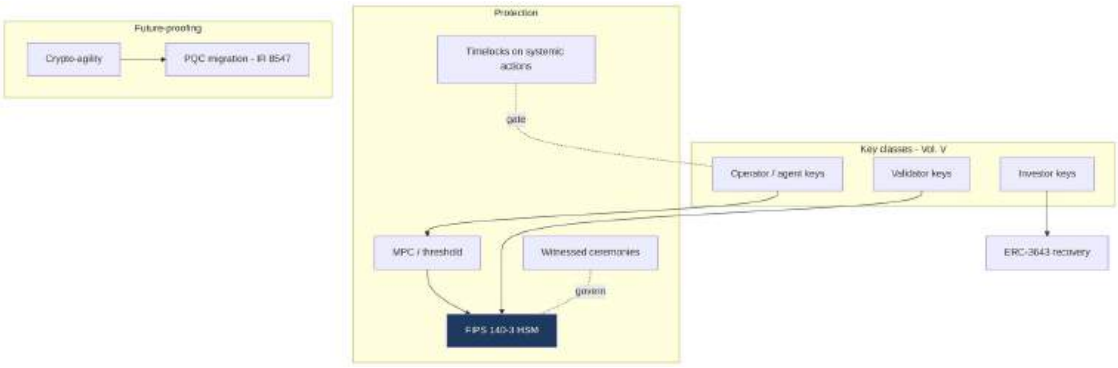
Figure 12 — End-to-end reference architecture.



One picture of the stack: applications call off-chain services, which drive the on-chain suite (tokens, identity, oracle, settlement) on the permissioned L1, all wrapped by the security, custody and resilience layer. Source: synthesis of Vols. II–V.

4.2 Security & key architecture (consolidated)

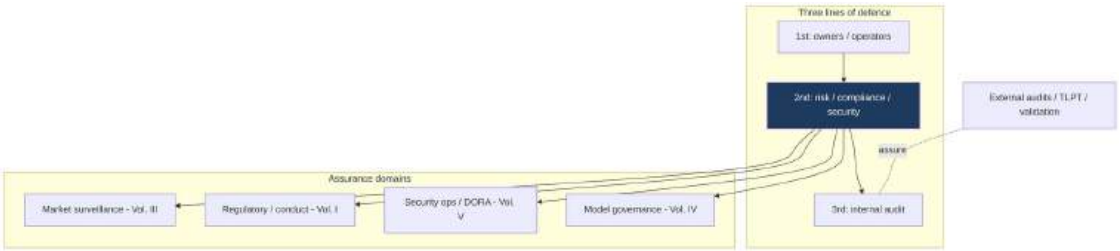
Figure 13 — Security & key architecture (consolidated).



The security spine: systemic keys under MPC and validated HSMs, governed by witnessed ceremonies and timelocks, with investor-key recovery and a crypto-agile path to post-quantum algorithms. Source: Vol. V Figs. 3–6.

4.3 Governance & assurance (consolidated)

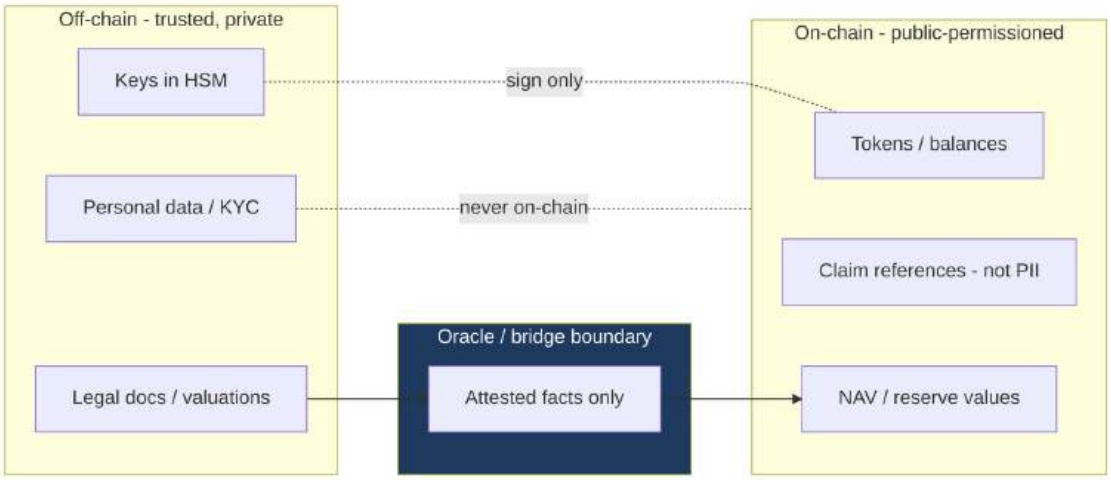
Figure 14 — Governance & assurance (consolidated).



Assurance is unified under three lines of defence across model, security/DORA, regulatory, and market-surveillance domains, backed by external audits, threat-led penetration testing, and independent validation. Source: Vols. I, III, IV, V.

4.4 Trust boundaries & data classification

Figure 15 — Trust boundaries & data classification.



The critical boundary: personal data, documents and keys stay off-chain; only attested facts (NAV, reserves) and non-personal references cross the oracle boundary onto the public-permissioned ledger. Personal data is never written on-chain. Source: Vol. I §9; Vol. II §1.4, §5.

CHAPTER 5 — MASTER DIAGRAM INDEX (VOLUMES I–VI)

This index catalogues every figure across Volumes I–VI (86 figures) so any diagram in the package can be located from one place. Figure numbers are as they appear in each source volume.

5.1 Volume I — Executive & Regulatory (15 figures)

Fig.	Title
1	Platform domain map
2	Dual-mode operating model
3	Governance and three lines of defence
4	Indicative organisation chart
5	Asset-backed issuance: SPV and rights structure
6	Forward-funding: SPV, escrow and drawdown structure
7	Token-classification decision tree
8	Ledger-based security lifecycle (CO 973d–973i) — state machine
9	Forward-funding milestone-drawdown sequence (Model B)
10	On-chain subscription and capital-call sequence
11	AML/CFT onboarding and monitoring flow
12	Collective-investment-scheme boundary decision tree
13	Regulatory-pathway roadmap (Switzerland-first) — Gantt
14	Tax structuring memorandum: decision flow
15	Vendor-risk management lifecycle

5.2 Volume II — Technical Architecture (17 figures)

Fig.	Title
1	System context (C4 Level 1)
2	Container view (C4 Level 2)
3	On-chain / off-chain split
4	Network topology: permissioned Avalanche L1 & interoperability
5	Chain-choice decision tree
6	ERC-3643 / T-REX contract suite (component view)
7	Compliant-transfer sequence
8	Dual-mode funding contracts (Model A / Model B)

Fig.	Title
9	Forward-funding escrow & milestone-drawdown sequence
10	UUPS upgrade flow with namespaced storage
11	Identity & claim-issuance flow (ONCHAINID)
12	Oracle & data-layer dataflow
13	Off-chain microservices container diagram
14	End-to-end subscription sequence (off-chain ↔ on-chain)
15	Crypto-agility & PQC layering
16	Delivery-versus-payment (DvP) settlement sequence
17	CI/CD with security gates (DevSecOps)

5.3 Volume III — Marketplace & Trading (15 figures)

Fig.	Title
1	Asset lifecycle: primary, secondary and corporate actions
2	Market-structure overview (participants and venue)
3	Venue-strategy decision tree
4	Multi-jurisdiction venue map
5	Trading-model comparison
6	Hybrid off-chain matching, on-chain settlement
7	Order lifecycle with pre-trade compliance
8	Matching-engine architecture
9	Atomic DvP settlement sequence
10	Failed-trade / settlement-exception handling
11	Liquidity sources and provision
12	Market-surveillance architecture
13	Point-of-trade conduct and suitability flow
14	Secondary-transfer compliance enforcement
15	Participant connectivity and onboarding

5.4 Volume IV — Financial Intelligence (13 figures)

Fig.	Title
1	Financial-intelligence architecture (data → model → decision → disclosure)
2	Valuation approaches and bases of value
3	NAV computation and oracle pipeline
4	DCF model structure
5	Sensitivity / tornado view
6	Monte Carlo simulation flow
7	Risk-metric distribution (VaR / expected shortfall)
8	Machine-learning model pipeline
9	Explainability (SHAP) and model card
10	Model lifecycle and three lines of defence
11	AI Act risk-tier mapping
12	LLM control flow (retrieval-grounded, human-in-the-loop)
13	Data architecture for intelligence

5.5 Volume V — Security & Operations (14 figures)

Fig.	Title
1	Layered defence-in-depth & security operating model
2	Custody models & FINMA segregation treatment
3	Custody & key-control architecture
4	Key ceremony (M-of-N, witnessed)
5	Key lifecycle
6	Post-quantum migration roadmap
7	DevSecOps secure SDLC with gates
8	Smart-contract security operations & circuit breaker
9	Incident-response lifecycle
10	SOC & detection architecture
11	DORA five pillars → platform controls
12	Business continuity & disaster recovery
13	Dev-phase fund-run stress scenario

Fig.	Title
14	Third-party risk & CTPP concentration

5.6 Volume VI — Business & Financial Model (12 figures)

Fig.	Title
1	Business-model frame and value flow
2	TAM / SAM / SOM funnel
3	The forecast-vs-reality gap
4	Value proposition by participant
5	Revenue streams
6	Platform-token decision tree
7	Unit economics of an issuance
8	Scenario ranges (illustrative)
9	Cost structure (build vs run)
10	Funding stages and capital
11	Phased roadmap
12	KPI tree

5.7 Coverage summary

Volume	Figures	Predominant diagram types
I	15	Flowcharts, decision trees, sequences, state, Gantt
II	17	C4, component, sequences, dataflow
III	15	Flowcharts, sequences, architecture
IV	13	Pipelines, flowcharts
V	14	Flowcharts, sequence, roadmap
VI	12	Flowcharts, funnels, trees
VII	**15 (new)**	**C4, class, ER, state, sequence, consolidated**
Total	**101**	—

Volumes I–VI contribute 86 figures; this atlas adds 15 consolidating/extending views, for 101 across the package.

INTERIM NOTE & HANDOVER TO THE CROSS-VOLUME AUDIT

What this volume did. It consolidated the package's 86 diagrams into one navigable index and added 15 higher-fidelity views — the C4 model to component level, a code-level class model of the ERC-3643 suite, an entity-relationship data model, a domain class model, a consolidated lifecycle state machine, the three core sequences, and four cross-cutting synthesis views — introducing no new external facts.

Handover to the audit. With all seven volumes drafted, the package is ready for the single **cross-volume Compliance & Completeness Audit**, which will: (1) resolve every forward reference across volumes; (2) re-verify each volume's Standards/Versions and Citation registers against primary sources on the audit date; (3) check terminological consistency against the canonical Control File; (4) confirm no fabricated citations, versions, or identifiers remain, and that all links resolve; (5) confirm that design options are labelled with trade-offs and that all illustrative figures (Vol. VI) are marked as such; and (6) produce a consolidated open-items list from the six Interim Audits. This atlas is the audit's visual map.

Standing caveats (unchanged). AI-authored draft; must be reviewed by qualified counsel and specialists before reliance; diagrams are simplified; canonical facts, options, and citations live in Volumes I–VI.

GLOSSARY (POINTER)

This atlas introduces no new terms. The master glossary is in Volume I; the technical glossary in Volume II; domain glossaries in Volumes III–VI. Canonical reminder: the instrument is a **ledger-based security** implemented as an **ERC-3643 permissioned token** on a **permissioned Avalanche L1**, with identity via **ONCHAINID**, value via the **decentralised oracle layer**, and keys protected by **MPC and FIPS 140-3 HSMs**.

APPENDIX A — NOTATION LEGEND

Notation	Shows	Used for (this volume)
Flowchart	Structure and flow	C4 views, reference architecture, consolidated views
C4 (Context/Container/Component)	Software architecture at increasing zoom	Figs. 1–4
Class diagram	Types/contracts and relationships	Figs. 5, 7

Notation	Shows	Used for (this volume)
Entity-relationship (ER)	Data entities and cardinality	Fig. 6
State diagram	Lifecycle states and transitions	Fig. 8
Sequence diagram	Ordered interactions over time	Figs. 9–11
Navy-filled node	The most systemic element in a view	Throughout

C4 views are rendered as styled flowcharts for portability. All notations are simplified for clarity and are not implementation-complete.

APPENDIX B — CROSS-VOLUME FIGURE MAP (ATLAS → SOURCES)

Where each atlas figure draws from in Volumes I–VI.

Atlas fig.	Title	Primary sources
1	C4 L1 — System context	Vol. II Fig. 1
2	C4 L2 — Container view	Vol. II Figs. 2, 13
3	C4 L3 — On-chain suite	Vol. II Fig. 6
4	C4 L3 — Off-chain & oracle	Vol. II Figs. 12, 13
5	Code/Class — ERC-3643	Vol. II Fig. 6
6	ER — data model	Vols. I–IV (synthesis)
7	Domain class — services	Vol. II Fig. 13; Vols. IV–V
8	State — lifecycle	Vol. I Fig. 8; Vol. III Fig. 1
9	Sequence — issuance	Vol. I Fig. 10; Vol. II Fig. 14
10	Sequence — DvP trade	Vol. III Figs. 6, 9; Vol. II Fig. 16
11	Sequence — NAV/PoR	Vol. II Fig. 12; Vol. IV Fig. 3
12	End-to-end architecture	Vols. II–V (synthesis)
13	Security & key	Vol. V Figs. 3–6
14	Governance & assurance	Vols. I, III, IV, V
15	Trust boundaries	Vol. I §9; Vol. II §1.4, §5

DIAGRAM INVENTORY (Volume VII)

Fig.	Title	Mermaid type	Section
1	C4 L1 — System context	flowchart	1.1
2	C4 L2 — Container view	flowchart	1.2
3	C4 L3 — On-chain compliance & token suite	flowchart	1.3
4	C4 L3 — Off-chain services & oracle	flowchart	1.4
5	Code/Class — ERC-3643 contract model	classDiagram	2.1
6	Entity-relationship — data model	erDiagram	2.2
7	Domain class model — services	classDiagram	2.3
8	State — security lifecycle	stateDiagram	3.1
9	Sequence — primary issuance	sequenceDiagram	3.2
10	Sequence — secondary DvP trade	sequenceDiagram	3.3
11	Sequence — NAV & proof-of-reserve	sequenceDiagram	3.4
12	End-to-end reference architecture	flowchart	4.1
13	Security & key architecture	flowchart	4.2
14	Governance & assurance	flowchart	4.3
15	Trust boundaries & data classification	flowchart	4.4

This atlas consolidates the full package's diagrams; the cross-volume audit follows.

END OF VOLUME VII (interim draft) — END OF THE SEVEN-VOLUME PACKAGE (drafts)

All seven volumes are now drafted. The remaining step is the single **cross-volume Compliance & Completeness Audit** described in the handover note above, after which — on explicit request — the full package can be compiled.