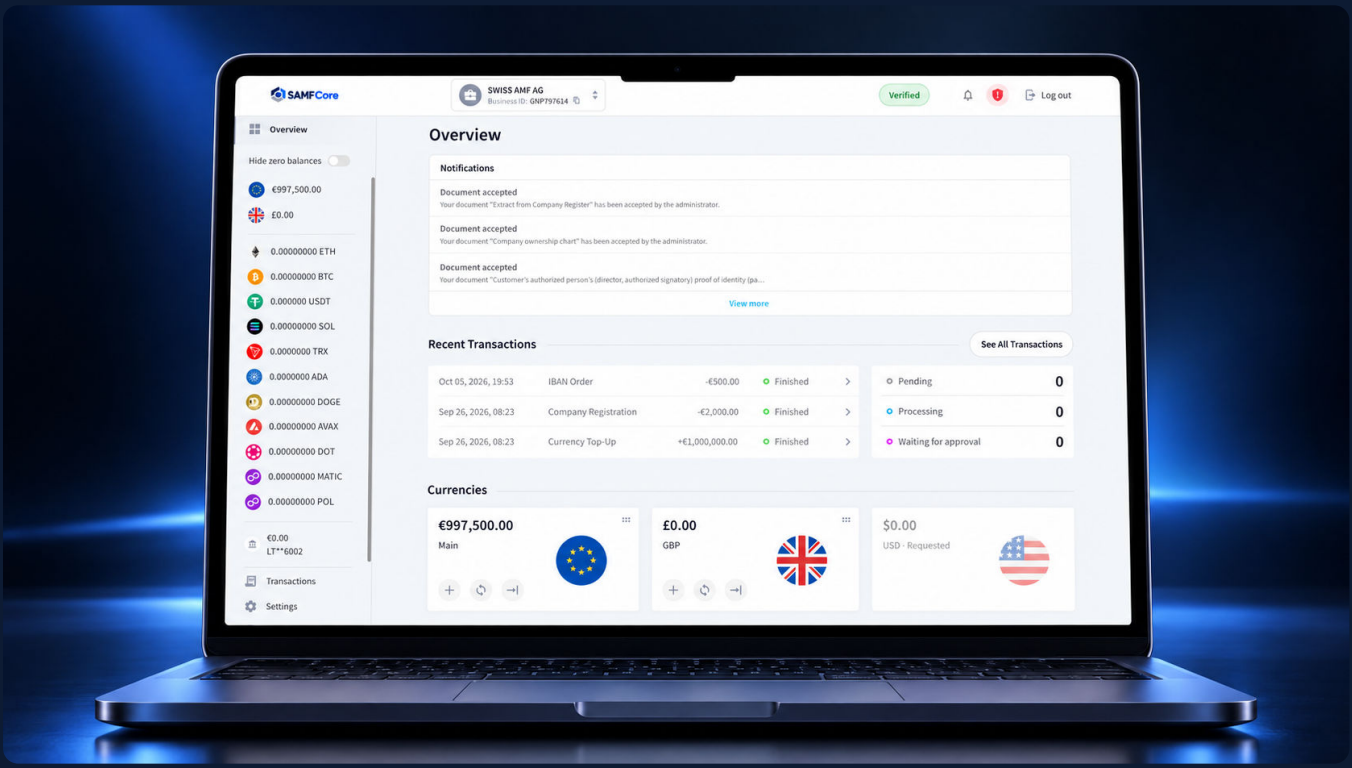
INFORMATION MEMORANDUM · VERSION 2.2 · 5 NOVEMBER 2026

SAMFCore Information Memorandum

An integrated financial-services software platform with built-in account management, transaction processing, onboarding and compliance workflows, available under perpetual licensing with Full Source Code options and customer-controlled deployment.



2018
Development began

Since 2021
In operational use in live financial-services environments

Perpetual
Licensing with Full Source Code options

No revenue share
No per-transaction SAMFCore software fees

Swiss AMF AG · Bahnhofstrasse 21 · 6300 Zug · Switzerland · samfcore.com
Buyer information for prospective licensees. It is not a binding offer. Final rights, scope, deliverables and pricing are governed by executed agreements.

CONTENTS

Inside this memorandum

01 Executive Summary 3

02 SAMFCore at a Glance 4

03 Built-In Account Management, Transaction Processing & Balance Management 5

04 Customer Onboarding, KYC & Corporate Verification 7

05 Built-In AML, Risk Management & Compliance Workflows 9

06 Functional Capability Matrix 11

07 Technical Architecture & System Design 13

08 Security, Access Control & Auditability 15

09 APIs, Integration Framework & Provider Connectivity 16

10 From Software Acquisition to Operational Launch 17

11 Full Source Code & Technical Handover 19

12 Progressive Cutover Migration 20

13 Commercial Model & Long-Term Economics 21

14 Licence Packages & Annual versus Perpetual 22

15 Enterprise Global & Group Licensing 23

16 Swiss Development, Legal Opinion & Responsibilities 24

17 Buyer FAQ 25

18 Next Steps: Demonstration & Sandbox 27

How to read this document

Sections 1–2 summarise the opportunity for executive readers. Sections 3–6 describe native functionality for operations and compliance teams. Sections 7–12 cover architecture, security, integration, deployment, optional Swiss AMF implementation and support services, and migration for technology leaders. Sections 13–16 set out licensing and commercial terms for finance and procurement. Section 17 answers common buyer questions.

Scope of this document

This memorandum describes the SAMFCore software and its licensing. Detailed technical documentation, security materials and legal opinions are kept for advanced due diligence. They can be provided to qualified prospective buyers under appropriate confidentiality arrangements.

FEATURE CLASSIFICATION USED THROUGHOUT

BUILT-IN native SAMFCore functionality INTEGRATION requires a connected external provider CONFIGURATION depends on deployment settings OPTIONAL optional or separately scoped. The modules included in each deployment are confirmed during solution design.

01 · EXECUTIVE SUMMARY

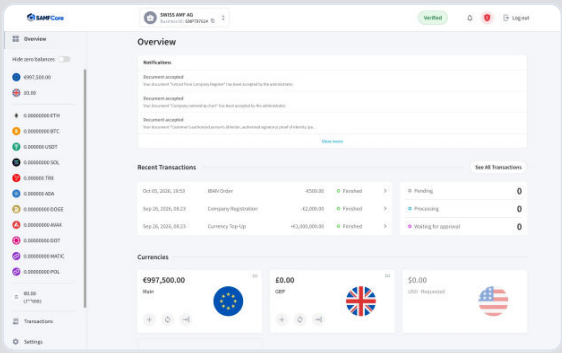
A complete financial-services platform you can own the right to run

SAMFCore is a modular financial-services software platform developed and commercialised by Swiss AMF AG. It gives banks, EMIs, payment firms, fintechs, digital-asset businesses and BaaS providers one integrated environment for customers, accounts, transactions and compliance.

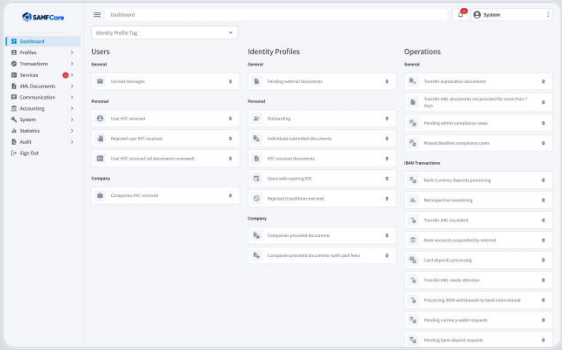
SAMFCore has its own application services, data models and transaction-processing workflows. It maintains individual and corporate customer accounts and multi-currency balances, and it records every deposit, withdrawal, card charge and exchange as a transaction with its own status and history. Administrators approve, reject or refund transactions, and flagged activity follows a separate AML review path.

Around this core, SAMFCore provides configurable customer onboarding with KYC and corporate KYB, a risk-scoring and AML rule engine, compliance case management, fee configuration, cards, crypto and digital-asset workflows, reporting, permissions and a full activity log. Specialist services such as banking, card issuing, identity verification and screening are connected through an API integration framework to providers each customer selects.

Commercially, SAMFCore is offered under **perpetual licensing**, with **Full Source Code** options and **customer-controlled deployment**. Across all licence models there is **no SAMFCore software fee per customer transaction and no share of transaction revenue**.



Customer panel: notifications, recent transactions and multi-currency balances.



Administration: operations dashboard with onboarding, AML and transaction work queues.

For the CEO

A ready-built platform for launching or consolidating financial services, with long-term rights instead of indefinite rental.

For the CFO

One-time perpetual licence options, no per-transaction SAMFCore fees and no revenue share as volumes grow.

For the CTO

A documented service architecture, versioned APIs, provider connectors and optional Full Source Code.

For Compliance

Native onboarding rules, risk scoring, monitoring rules, case management, document requests and audit trails.

THE PROPOSITION IN ONE SENTENCE

Acquire a proven, extensive financial-services software platform, run it on infrastructure you control, connect the providers you choose, and keep the economics of your growth.

02 · SAMFCORE AT A GLANCE

One environment for customers, money movement and control

Customer-facing and administrative applications work on the same customer records, accounts and transactions.

01
Accounts & balances
Individual and corporate accounts, multi-currency balances, IBAN-related workflows, statements and daily balance snapshots.

02
Transactions & transfers
Deposits, withdrawals, internal transfers, batch payments, exchanges and card charges, recorded with status and history.

03
Onboarding, KYC & KYB
Configurable registration and onboarding by country and customer category, corporate ownership and UBO collection.

04
AML & compliance
Risk levels and scores, real-time transaction rules, re-screening, compliance cases, Ongoing Due Diligence and approvals.

05
Cards
Physical and virtual card ordering, activation, PIN management, freeze and unfreeze and top-ups through a card-issuing integration.

06
Crypto & digital assets
Currency and crypto accounts, market and limit exchange, blockchain addresses per network and administrative asset control.

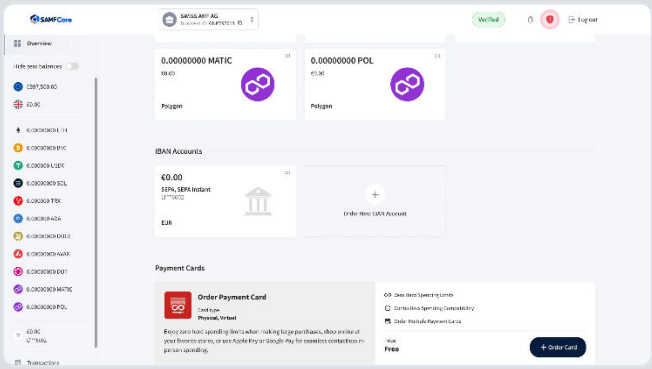
07
Fees
Fee baskets combining periodic, volume-based and risk-level-based fees, assigned to customers or customer groups.

08
CRM & administration
Customer profiles, support messaging, notifications, document management, tags, bulk actions and approval queues.

09
Reporting & control
Report catalogue, transaction and fee reporting, embedded analytics, administrator roles and a full activity log.

Built for a broad range of financial businesses

- **Banks and digital banks** adding digital accounts, cards and digital assets alongside existing core systems.
- **EMIs and payment firms** needing account, transfer, onboarding and compliance workflows in one platform.
- **Fintechs and neobank founders** seeking a ready-built platform instead of a multi-year build.
- **Digital-asset businesses and VASPs** combining fiat and crypto accounts and exchange workflows.
- **BaaS providers and financial groups** serving several brands or legal entities.



Customer panel: digital-asset balances, IBAN accounts and card ordering.

03 · CORE FINANCIAL FUNCTIONALITY

Built-In Account Management, Transaction Processing & Balance Management

SAMFCore is not a graphical layer over unrelated systems. Its own services, data models and workflows maintain accounts, record transactions and update balances.

Customer accounts and account structures

Each individual or corporate customer has an identity profile with its associated accounts. The customer dashboard shows all of a customer's assets together: bank accounts, cards, currency accounts and digital assets.

- Individual and corporate customer accounts, including company users.
- Multi-currency fiat accounts and IBAN-related accounts.
- Payment-card accounts and digital-asset accounts.
- Closed-loop token accounts where configured.
- Account statements and exportable transaction histories.

Internal transaction ledger

SAMFCore records every financial movement affecting a customer account. Each deposit, withdrawal, card charge and exchange is a transaction in SAMFCore, with its own status, references and history.

- Transaction amount and debit or credit classification.
- Account balance before and after the movement.
- References linking related transactions.
- Status tracking from pending through completion.
- Tags and operational information for administration and compliance.

How it works: a worked example

Balance €10,000
Customer account before the transfer

▶

Transfer €2,000
Customer initiates; available balance checked

▶

Debit recorded
Amount, before/after balances and references stored

▶

Balance €8,000
Balance updated; transaction kept in the history

For transfers between customer accounts, SAMFCore records linked debit and credit movements against both accounts. Exchanges create a paired transaction for the target account.

Automated balance management

Balances are calculated and updated as transactions are posted, with available-balance checks and configurable posting and balance-handling modes.

Reversals and corrections

For supported reversal and failure scenarios, SAMFCore creates correction records and keeps the original transaction history intact.

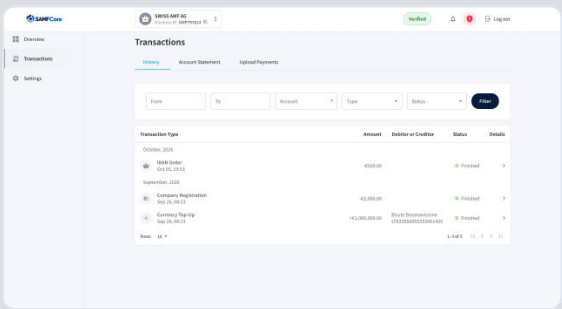
Daily balances and reporting

A scheduled process captures daily account-balance snapshots, supporting balance reporting, accounting summaries and fee revenue reports.

Internally or externally managed balances

Internally managed: SAMFCore keeps customer balances through its own account and transaction management.

Externally managed: where a bank or provider holds balances in its own systems, SAMFCore retrieves account information through API integration and adapts transaction workflows to that provider's requirements. Each deployment selects the model that fits its commercial, technical and regulatory set-up.



Customer panel: transaction history with type, amount and status.

03 · CONTINUED

The transaction lifecycle

An illustrative view of how a transaction moves through SAMFCore. Steps that apply depend on the transaction type, configured rules and connected provider.

1 · Initiated
Customer, administrator, batch file or provider deposit

▶

2 · Validated
Account, permissions and available balance checked

▶

3 · Screened
Active AML rules evaluated; clear or flag

▶

4 · Reviewed
Approval, rejection or refund where required

▶

5 · Recorded
Transaction completed and stored with history

▶

6 · Reflected
Balances updated; visible to customer and administrators

Provider execution where applicable
External transfers, card top-ups and settlement are carried out by the connected bank, payment or card provider; their status is reflected back in SAMFCore

Flagged path
A flagged transaction gets an AML review record; administrators approve, reject or escalate it before it proceeds

Ongoing visibility
The activity log, reports, daily balances and compliance reviews all use the same transaction record

SAMFCore processing step · Outcome · Related path

Deposits and withdrawals

Customers can request IBAN accounts and submit currency and bank deposits. A deposit creates a pending transaction, which is then cleared automatically by AML rules or approved by an administrator. Withdrawals can be processed in batches. Money movement outside SAMFCore is executed by the connected banking or payment provider.

Administrative transaction control

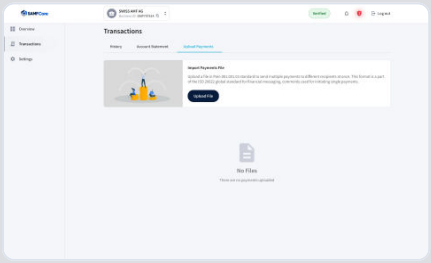
Administrators open a transaction's detail view to review, approve, reject or refund it. Flagged transactions follow a separate AML review path. Transactions can be tagged for filtering and segmentation, and every decision is recorded in the activity log.

Internal transfers and batch payments

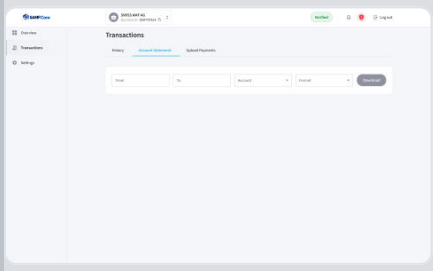
Account-to-account transfers between customers are recorded as linked movements. Corporate customers can upload batch-payment files to send several payments at once. External payments are routed through the selected provider.

Fees applied to customer activity

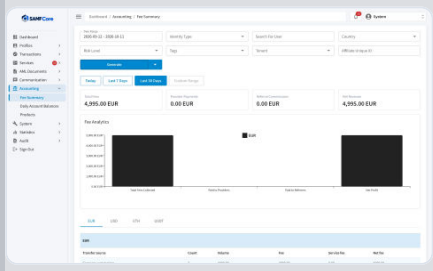
Operators configure the fees they charge their own customers, such as periodic, volume-based and risk-level-based fees, using reusable fee baskets. Fee summaries report fee revenue by period and currency. These are the operator's fees, not SAMFCore licence fees.



Batch-payment file upload.



Account statements by period and format.



Administration: fee summary and analytics.

04 · CUSTOMER ONBOARDING

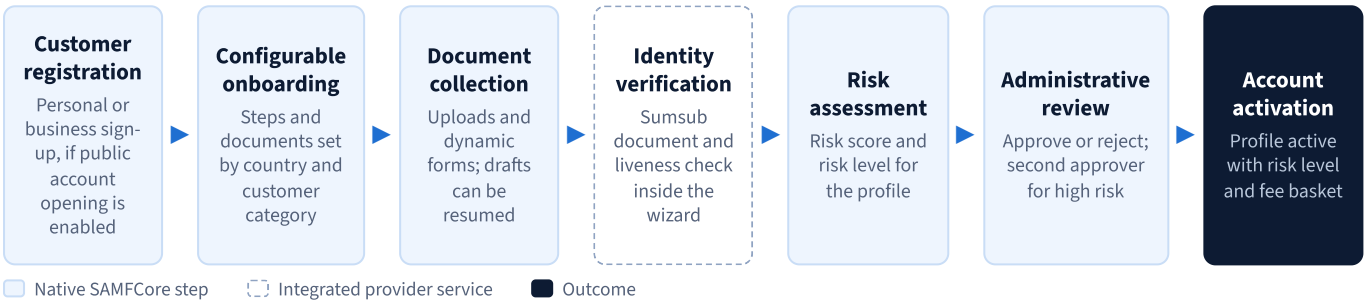
Customer Onboarding, KYC & Corporate Verification

SAMFCore includes its own onboarding workflow engine for individual and corporate customers. It is one of the platform's most important operational strengths.

NATIVE WORKFLOW, SPECIALIST VERIFICATION

The onboarding process, rules, customer records and administrative workflows are native SAMFCore capabilities. Sumsub provides specialised verification services integrated into those workflows. Sumsub performs document and biometric/liveness checks, and its results are returned to SAMFCore, which updates the customer's KYC status.

Customer onboarding workflow



Configurable onboarding rules

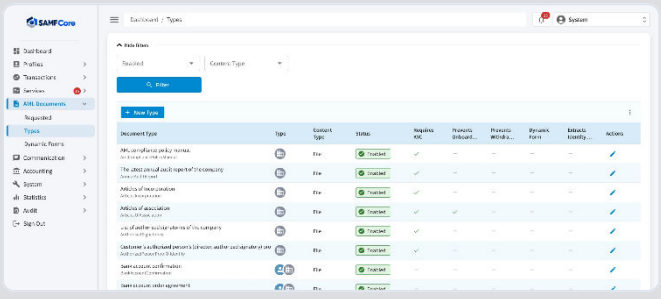
An onboarding rule engine decides which steps and documents are required for each country and customer category. Compliance teams can therefore apply different requirements to, for example, a retail customer in one jurisdiction and a corporate customer in another, without code changes.

- Country- and category-based onboarding settings.
- Customisable document types and dynamic forms.
- Questionnaires and information collection.
- Permissions controlling public personal and business account opening.

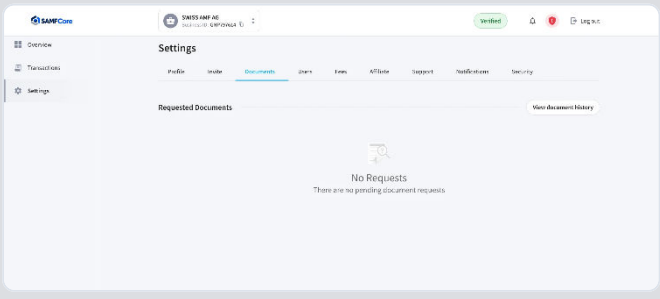
Individual KYC

After sign-up, a personal customer moves straight into a multi-step onboarding wizard. At the identity step, SAMFCore launches the integrated Sumsub verification. The customer completes the document and liveness capture, and Sumsub sends the result back asynchronously to update the KYC status.

- Onboarding progress and verification status are visible to customers and administrators.
- Document requests can be raised at any time during or after onboarding.
- KYC status changes trigger customer notifications.



Administration: configurable document types for onboarding and compliance.



Customer panel: requested documents and document history.

04 · CONTINUED

Corporate KYB, beneficial owners and approvals

Business customers go through a dedicated KYB journey that captures legal details, ownership and supporting evidence.

01
Company application
A multi-step KYB wizard collects company legal details and corporate structure. Drafts are saved automatically so applicants can resume later.

02
Ownership & UBOs
Ownership structures and ultimate beneficial owners are recorded under the company, as individual or corporate beneficiaries, with screening started and updated per beneficiary.

03
Supporting documents
The company form and required documents are submitted together and stored with the company's KYB profile and document requests.

04
Company users
Corporate customers can invite colleagues by email so several users can work under one company profile.

05
Administrative review
Administrators review the KYB profile, approve or reject documents, raise further document requests and set the company's risk level.

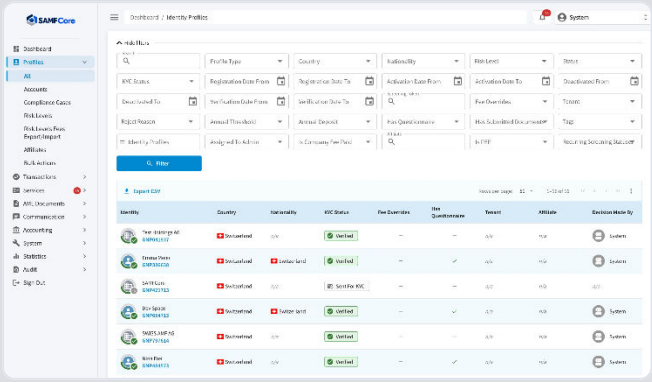
06
Activation
On approval the profile becomes active, with its risk level and fee basket assigned, and the customer is notified.

Identity profile review and approval

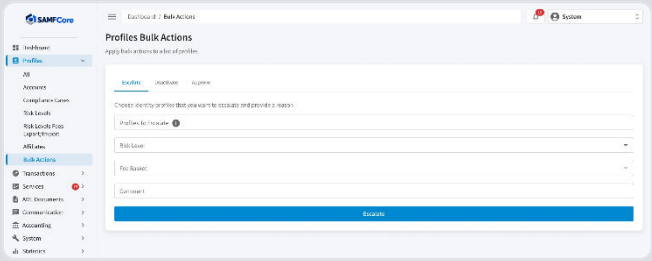
Identity profile review is the central administrative workflow for KYC and KYB. From one review screen, administrators can:

- approve or reject individual and corporate profiles;
- adjust the customer's risk level;
- assign the fee basket that applies to the customer;
- send high-risk personal profiles to a second administrator for approval;
- apply bulk actions, such as escalation with a recorded reason, to several profiles;
- filter profiles by KYC status, country, risk level, tags, screening status and more.

Document requests support partial saves, dynamic forms and file uploads. Each is approved or rejected by an administrator, and high-risk cases take an escalated approval path.



Administration: identity profiles with KYC status, risk and screening filters.



Bulk actions on selected profiles, with a recorded reason.

What is native and what is integrated

BUILT-IN registration, onboarding wizard, onboarding rules, KYB and UBO collection, document requests, risk levels, review, approvals and customer records. INTEGRATION document authentication, biometric/liveness checks and external sanctions/PEP screening through Sumsub or another compatible provider.

05 · COMPLIANCE MANAGEMENT

Built-In AML, Risk Management & Compliance Workflows

SAMFCore's compliance functions run inside the platform, on the same customers, accounts and transactions. External screening data can be integrated where needed.

Compliance workflow

Customer or transaction
Profile, onboarding event or transfer

▶

Risk assessment or rule
Risk score, country risk or active AML rule

▶

Review or flag
Cleared automatically or flagged

▶

Compliance case
Opened manually or by scheduled ODD

▶

Investigation
Required document requests attached

▶

Approval / escalation
Approve, reject or escalate

▶

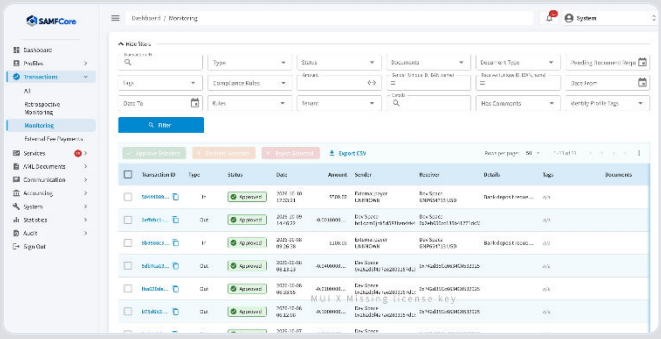
Recorded outcome
Stored with case, profile and activity log

Customer risk management

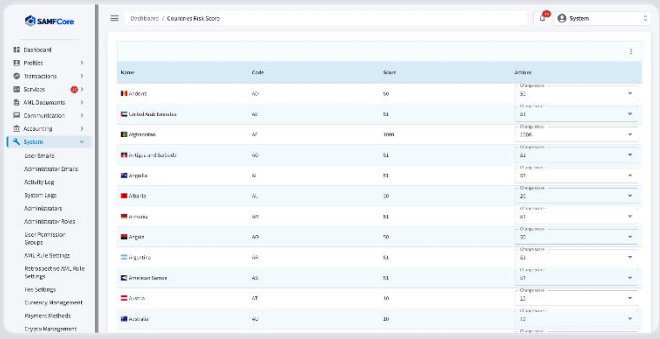
- **Configurable risk levels**, each of which can carry its own fee schedule.
- **Customer risk-score calculation** for personal identities, with PDF export of the risk assessment.
- **Country-level risk scoring** maintained by administrators.
- **AML/PEP-related assessment** and screening status kept on the customer profile.
- **Risk-profile management:** administrators adjust risk levels during review and approval.
- **Higher-risk approval** through a second-administrator workflow.

Transaction monitoring and screening

- **Configurable monitoring rules** evaluated as transfers are processed.
- **Real-time flagging:** a transfer that triggers a rule gets an AML review record; others proceed normally.
- **Retrospective re-screening** of historical transfers in batches.
- **Recurring sanctions/PEP re-screening** of identities, through integrated providers such as Sumsub.
- **Transaction-related AML review:** administrators approve, reject or escalate flagged transfers.
- **Monitoring views** with filters for status, compliance notes, documents and tags.



Administration: transaction monitoring with status, amounts and compliance filters.



Administration: country risk scores maintained in SAMFCore.

05 · CONTINUED

Case management, Ongoing Due Diligence and evidence

The investigation and evidence trail that compliance officers and MLROs need, held inside the platform.

AML case management

Compliance cases support AML monitoring and investigation, including Ongoing Due Diligence, pending-transfer review and cardholder KYC. The case type is checked when a case is created.

Automatic document requests

Each case automatically attaches the document requests its case type requires, so the evidence to collect is defined from the start.

Ongoing Due Diligence

Cases can be opened manually by an administrator or by a scheduled Ongoing Due Diligence process, supporting periodic customer reviews.

Review and escalation

Administrators review, complete or escalate cases and flagged transactions. High-risk document approvals take an escalated path.

Customer communication

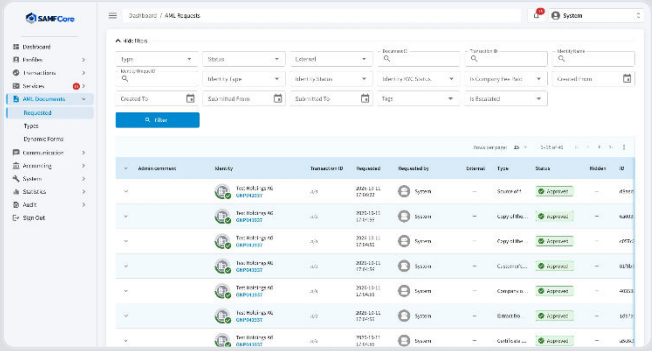
Customers see document requests in their panel, upload evidence and receive notifications and actionable alerts.

Evidence and audit

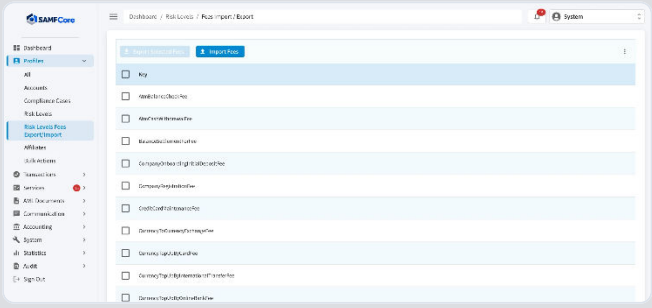
Decisions, document outcomes and status changes are written to the activity log and linked to the customer and transaction records.

How compliance connects to the rest of the platform

Because onboarding, accounts, transactions and compliance share the same data, a risk decision has direct operational effect. A customer's risk level can determine the fees applied to them. A flagged transfer stays on hold until it is reviewed. A completed case updates the customer profile. Compliance teams work from the same customer and transaction records as operations, rather than reconciling exports between separate systems.



Administration: AML document requests with status, type and escalation.



Risk-level fee configuration with import and export.

Responsibilities

SAMFCore provides compliance workflow, risk-management and control software. The licensee remains responsible for its AML policies, rule settings, risk methodology and regulatory obligations. External screening and verification data are supplied by the providers it selects. SAMFCore does not hold a regulatory certification and does not guarantee the detection of suspicious activity.

06 · WHAT IS ALREADY AVAILABLE

Functional Capability Matrix

Documented SAMFCore functionality by area, classified by how it is delivered. Modules in scope for a deployment are confirmed during solution design.

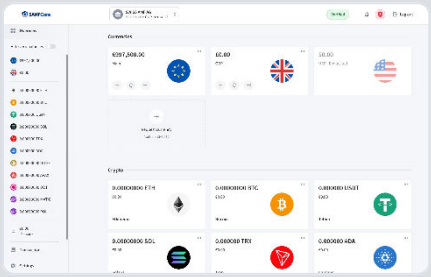
Area	Capability	Classification
Accounts & banking-related workflows	Individual and corporate accounts, multi-currency balances, combined asset dashboard, statements, transaction histories and export	BUILT-IN
	IBAN account requests and issuance, bank deposits, batch withdrawals	BUILT-IN INTEGRATION
	Internally or externally managed balance model	CONFIGURATION
Payments & transfers	Internal account-to-account transfers, transaction status tracking, approvals, rejections and refunds	BUILT-IN
	Batch-payment file upload and processing	BUILT-IN
	External payment instructions and settlement through banking and payment providers	INTEGRATION
Cards	Physical and virtual card ordering, activation, PIN and ePIN management, freeze and unfreeze, top-ups, card transactions in history	BUILT-IN INTEGRATION
	Card issuing, processing and programme management by the selected issuer	INTEGRATION
Crypto & digital assets	Currency and crypto accounts, market and limit exchange between a customer's accounts, fiat/crypto conversion workflows	BUILT-IN INTEGRATION
	Administrative control of enabled cryptocurrencies, balance activation and wallet-request approvals	BUILT-IN
	Blockchain addresses per network, custody and liquidity	INTEGRATION
Onboarding & compliance	Registration, onboarding wizard, onboarding rules, KYB, UBOs, document requests, risk levels and scores, AML rules, compliance cases, ODD	BUILT-IN
	Document and biometric/liveness verification, recurring sanctions/PEP screening (e.g. Sumsub)	INTEGRATION
	Required steps, documents, rules and risk settings per country and customer category	CONFIGURATION
Fees & commercial configuration	Fee baskets with periodic, volume-based and risk-level-based fees; assignment to customers or affiliate groups; fee reporting	BUILT-IN
	Fee amounts, products and pricing plans offered to end customers	CONFIGURATION

Fees in this matrix are fees the licensee charges its own customers through SAMFCore. They are separate from SAMFCore software licence fees, which never include a per-transaction charge or revenue share.

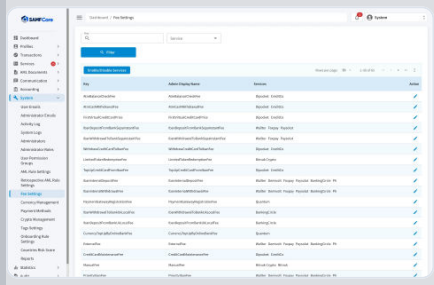
06 · CONTINUED

Administration, reporting and additional modules

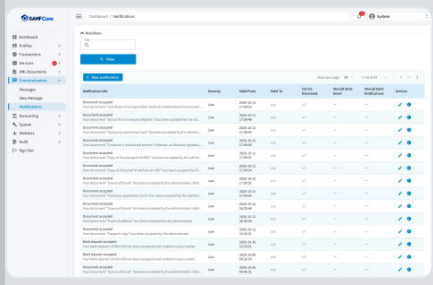
Area	Capability	Classification
CRM & customer administration	Customer profiles, identity-profile review, bulk actions, tags, document management and approval queues	BUILT-IN
	In-app support messaging between customers and administrators, with conversation tagging	BUILT-IN
	Customer notification inbox, administrator broadcasts, real-time push and actionable alerts	BUILT-IN
Reporting & analytics	Report catalogue, ad-hoc report queries, daily balances, accounting summaries, transaction and fee reporting	BUILT-IN
	Embedded Microsoft Power BI analytics	INTEGRATION
Platform administration	Administrator roles, permission groups, risk levels, onboarding settings, document types, transactional email templates	BUILT-IN
	Activity log of business events across modules	BUILT-IN
Additional modules	Tenant provisioning and outbound tenant webhooks for white-label set-ups	CONFIGURATION
	Referral programme with reward payouts; affiliate tracking	OPTIONAL
	Closed-loop and loyalty tokens with redemption	OPTIONAL
	External fee-payment handling, card shipment addresses, mobile deep links, open-banking contactless payments	OPTIONAL INTEGRATION
	Promotional giveaways	OPTIONAL



Customer panel: currency and crypto accounts.



Administration: fee settings by service.



Administration: notifications.

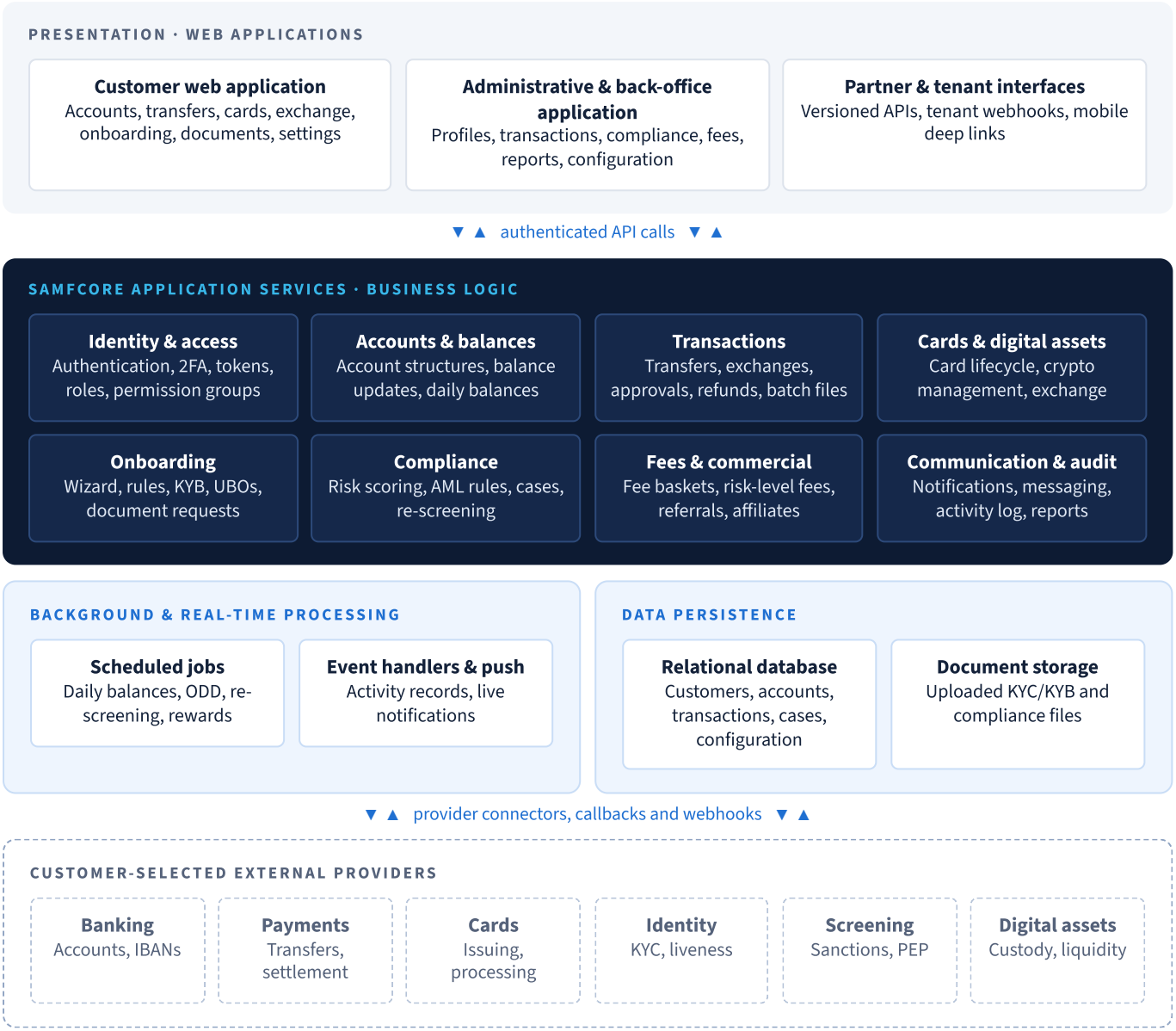
Availability and status

The matrix reflects SAMFCore's documented functionality. Additional modules are included only where they suit a deployment. For integration-dependent features, availability depends on a compatible provider, its commercial terms and the agreed integration scope. The modules active in the current release and in each proposed deployment are confirmed during demonstration and solution design.

07 · FOR TECHNOLOGY LEADERS

Technical Architecture & System Design

A logical view of SAMFCore's main components and how they relate. Physical topology is defined for each deployment.



Separation of interfaces

Customer and administrative applications are separate, each with its own access controls, and both use the same backend services.

Command-based services

Business operations such as approving a transfer or a profile are handled by dedicated application commands that validate and persist each change.

Event-driven audit

Business events across nearly every module trigger handlers that write persisted activity records.

07 · CONTINUED

Technology stack and design principles

Technology confirmed in SAMFCore's internal technical reference, summarised at a level suitable for initial evaluation.

Layer	Technology
Backend services	Microsoft .NET application services written in C#, structured as API controllers and application commands
Web front ends	React single-page applications in TypeScript, using Redux and RTK Query for state and data fetching, for the customer and administrative interfaces
Database	Microsoft SQL Server
Background processing	Hangfire scheduled and recurring jobs, for example daily balance calculation, Ongoing Due Diligence and reward payouts
Real-time communication	SignalR hub over WebSockets, used for live notifications
Authentication	JWT access and refresh tokens with automatic refresh; optional Google Authenticator 2FA; cookie-session-based administrative access control
Document storage	Azure Blob Storage in the documented configuration
Analytics	Embedded Microsoft Power BI reporting, alongside SAMFCore's own report catalogue
APIs	Versioned REST-style APIs, so new versions can be introduced alongside existing ones

Configurability and modularity

Much of the operating model is configuration rather than code: onboarding rules by country and category, document types, risk levels and country risk scores, AML monitoring rules, fee baskets, enabled cryptocurrencies, administrator roles and permission groups, notification templates and tags. Modules can be enabled to match the licensee's products.

White-label and tenant functionality

SAMFCore includes tenant provisioning and outbound webhook dispatch to tenants, supporting white-label and partner set-ups. Branding, brands and tenant structure for each deployment are defined in solution design and must fall within the licensed brand scope.

Hosting and infrastructure

SAMFCore runs on infrastructure the licensee controls. A deployment needs hosting for the .NET services and web applications, a SQL Server database, document storage and background job processing. Hosting environment, sizing, scalability, resilience and database configuration are specified for each deployment during solution design.

What is kept for due diligence

Source-code structure, internal endpoints, infrastructure configuration and detailed implementation documentation are not included in this memorandum. They can be reviewed during advanced technical due diligence under appropriate confidentiality arrangements.

08 · OPERATIONAL CONTROL

Security, Access Control & Auditability

Documented controls that help a licensee govern who can do what, and keep a record of what was done.

Customer authentication

Email and password sign-in with JWT access and refresh tokens that refresh automatically. Sign-in attempts are recorded. Customers can see signed-in devices and recent sessions in their security settings.

Two-factor authentication

Optional two-factor authentication with Google Authenticator. Customers are prompted to enable it from their security settings.

Administrator access and roles

Administrative access uses a separate, cookie-session-based role-based access control model. Named administrator roles bundle permissions that control both access to pages and individual interface controls.

Permission groups

Separate, configurable permission groups bundle customer-side permissions, for example whether public personal or business account opening is allowed, independently of administrator roles.

Approval controls

Transaction approval, rejection and refund, identity-profile approval, document approval with an escalated high-risk path, and second-administrator approval for high-risk personal profiles.

Activity logging and audit trails

A domain-event-driven activity log: business events across nearly every module write a persisted activity record, visible to administrators and, where relevant, to customers.

Transaction and compliance histories

Transaction status, AML review records, compliance cases, document requests and profile decisions are kept and linked to the customer.

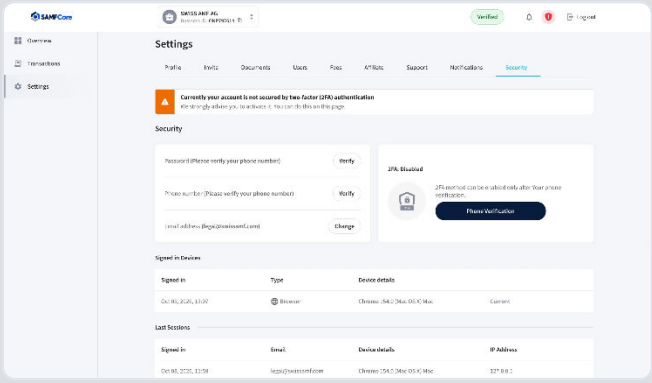
Monitoring and notifications

Operational work queues on the administration dashboard, actionable alerts and real-time notifications keep teams informed of items needing attention.

Security responsibilities in customer-controlled deployment

Because the licensee runs SAMFCore on infrastructure it controls, it is responsible for hosting security, network controls, encryption settings, key and secret management, backups, disaster recovery, infrastructure monitoring and security testing of its environment. Swiss AMF AG supplies the licensed software and can provide agreed implementation and support services. Security architecture is reviewed together during solution design.

This memorandum makes no claim of ISO certification, SOC reports, penetration-test results, uptime commitments or recovery objectives. Supporting technical and security documentation can be considered during advanced due diligence, subject to availability and appropriate arrangements.

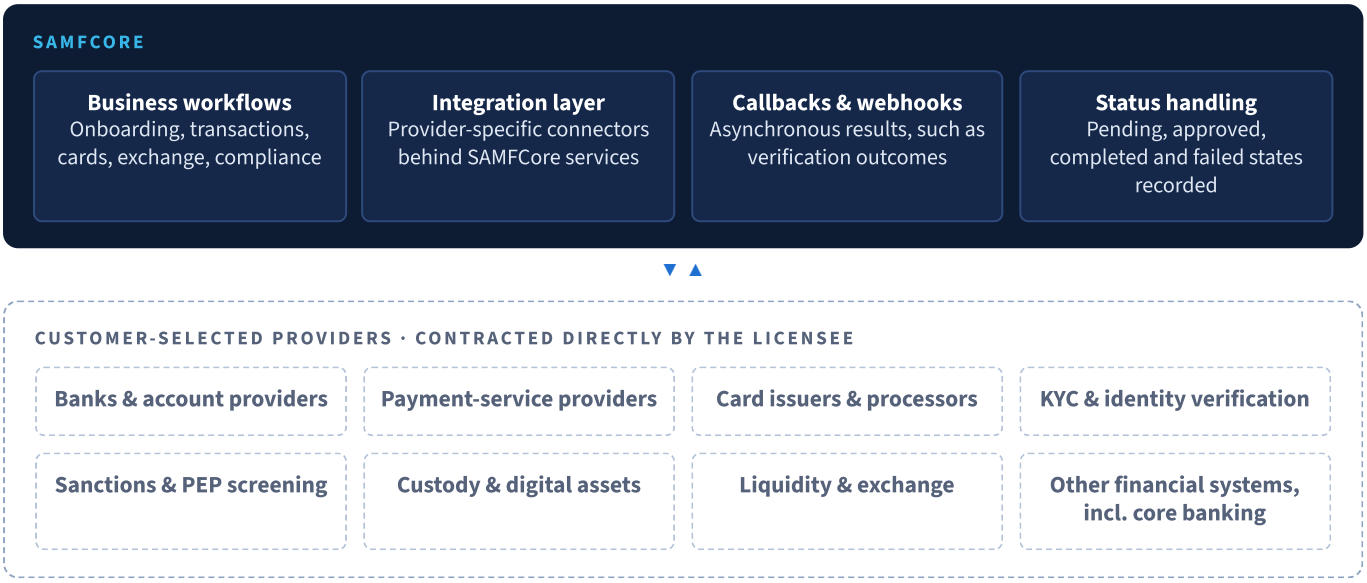


Customer panel: security settings with 2FA, signed-in devices and sessions.

09 · PROVIDER INDEPENDENCE

APIs, Integration Framework & Provider Connectivity

SAMFCore keeps customer, account, transaction and compliance logic in the platform and connects specialist services through provider-specific connectors.



Existing and new integrations

Existing integrations documented in SAMFCore include Sumsub for identity verification and screening, a card-issuing integration for the card lifecycle, open-banking, analytics and attribution services, and blockchain address provisioning. Whether an existing integration can be reused depends on the licensee's contract with that provider.

New integrations with other banks, PSPs, issuers, custodians or existing core banking systems need implementation work, scoped according to the provider's APIs and the workflows required. SAMFCore does not claim universal compatibility, and naming a provider category does not mean it is pre-integrated.

The integration process

1 · Provider selection
The licensee chooses and contracts providers suited to its business and jurisdictions

2 · Technical assessment
APIs, authentication, callbacks, data and status models reviewed

3 · Configuration or development
Existing connector configured, or a new connector built within agreed scope

4 · Testing
End-to-end journeys, status handling and failure cases validated in a non-production environment

5 · Operation
The licensee runs the live connection; provider services and fees remain under its provider contracts

API authentication uses token-based access. Provider results that arrive asynchronously, such as identity-verification outcomes, are received through callbacks and update the relevant SAMFCore record. Detailed interface specifications are shared during technical due diligence. SAMFCore is licensed software and is not itself a bank, card issuer, processor, custodian, exchange or regulated KYC/AML provider.

10 · AFTER PURCHASE

From Software Acquisition to Operational Launch

Ready-built software removes the multi-year build phase. Where provider connections and configuration are already in place, a branded deployment can be established in days; timing depends on integrations, configuration, regulatory requirements and scope.

01
Requirements discovery
Business model, products, customer types, jurisdictions, providers and licence scope.

02
Technical solution design
Modules, balance model, integrations, environments, security architecture and responsibilities.

03
Infrastructure preparation
Licensee-controlled hosting, SQL Server database, document storage and background processing.

04
Deployment & configuration
Onboarding rules, risk levels, AML rules, fees, roles, permissions, products and notifications.

05
Provider integrations
Existing connectors configured and new connectors implemented within agreed scope.

06
Customer branding
Brand identity, domains, communications and email templates, within licensed brand scope.

07
Testing & user acceptance
Customer journeys, administration, compliance workflows and provider flows tested and accepted.

08
Production launch
Go-live on the licensee's infrastructure, once its regulatory and provider arrangements are in place.

09
Post-launch support
Optional Swiss AMF integration, maintenance, support and compliance services, agreed separately (see next page).

Configuration, integration and custom development

Type of work	What it means	Typical treatment
Standard configuration	Settings in the existing software: onboarding rules, document types, risk levels, AML rules, fees, roles, branding elements	Part of deployment and configuration
Additional integrations	Connecting a provider without an existing SAMFCore connector, or one with a different API model	Scoped and quoted per provider
Custom development	New functionality or material changes to existing workflows beyond the current release	Scoped and quoted, or built by the licensee under source-code rights

Licensee responsibilities

Regulatory permissions; contracts with banking, card, KYC, screening, custody and liquidity providers; production infrastructure and its operation; and operating staff for customer service, operations and compliance.

Swiss AMF AG responsibilities

The licensed software, agreed implementation and integration within scope, Progressive Cutover Migration with Enterprise Global, and any separately agreed support, maintenance and development.

10 · OPTIONAL SWISS AMF SERVICES

Keep the Control. Let Us Handle the Technical Work If You Want.

SAMFCore can be operated and maintained by your own team, but Swiss AMF can also provide the technical resources needed to integrate providers, support the platform and coordinate post-sale security and compliance work. These services are optional and agreed separately.

End-to-End Provider Integration

Our development team can manage the complete provider-integration process—from technical scoping and API mapping through development, configuration, sandbox testing, reconciliation and production go-live—for banking, payment, card, custody, liquidity, KYC/KYB, AML, compliance and other providers where suitable APIs, documentation and technical access are available.

Subject to API availability, compatibility, provider cooperation, credentials, testing, commercial and regulatory requirements; separately scoped and priced.

Ongoing Support & Maintenance

After launch, Swiss AMF can continue as your technical partner for ongoing maintenance, troubleshooting, software updates, infrastructure and deployment support, provider changes, additional integrations and further platform development.

Support is optional under applicable perpetual licensing structures—you retain the freedom to use your own technical team while having Swiss AMF available when you need us.

Compliance, Security & Certification Support

After purchase, Swiss AMF can coordinate and support security, privacy, compliance and independent assurance work for your SAMFCore deployment, helping customers prepare the deployed environment for the standards and compliance programmes relevant to their business model.

Available services can include ISO/IEC 27001, ISO/IEC 27701, VAPT, SOC 2 Type II, PCI DSS where applicable, and GDPR/CCPA compliance programmes, commissioned individually or in parallel.

Compliance, Security, Assurance & Certification Services

Service	Type of engagement	Indicative price
ISO/IEC 27701 – Privacy Information Management System (PIMS)	Independent certification	€6,000
VAPT – Vulnerability Assessment & Penetration Testing	Security testing	€10,000
ISO/IEC 27001 – Information Security Management System (ISMS)	Independent certification	€8,000
SOC 2 Type II (AICPA) – System and Organization Controls	Independent attestation	€20,000
GDPR Compliance Programme	Compliance programme	€15,000
CCPA Compliance Programme	Compliance programme	€13,000
PCI DSS Level 1 Validation, where applicable	Compliance validation	€20,000

Indicative pricing. Final scope, deliverables, independent third-party costs and timing are confirmed in the applicable engagement documentation. The VAPT indicative price includes initial testing and fixes, as applicable. PCI DSS applicability depends on deployment scope; it includes vulnerability and penetration-testing requirements for applicable in-scope environments.

Timing: target implementation and compliance programme approximately 90 days; multiple workstreams may run in parallel; actual timing depends on scope, remediation needs, customer readiness and third-party auditor/certification-body processes. **Who issues what:** ISO/IEC certificates come from independent certification bodies and SOC 2 Type II reports from independent auditors; Swiss AMF coordinates and supports this work but does not issue certificates, no outcome is guaranteed, and SAMFCore itself does not currently hold ISO, SOC 2 or PCI DSS certification. GDPR and CCPA are compliance programmes, not certifications.

YOU DO NOT HAVE TO CHOOSE BETWEEN LONG-TERM INDEPENDENCE AND HANDS-ON TECHNICAL SUPPORT.

Operate SAMFCore with your own team, use Swiss AMF for specific projects, or engage us as an ongoing technical partner—the choice remains yours.

11 · TECHNICAL INDEPENDENCE

Full Source Code & Technical Handover

Greater control over a licensed deployment: inspect, maintain and develop it with your own team or with developers you appoint.

What Full Source Code enables

- Inspect the licensed codebase and application architecture.
- Maintain, customise and further develop your deployment.
- Use internal engineers or appointed third-party developers.
- Set your own development priorities and release timing within the rights granted.
- Reduce dependence on a single vendor for the future of your platform.



Illustration; not a screenshot of the source repositories.

Availability

Full Source Code is included with **Perpetual + Full Source Code (from €620,000)** and **Enterprise Global (€790,000)**. Customer-controlled deployment does not in itself require Full Source Code.

Technical handover

The deliverables for a Full Source Code licence are agreed in the licence and implementation contract. They typically fall into these categories:

Source code

Backend services, web applications and related components within the licensed scope.

Build & deployment

Build and deployment materials and environment configuration guidance for the agreed environments.

Documentation

Technical and implementation documentation for the delivered components.

Knowledge transfer

Training and handover sessions for the licensee's technical team, as agreed.

Skills to operate and develop

Teams maintaining the code typically work with C#/.NET, React and TypeScript, Microsoft SQL Server and the hosting environment chosen for the deployment.

Your contractual rights

The licence defines the right to maintain, modify and develop the system independently for the licensed entities, brands and permitted business scope.

RIGHTS, NOT OWNERSHIP

Source-code rights are defined by the applicable agreement. The underlying SAMFCore intellectual property remains with Swiss AMF AG. Source-code access does not automatically grant resale, sublicensing, redistribution or use by unrelated third parties.

12 · CONTROLLED TRANSITION

Progressive Cutover Migration

A staged framework for moving from an existing platform to SAMFCore with validation at every step. Included with Enterprise Global within the agreed implementation scope.

1 · Discovery
Current systems, data, providers, constraints

▶

2 · Data mapping
Customers, accounts, balances, histories

▶

3 · Integration preparation
Provider transition where feasible

▶

4 · Testing
Migrated data and journeys validated

5 · Progressive transition
Agreed users or segments moved in stages

▶

6 · Reconciliation
Balances and records checked against source

▶

7 · Acceptance
Against agreed acceptance criteria

▶

8 · Final cutover
Transition and agreed decommissioning support

Why a progressive approach

Moving customers in stages lets each group be validated before the next moves. Balances and transaction records are reconciled with the source system, and issues are dealt with while the existing platform is still available. Provider continuity, data quality and operational readiness are assessed before any customer moves.

Data in scope

Customer and company profiles, account structures, balances, transaction histories and documents, as agreed in the migration design.

Acceptance

Criteria and reconciliation checks are agreed before migration begins and signed off at each stage.



Illustration; the migration design is specific to each deployment.

Existing platform stays available

Segments not yet migrated continue on the current platform while each stage is validated.

Provider continuity assessed

Banking, card and other provider relationships are reviewed for transfer or re-connection before cutover.

Customer communication

Each migrated group can be informed and supported according to an agreed communication plan.

ENTERPRISE GLOBAL ONLY

Progressive Cutover Migration is **included with Enterprise Global within agreed implementation scope**. It is not included with the Annual, Perpetual or Perpetual + Full Source Code licences. Exceptional data-extraction charges, third-party costs and material custom development outside scope may be quoted separately. No zero-downtime, zero-risk, credential-continuity or provider-retention guarantee is given.

13 · FOR FINANCE AND PROCUREMENT

Commercial Model & Long-Term Economics

SAMFCore's licensing is designed so that the licensee, not the software vendor, keeps the benefit of growth.

NO PER-TRANSACTION FEES. NO REVENUE SHARE.

Across all SAMFCore licensing models, there is **no SAMFCore software fee per customer transaction** and **no share of transaction fees or transaction revenue**. More customer activity does not increase SAMFCore software licence costs.

01

Perpetual contractual usage rights

A one-time licence grants permanent usage rights within the licensed entities, territory, brands and permitted business scope, so there is no indefinite renewal just to keep access.

02

Full Source Code availability

Full Source Code is available with Perpetual + Full Source Code and Enterprise Global, supporting independent maintenance and development.

03

Customer-controlled infrastructure

Run SAMFCore on hosting you select and control, under your own operating, security and data arrangements.

04

No per-end-customer licence fees

Unlimited end customers within the licensed scope, without a SAMFCore charge per user or customer.

05

Provider independence

Contract directly with the banking, payment, card, verification and custody providers that suit your business, and change them as your strategy evolves, subject to integration scope.

06

Enterprise Global scope

Global rights, unlimited white-label brands for one legal entity, Full Source Code and Progressive Cutover Migration within agreed scope.

Costs that remain separate

Third-party provider fees (banking, payments, cards, verification, screening, custody, liquidity), infrastructure and hosting, implementation and additional integrations, and optional maintenance, support and development are contracted and paid separately and may scale with the business.

Legal and accounting clarification

Usage rights are not ownership of the underlying SAMFCore intellectual property, which remains with Swiss AMF AG. Accounting and tax treatment depend on the buyer's policies and professional advice. No zero-future-cost or guaranteed-savings claim is made.

What the buyer acquires

A licensed software deployment, plus contractual rights defined by the selected package. Annual usage, perpetual usage, source-code access and Enterprise Global scope are distinct choices. They are alternatives, not cumulative steps, so the buyer can match rights to its strategy and budget.

Payment currencies

List prices are in EUR. Payment can be made in EUR, CHF, USD or GBP. Indicative conversions on samfcore.com use the latest ECB reference rates. Final contractual pricing is set in the licence agreement.

14 · COMMERCIAL OPTIONS

Licence Packages & Annual versus Perpetual

Four published packages at EUR list prices; each is an alternative, not a cumulative step.

Annual Licence
€80,000
per year
The right to use SAMFCore during the annual licence term.

Perpetual Licence
€325,000
one-time
Permanent contractual usage rights within the licensed scope.

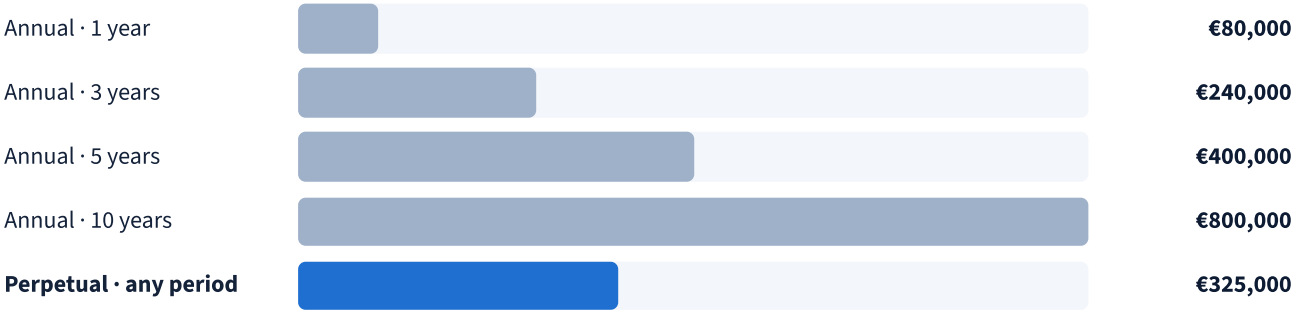
Perpetual + Full Source Code
€620,000
from, package price
Perpetual rights plus Full Source Code; not a surcharge on top of the Perpetual Licence.

Enterprise Global
€790,000
one-time
Perpetual rights, Full Source Code, global rights, unlimited brands for one entity and migration.

Included	Annual	Perpetual	Perpetual + Source	Enterprise Global
Permanent usage rights	No	Yes	Yes	Yes
Full Source Code	No	No	Yes	Yes
Legal entities included	1	1	1	1
Unlimited end customers	Yes	Yes	Yes	Yes
SAMFCore fee per transaction	None	None	None	None
Share of transaction revenue	None	None	None	None
Customer-controlled deployment	Yes	Yes	Yes	Yes
Geographic rights	As selected	As selected	As selected	Global
White-label brands	As selected	As selected	As selected	Unlimited, one entity
Progressive Cutover Migration	No	No	No	Within agreed scope

Annual versus perpetual: cumulative SAMFCore licence fees

Illustrative only. List licence fees, assuming the annual price stays unchanged. Excludes infrastructure, providers, implementation, support and maintenance.



On list licence fees alone, cumulative Annual Licence fees exceed the one-time Perpetual Licence price during year 5. The Annual Licence suits buyers who want lower initial commitment. The Perpetual Licence suits those planning to operate SAMFCore over the long term.

15 · BROADEST PUBLISHED SCOPE

Enterprise Global & Group Licensing

ENTERPRISE GLOBAL · €790,000

Perpetual usage rights, Full Source Code, global geographic rights, unlimited white-label brands and end customers for one licensed legal entity, and Progressive Cutover Migration within agreed implementation scope. There is no charge per customer transaction and no revenue sharing.

Included in Enterprise Global

- One licensed legal entity; further group entities are priced separately.
- Perpetual usage rights and Full Source Code under the agreement.
- Global geographic usage rights within licensed scope.
- Unlimited white-label brands and end customers within licensed scope.
- No SAMFCore per-user or transaction-volume licence fee.
- Customer-controlled deployment and provider-independent architecture.
- Progressive Cutover Migration within agreed implementation scope.

Scope remains defined

Global rights do not automatically license separate companies, third-party redistribution or unrelated operators. Provider agreements, regulatory permissions, implementation and separately quoted services remain separate. The published licence price is €790,000. Payment can be made in EUR, CHF, USD or GBP, with payment arrangements confirmed in the agreement.

Group and multi-entity licensing

Additional legal entities under common ownership or control are priced as transparent, non-compounding additions to the primary configured licence. Unrelated companies need a separate SAMFCore licence.

Licensed entities	Calculation	Total as % of primary licence
1	Included in the primary licence	100%
2	First additional entity: +40%	140%
3	Further entity: +25%	165%
4	Further entity: +25%	190%
5	Further entity: +25%	215%

Examples at EUR list prices: Annual Licence for two entities €112,000 / year; Perpetual Licence for two entities €455,000 one-time. These examples use the unmodified primary licence price. Additional configured scope, such as territory or brands, can change the primary amount. Each percentage is calculated on the primary configured licence and never compounds.

Configure your licence online

The SAMFCore licence configurator lets you compare packages and configure entities, brands, geographic scope and source-code requirements in EUR, CHF, USD or GBP: samfcore.com/overview#licence-configurator.

16 · AN ESTABLISHED PLATFORM

Swiss Development, Legal Opinion & Responsibilities

2018
Development began in partnership with a Swiss software development firm.

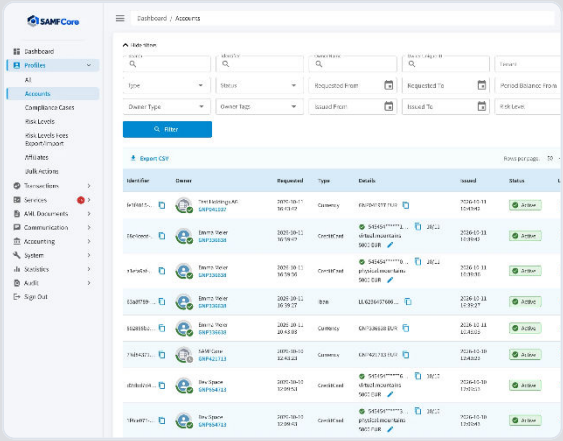
2021
Deployed in live financial-services environments since 2021.

Ongoing
Development and improvement have continued without interruption to the present day.

Zug
Developed and commercialised by Swiss AMF AG, Switzerland.

Development and operational history

SAMFCore is not a concept or a prototype. It has been in development since 2018 and in operational use since 2021. Prospective buyers evaluate actual customer and administrative interfaces, documented workflows and an established technical architecture.



Administration: customer accounts across currencies, IBANs and cards.

Independent Swiss Legal Opinion

Independent Swiss legal counsel has reviewed the legal and commercial foundation of SAMFCore, including IP ownership, perpetual and Full Source Code licensing rights, customer-controlled deployment, provider independence and the documented operational history.

A legal opinion may be made available to qualified prospective buyers during advanced due diligence, subject to confidentiality and the terms of the opinion.

Commercial responsibilities

Swiss AMF AG

Licensed software; implementation and integration within the agreed scope; Progressive Cutover Migration with Enterprise Global within scope; optional support, maintenance and development.

Licensee and its providers

Regulatory permissions; banking, card, KYC/KYB, screening, custody, liquidity and other provider contracts; infrastructure; separate service charges.

Due-diligence materials

For qualified buyers at an advanced stage, the following may be made available under confidentiality, subject to availability: detailed technical and implementation documentation, security and infrastructure information, the legal opinion, and draft licence and implementation agreements.

SAMFPay is a separate Swiss AMF AG product with its own licensing. SAMFCore rights, prices and fee policies do not extend to it.

17 · QUESTIONS BUYERS ASK

Buyer FAQ

1 What financial-services functionality is built into SAMFCore?

Customer accounts and multi-currency balances, transaction recording and status tracking, internal and batch transfers, approvals and refunds, onboarding with KYC/KYB, risk scoring, AML rules, compliance cases, fees, card and digital-asset workflows, CRM, notifications, reporting, permissions and an activity log.

2 Does SAMFCore maintain customer balances and transaction histories?

Yes. Its own transaction ledger records each movement with before and after balances and updates the account balance. Histories, statements and daily balance snapshots are kept in SAMFCore. Where a provider holds balances, SAMFCore can work with them through integration instead.

3 How are payments and externally settled transactions handled?

SAMFCore creates, validates, screens, approves and records the transaction. The connected bank, payment or card provider executes external money movement, and the resulting status is reflected in SAMFCore.

4 Does SAMFCore include its own customer onboarding software?

Yes. Registration, the onboarding wizard, country- and category-based rules, KYB with UBOs, document requests, risk levels and administrative approvals are native SAMFCore functionality.

5 How does Sumsub integrate with onboarding?

At the identity step of the SAMFCore wizard, the Sumsub verification is launched for document and liveness checks. Sumsub returns the result asynchronously and SAMFCore updates the KYC status. Sumsub can also support recurring sanctions/PEP re-screening.

6 Does SAMFCore have built-in AML and transaction-monitoring workflows?

Yes. A configurable rule engine flags transfers in real time, historical transfers can be re-screened, and flagged items go through AML review and compliance case management, including Ongoing Due Diligence.

7 Can we configure risk scoring and onboarding requirements?

Yes. Risk levels, country risk scores, monitoring rules, document types and onboarding rules by country and customer category are all configured by administrators. The licensee defines its own risk methodology.

8 Can we use our existing banking, payment and card providers?

Usually, yes. Existing connectors can be reused where the licensee has a contract with that provider. Other providers are connected through new integrations, scoped according to their APIs during solution design.

9 Can SAMFCore connect to other existing financial systems?

Yes, through API integration, including alongside an existing core banking system, for example to retrieve balances, initiate transfers and synchronise transactions. Feasibility depends on the APIs available in the other system.

10 Can we deploy SAMFCore on our own infrastructure?

Yes. Customer-controlled deployment is available with every package. The hosting environment and configuration are specified during solution design.

17 · CONTINUED

11 What technical resources are required to operate it?

Infrastructure and database operations for the hosting environment and Microsoft SQL Server, application support, and operations and compliance staff using the administrative application. Teams developing the code under source-code rights typically work with C#/.NET, React and TypeScript. Staffing is planned during solution design.

12 What does the Full Source Code licence provide?

Contractual rights to inspect, maintain, modify and further develop the licensed deployment, with deliverables such as source code, build and deployment materials, documentation and handover as agreed. The IP remains with Swiss AMF AG.

13 Can we appoint our own developers?

Yes. Under Full Source Code rights, the licensee can use internal engineers or appointed third-party developers within the rights granted by the agreement.

14 Are there per-user or per-transaction SAMFCore software fees?

No. All packages include unlimited end customers within licensed scope. No licence model has a SAMFCore fee per customer transaction or a share of transaction revenue. Provider, infrastructure and service costs are separate.

15 What is included in Enterprise Global?

Perpetual rights, Full Source Code, global geographic rights, unlimited white-label brands and end customers for one legal entity, and Progressive Cutover Migration within agreed scope, for €790,000.

16 How are migration and implementation handled?

Implementation follows discovery, solution design, configuration, integration, testing and launch. Migration follows the staged Progressive Cutover framework, which is included with Enterprise Global within agreed scope and can be scoped for other packages.

17 What support and maintenance arrangements are available?

Optional support, maintenance and development services can be agreed separately, with scope and terms set in the service agreement. With Full Source Code, the licensee can also maintain the system itself.

18 How do we arrange a demonstration or sandbox evaluation?

Schedule a call for a live demonstration and a requirements discussion, or request sandbox access to explore the customer and administrative environments, subject to access arrangements. Links are on the next page.

WHAT IS CONFIRMED LATER

Matters that depend on a specific deployment are confirmed during solution design and due diligence, and set out in the executed agreements. These include the hosting architecture, integrations in scope, service levels, deliverables and security documentation. This memorandum makes no commitment to specific SLAs, integrations or certifications.

18 · YOUR NEXT STEP

See SAMFCore. Discuss your scope.

The best way to judge SAMFCore is to see it working on your use case.

Schedule a Call

A live platform demonstration and direct discussion of your business model, provider stack, account and transaction workflows, onboarding and compliance needs, licence requirements and implementation scope.

SCHEDULE A CALL →

REQUEST SANDBOX ACCESS →

1 · Live demonstration

Customer panel, administration, onboarding, compliance and transaction workflows shown live.

2 · Sandbox evaluation

Explore the customer and administrative environments yourself, subject to access arrangements.

3 · Due diligence & proposal

Technical review, solution design, commercial proposal and agreements.

Configure your licence

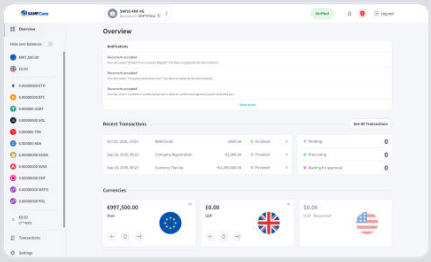
Compare EUR list pricing and configure entities, brands, geographic scope and source-code requirements.

OPEN THE LICENCE CONFIGURATOR →

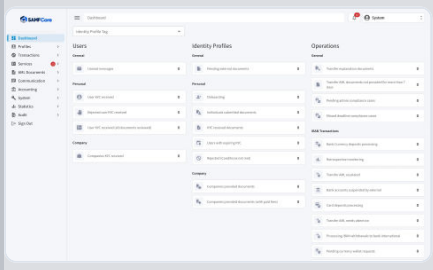
Swiss AMF AG

Bahnhofstrasse 21 · 6300 Zug · Switzerland
sales@swissamf.com · +41 43 508 26 22
samfcore.com

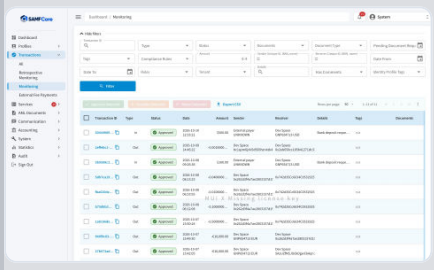
What you will see in a demonstration



Customer panel and accounts.



Operations dashboard and work queues.



Onboarding, AML and transaction monitoring.

This memorandum is buyer information only. Commercial terms, rights, deliverables, implementation scope and services are subject to definitive agreements. SAMFCore is licensed software. Banking, payment, card-issuing, custody, identity-verification and screening services are provided by the regulated providers each licensee selects. No regulatory approval, certification or regulated-service-provider status is claimed for SAMFCore. Screenshots show actual SAMFCore interfaces with demonstration data; they are not proof of a provider agreement or regulatory permission.