

ARMFast

Governed Agent Infrastructure for *Regulated Finance*

The control layer that lets financial institutions run auditable AI agents and durable compliance workflows on infrastructure they own — what it is today, what it is designed to become, and the evidence that separates the two.

AUTHOR

Aftab Ahmad

Director of Cyber Operations, ARM Technology Holding

Publication information

This white paper presents a strategic and technical assessment of ARMFast, the governed agent-infrastructure layer of ARM Technology Holding, with a focus on regulated financial services. It is intended for leadership, enterprise technology and security executives, compliance leaders, partners, and investors.

Title	ARMFast: Governed Agent Infrastructure for Regulated Finance
Author	Aftab Ahmad, Director of Cyber Operations
Publisher	ARM Technology Holding
Series	Sovereign Infrastructure Series — White Paper
Version	3.0
Publication date	August 2026
Reference	ATH-WP-003

Suggested citation

Ahmad, A. (2026). ARMFast: Governed Agent Infrastructure for Regulated Finance (White Paper, Version 3.0). ARM Technology Holding.

Copyright & rights

© 2026 ARM Technology Holding. All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form without the prior written permission of ARM Technology Holding, except for brief quotations with attribution. "ARMFast", "ARMcloud", "JoinMail", and associated marks are trademarks of ARM Technology Holding.

Legal notice

This document is provided for information only and does not constitute legal, financial, investment, or professional advice. It contains forward-looking statements about product plans, architecture, and strategy that are subject to change and describe intent rather than commitment. Capabilities are labelled by evidence status (see Notation & Evidence Standards, overleaf), and performance figures attributed to third-party open-source projects are the results of those projects, not of ARMFast. ARM Technology Holding makes no warranty as to the accuracy or completeness of the information and accepts no liability for reliance upon it.

Naming disambiguation

ARMFast and ARM Technology Holding are not affiliated with Arm Holdings plc, the semiconductor IP company (LSE/NASDAQ: ARM), nor the Arm processor architecture. Where this paper refers to "Arm hardware" it means the Arm64 CPU instruction set, a separate matter from the ARMFast brand.

Contact · **armfast.com** · ARM Technology Holding

Notation & evidence standards

This paper is written to survive technical and commercial due diligence. Its central discipline is the separation of what ARMFast *is* from what it is *designed to become*. Every material capability carries one of seven labels, and capabilities belonging to third-party open-source projects are attributed to those projects rather than presented as ARMFast's own.

[VERIFIED] Demonstrated or supported by reliable, independent evidence.

[DEMONSTRATED] Shown by ARMFast's team; not independently validated.

[SPECIFIED] Defined in the Platform Scope; implementation not yet proven.

[UPSTREAM] Capability and any benchmark belong to a third-party project ARMFast integrates.

[PLANNED] Roadmap capability.

[STRATEGIC HYPOTHESIS] A proposed business or product assumption to be validated.

[UNVERIFIED] Insufficient evidence at the time of writing.

Contents

Executive Summary	5
1. The Shift to Agentic Enterprise Computing	7
2. The Problem: AI in Regulated Environments	7
3. Why Financial Services Is Different	7
4. What ARMFast Is — and Is Not	8
5. ARMFast Core	9
6. ARMFast FinTech Compliance Suite	9
7. ARMFast Architecture	11
8. Agent Identity & Governance	12
9. Agent Security	13
10. Workflow & Orchestration	13
11. AI Inference, Memory & RAG	14
12. Sovereign & Portable Deployment	14
13. Security & Compliance	15
14. AML Investigation Use Case	17
15. Other FinTech Opportunities	18
16. ARM Technology Holding Ecosystem	18
17. Competitive Landscape	18
18. Build vs Buy vs Cloud	19
19. Market Gap	20
20. Ideal Customer Profile	20
21. Beachhead Market	20
22. Market Opportunity	21
23. Business Model	21
24. Product Strategy	22
25. Differentiation & Moat	22
26. Product Maturity & Evidence	24
27. Risks & Limitations	24
28. Proof Agenda	25
29. 12-Month Roadmap	25
30. Strategic Outlook	26
Conclusion, Scorecard & Recommendation to the Board	26
Appendices A–M	28

Executive Summary

Enterprise computing is entering its agentic phase. Software is moving from producing answers on request to pursuing goals — planning across steps, calling tools, retrieving knowledge, and acting with limited supervision. In regulated industries this shift collides with a hard constraint: an autonomous system that touches sensitive data and takes consequential actions must be identifiable, governable, auditable, and, increasingly, run where the institution's data is legally allowed to live. That is not a model problem; it is an infrastructure and control problem.

ARMFast is being built to address exactly that control problem. This paper makes a deliberate, disciplined case for it — and is equally deliberate about what is not yet proven, because for a platform whose product is trust, credibility is the asset and overstatement is the fastest way to lose it.

The position

ARMFast is best understood as two things, and the distinction is load-bearing throughout this paper. **ARMFast Core** is a governed agent control layer: agent identity, policy enforcement, durable workflows, memory and retrieval, model routing, auditability, and self-hosted deployment. **The ARMFast FinTech Compliance Suite** is the customer-facing solution built on that core — AML alert triage, investigation, KYC, transaction monitoring, sanctions, and auditable document intelligence. The Core is the platform; the Suite is what an institution actually buys first.

Positioning

ARMFast is the governed, self-hosted agent control layer for regulated financial institutions that enables auditable AI agents and durable compliance workflows while keeping sensitive data on infrastructure the institution owns. The recommended entry point is a single high-value workflow — AML alert triage and investigation with auditable document intelligence — not a general platform.

Why now, in one paragraph

The demand is evidenced, not asserted. In a 2025 survey of 2,567 senior decision-makers across 30+ markets, 95% called private or sovereign AI important to their strategy and 97% said critical workloads belong on-premises or in private environments; integration complexity in hybrid environments ranked as the single biggest obstacle. Regulation is turning this from preference into procurement gate — DORA took effect for EU financial services in January 2025, alongside the EU AI Act, NIS2, APRA and AUSTRAC obligations, and the NIST AI RMF. Independent estimates place the sovereign-cloud market near USD 80 billion in 2026. Financial services, with compliance already embedded in its culture, is the sector most ready to buy governed, self-hosted AI.

What is genuinely strong

- **The market thesis.** Sovereignty is now a purchasing requirement in regulated finance, and fragmentation is the number-one operational pain — both independently evidenced.
- **The architectural strategy.** Composing mature open-source infrastructure into a governed, self-hostable control plane is a sound, capital-efficient path — provided the composition is disciplined.
- **A concrete, demonstrable capability.** The document-intelligence approach ARMFast adopts (PageIndex-style vectorless retrieval) is a legitimately strong, independently-reported capability for financial-document analysis — attributed correctly below.
- **Ecosystem distribution.** ARM Technology Holding already operates regulated products (ARMUP, ARMF, ARMreview) that can serve as the first, captive customers and reference deployments.

What must be proven — stated plainly

- **No proprietary technology moat exists today.** Substantially the entire stack — including the agent-orchestration engine — is third-party open source. ARMFast’s defensible value must come from integration, governance, sovereign operations, and ecosystem, not from owning novel technology.
- **The headline performance numbers are upstream.** Every eye-catching figure belongs to an open-source component measured on its own hardware and dataset. None is an ARMFast platform benchmark, and the paper never presents them as such.
- **The product is pre-release.** The code described as open is not yet public; there are no independent security assessments, customers, or platform benchmarks. Maturity is early.
- **The specified architecture is too complex to ship as-is.** It must be cut to a minimal Core before a first customer; this paper specifies that cut.

The conclusion is constructive and conditional. The market is moving toward ARMFast, the product taxonomy is clean, and the FinTech-compliance beachhead is real and legally driven. The winning move is to get sharper, not bigger: ship a minimal Core, own one workflow, attribute every claim honestly, and build the moat in the ecosystem and the regulated data — not the technology. On that basis the recommendation to the board is **proceed, with conditions**.

1. The Shift to Agentic Enterprise Computing

Each era of enterprise software is defined by the unit of work it automates: packaged software automated tasks, cloud automated infrastructure, and generative AI automated the production of content. The agentic phase automates the pursuit of goals — an agent is given an objective, decomposes it, selects and calls tools, retrieves what it needs, observes results, and iterates, with a human reviewing rather than executing each step.

This changes the infrastructure requirement. An agentic workload is long-running and stateful, touches multiple systems, and can incur real-world consequences — so durable orchestration, persistent memory, machine and agent identity, and governance stop being optional. Independent 2025–26 estimates size the standalone agentic-AI market at roughly USD 7–8.5 billion, growing 40–46% annually. The discipline that matters more than the number: adoption trails spend — McKinsey finds only about 23% of organisations have scaled agent deployments, and Gartner warns that a large share of agentic projects may be cancelled by 2027 on cost, unclear value, or inadequate control. Infrastructure that makes agents governable and economical to run in production is therefore selling into a proven pain.

2. The Problem: AI in Regulated Environments

Moving an agent from demonstration to production requires assembling a stack: compute and GPU scheduling, model serving, an agent framework, a durable workflow engine, a vector store and retrieval pipeline, identity for humans and agents, secrets management, an API/LLM gateway, observability, and the security and compliance controls regulators expect. Each part is individually mature; the difficulty is the seams — integration, credential plumbing, and the audit fabric that ties an agent's actions to evidence.

For regulated organisations this fragmentation carries three compounding costs: engineering diverted from the application to integration; an enlarged attack surface spread across a dozen tools; and a slow, brittle path to the evidence an auditor or regulator demands. In the 2025 survey cited above, integration complexity in hybrid environments was the single most-cited obstacle to running AI on private infrastructure. A credible consolidation layer must do something specific and hard: unify the control plane — identity, policy, orchestration, and audit — while keeping the model and data planes open and replaceable, so consolidation does not simply re-create lock-in.

3. Why Financial Services Is Different

Financial services is the sharpest instance of the regulated-AI problem, for structural reasons that make it the natural beachhead.

- **Obligations are legal, not discretionary.** Anti-money-laundering, know-your-customer, sanctions screening, transaction monitoring, and virtual-asset travel-rule messaging are mandated and continuously evolving. The buyer has to act.
- **The work is exactly what agents are for.** These are long-running, auditable, human-in-the-loop investigative workflows over documents and data — durable orchestration and governed agents map onto them directly.

- **The data resists the cloud.** It is precisely the data institutions are reluctant or legally unable to send to a third-party cloud, which is why self-hosted and sovereign deployment is a purchase driver rather than a preference.
- **Governance culture already exists.** Financial institutions already run model-risk, audit, and approval processes; governed AI extends a discipline they understand, rather than imposing a new one.

The commercial implication is that the same capability — governed, auditable, self-hosted agent execution — is a "nice to have" in a generic enterprise and a "must have" in a regulated bank, exchange, or virtual-asset service provider. That is where ARMFast should start.

4. What ARMFast Is — and Is Not

ARMFast is the infrastructure layer of the ARM Technology Holding ecosystem — the middleware that powers ARM's own applications and, commercially, a governed agent control layer offered to regulated institutions. The Platform Scope draws a clean taxonomy that this paper adopts: **ARMFast** is the infrastructure layer (the equivalent of a cloud platform beneath products); **ARMcloud** is a business-productivity suite built on it (in development); and **JoinMail** is a consumer email product (in development). This paper concerns ARMFast, the infrastructure layer.

What ARMFast is

- **A governed agent control plane ([SPECIFIED])**: agent identity, policy, durable workflow, memory/RAG, model routing, audit, and self-hosted deployment.
- **An integrator of mature open-source infrastructure ([VERIFIED])**: it composes, hardens, and governs existing projects rather than reinventing them.
- **A FinTech-compliance solution vendor ([STRATEGIC HYPOTHESIS])**: the commercial product is the Suite built on the Core.

What ARMFast is not

- **Not a generic AI platform for everyone.** Attempting to serve all enterprises and use cases at once would dissolve its focus and its credibility.
- **Not the owner of novel core technology.** Its components — including the agent engine — are third-party open source (Sections 7, 11, 25).
- **Not "compliant," and not a producer of the headline benchmarks.** It supports compliance objectives; it integrates components whose benchmarks are theirs, not the platform's.

The four consistent explanations of ARMFast

30-second: governed AI agents for regulated finance, on infrastructure you own. Executive: a control layer that lets a bank run auditable AI agents for AML/KYC work without sending data to a hyperscaler. Technical: agent identity + policy + durable workflow + retrieval + audit over a self-hosted, open-source stack. Buyer: faster, auditable AML investigations with a complete evidence trail, deployed in your jurisdiction. All four describe the same product.

5. ARMFast Core

ARMFast Core is the reusable control layer. It is deliberately defined by the *functions* it must provide, not by the components that implement them — because the components are replaceable and the functions are the durable value.

Core function	What it provides	Status
Agent identity	Cryptographic identity per agent; distinct from user/service identity	SPECIFIED
Agent governance	Registration, approval, tool/data permissions, lifecycle, revocation	SPECIFIED
Policy enforcement	Default-deny permissions; human-approval gates for critical actions	SPECIFIED
Durable workflow	Fault-tolerant, long-running, auditable execution	UPSTREAM (Temporal)
Memory & RAG	Retrieval and agent memory over owned indexes	UPSTREAM (TurboVec, PageIndex)
Model routing	Model-agnostic serving; self-hosted models	UPSTREAM (Ollama/vLLM)
Auditability	Full, traceable audit of every user/agent action	SPECIFIED
Deployment control	Self-hosted; per-jurisdiction data residency	SPECIFIED

The commercial logic of the Core is a chain, not a feature list: *agent identity* → *controlled access* → *reduced privilege risk* → *a deployment a regulator will accept*; and *auditable workflow* → *traceable decisions* → *stronger compliance evidence* → *lower investigation friction*. Every Core function earns its place only if it terminates in customer value of this kind.

6. ARMFast FinTech Compliance Suite

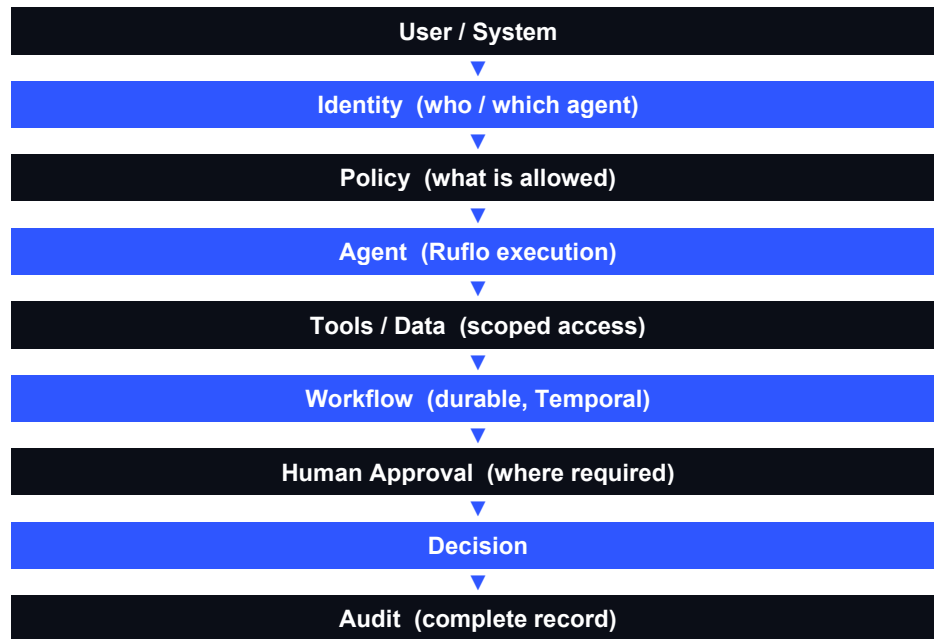
The Suite is what an institution buys. It is a set of customer-facing solutions built on the Core, and it is where ARMFast's story becomes concrete and demonstrable rather than infrastructural.

ARMFast Core (platform)	FinTech Compliance Suite (solution)
• Agent identity & governance • Policy enforcement & approvals • Durable workflow orchestration • Memory, RAG & document intelligence • Model routing (self-hosted) • Auditability & observability • Sovereign / self-hosted deployment	• AML alert triage • Investigation & case management • KYC / onboarding orchestration • Transaction monitoring • Sanctions & travel-rule workflows • Document intelligence & evidence • Regulatory-ready audit records

The separation matters commercially: the Core is sold once and reused across every workflow, while each Suite module is a discrete, evidenceable outcome a compliance buyer can evaluate. The recommended first module — AML alert triage and investigation — is developed in Section 14.

7. ARMFast Architecture

The architecture is best read from the customer's perspective, not the technology's. What a regulated buyer needs to see is a governed path from a request to an audited decision:



Underneath, ARMFast composes established open-source infrastructure. The honest and important question is whether this composition *simplifies* infrastructure for the customer or merely hides a complicated collection of technologies. As specified in the Platform Scope, the answer today is the latter: three workflow engines, three-plus agent frameworks, five-plus inference layers, six-plus retrieval tools, the full observability stack, four WSO2 products, and Kafka plus BullMQ plus Redis is more than a small team can operate, patch, secure, and support across two sites and five jurisdictions. Each component is a separate vulnerability, upgrade, and failure-mode stream.

Current, target, and MVP architecture

The paper therefore distinguishes three architectures and recommends shipping the third first.

Layer	Current scope (specified)	Recommended MVP	Deferred
Workflow	Temporal + Conductor + Prefect	Temporal	Conductor, Prefect
Agents	Ruflo + SIA + DeerFlow	Ruflo	SIA, DeerFlow
Inference	Ollama + Aibrix + vLLM + LMCache + cascadeflow + Exo	Ollama (+vLLM) + LMCache	Aibrix, Exo, cascadeflow
RAG / docs	MinerU + PageIndex + Proxy-Pointer + Hyper-Extract + TurboVec + GraphGen	MinerU + PageIndex + TurboVec	Proxy-Pointer, Hyper-Extract, GraphGen
Identity	WSO2 IS + Agent ID + APIM + AI GW + Agent Mgr	WSO2 IS + Agent ID	AI Gateway, Agent Manager
Messaging	Kafka + MirrorMaker + BullMQ + Redis	BullMQ + Redis	Kafka (multi-site only)
Data	PostgreSQL + Patroni + Citus + TimescaleDB	PostgreSQL + Patroni	Citus, TimescaleDB

Layer	Current scope (specified)	Recommended MVP	Deferred
Observability	Prometheus + Grafana + Loki + Tempo + OTel	Prometheus + Grafana + Loki	Tempo

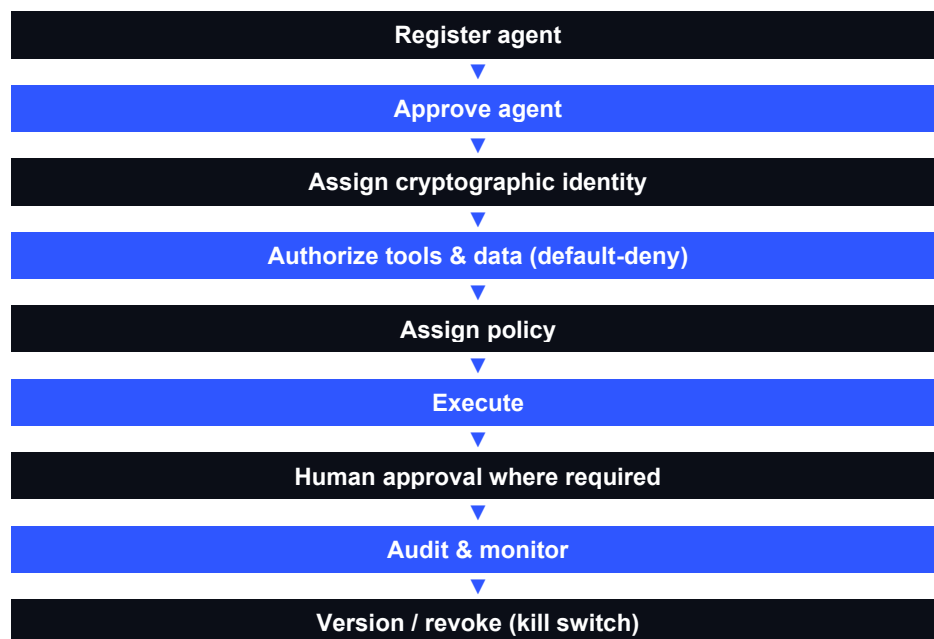
The answer to the most important architecture question

Does ARMFast simplify enterprise AI infrastructure, or hide a complicated collection of technologies? As specified, it hides complexity; as recommended (the MVP Core, roughly one-third the components), it can genuinely simplify — a coherent set a small team can operate, harden, and support, with everything else deferred to the point a paying customer needs it. Simplification is not a cosmetic choice; it is what makes the FinTech beachhead deliverable in twelve months rather than thirty-six.

8. Agent Identity & Governance

Agent identity is the architectural idea on which the regulated story rests. Enterprises already manage human identity, service identity, and workload identity; autonomous agents introduce a fourth category with different requirements, because an agent acts on a human's behalf, selects its own tools, and can chain actions across systems. Treating an agent as a first-class, cryptographically identified principal — rather than a script running under a shared service account — is what makes least privilege, delegation, revocation, non-repudiation, and a truthful audit trail possible.

ARMFast's specified approach uses WSO2 Agent ID for cryptographic agent identity and WSO2 Agent Manager for lifecycle governance, with Ruflo handling execution and memory. The intended governance lifecycle is a genuine value proposition for regulated buyers:



[SPECIFIED] This lifecycle is designed, not yet demonstrated end-to-end. The white paper claims it as target architecture; the proof that unlocks the claim is a reference deployment exercising the full lifecycle with a real audit trail (Section 28). Why it matters for finance: an institution can only deploy autonomous agents into AML or KYC work if it can prove, to an auditor, exactly which agent did what, under whose authority, with which permissions, and where a human intervened.

9. Agent Security

Agent infrastructure introduces threats that traditional application security does not fully cover. The right reference is the emerging OWASP guidance for LLM and agentic applications. ARMFast’s architecture is directionally sound and, in the Platform Scope, adds an unusually concrete control: SkillSpectre, a pre-deployment scanner that gates every new agent skill. The gaps are evidentiary — the controls are specified, not independently assessed.

Threat	Architectural mitigation (status)	Evidence still required
Prompt / indirect injection	PII stripping, policy gating, approval (SPECIFIED)	Tested tool-boundary guardrails
Excessive agency	Scoped agent identity, default-deny RBAC (SPECIFIED)	Enforcement proof
Tool poisoning / malicious skills	SkillSpectre pre-deployment scan (SPECIFIED)	Gate integrated & mandatory
Credential theft	OpenBao KMS, hardware passkeys (VERIFIED primitives)	Config & rotation evidence
Data exfiltration	Zero-trust, egress control, residency (SPECIFIED)	Demonstrated egress controls
RAG / memory poisoning	Owned indexes, access control (SPECIFIED)	Provenance validation
Agent impersonation	Cryptographic agent identity (SPECIFIED)	Implementation verification
Supply-chain risk	Licence-verified deps, hardened base (PARTIAL)	SBOM, signing, CVE scanning

The honest position: ARMFast is designed to mitigate these risks; it has not yet demonstrated that it does. The security-readiness roadmap in Section 28 converts this design into procurement-grade evidence — which, for a regulated buyer, is the difference between an interesting architecture and a deployable one.

10. Workflow & Orchestration

Durable workflow is the least glamorous and most important part of the Core for compliance work, because AML and KYC processes are long-running, must survive failures exactly once, and must be fully reconstructable after the fact. ARMFast’s selection of Temporal for compliance-critical execution is well-judged — Temporal is the strongest open-source option for durable execution, MIT-licensed, and production-proven. [\[UPSTREAM\]](#) The engine is Temporal’s; ARMFast’s contribution is selecting it, integrating it into the governed control plane, and wrapping it in agent identity and audit.

The Platform Scope also specifies Conductor and Prefect. For the MVP, this paper recommends Temporal only (Section 7): running three orchestration engines multiplies operational burden without a first-customer need. The value ARMFast adds is not another engine — it is the single governed control plane that makes durable workflow, agent identity, and audit one coherent surface instead of three systems to operate.

11. AI Inference, Memory & RAG

This section carries the paper’s strictest claim discipline, because it is where ARMFast’s most impressive numbers originate — and every one of them belongs to an upstream open-source project, not to ARMFast.

They are presented here as component capabilities, correctly attributed, and must never be read as ARMFast platform benchmarks.

Capability	Upstream owner	Reported result	Correct reading
Vectorless document RAG	PageIndex / Mafin 2.5 (VectifyAI, MIT)	98.7% on FinanceBench (vendor-reported SOTA)	Strong for structured filings; upstream, not ARMFast's
Vector index	TurboVec (RyanCodrai, MIT)	~16× compression; ~12–20% vs FAISS on Arm	Upstream; Arm-specific, one FAISS baseline
KV-cache reuse	LMCache (Apache 2.0)	up to 14× TTFT on H200-class HW	Upstream; specific hardware
Model cost/latency routing	cascadeflow (MIT)	40–85% cost / 2–10× (own tests)	Upstream; vendor tests
Structural chunking	Proxy-Pointer RAG	100% on 10-K filings at k=5	Upstream; narrow benchmark

The claim rule, once, for the whole paper

The correct form is: "An upstream technology in the proposed ARMFast architecture reports X; this is not an ARMFast platform benchmark." ARMFast's own platform-level performance — the behaviour of the composed system under real regulated workloads — has not yet been measured and will differ. The genuine opportunity here is real: PageIndex-style vectorless retrieval is a legitimately strong, auditable approach to financial-document analysis, and adopting it is a sound decision. The discipline is simply to credit it, and to publish ARMFast's own evaluation before claiming a platform result.

12. Sovereign & Portable Deployment

Sovereignty is used precisely in this paper, because it is ARMFast's strongest demand driver and its most easily overstated one. It is not one property but several, and ARMFast contributes genuinely to some and only partially to others.

Dimension	ARMFast contribution	Status
Data sovereignty	Self-hosted; per-jurisdiction residency zones	SPECIFIED (strong)
Compute sovereignty	Owned A100 capacity (AU); self-hosted inference	DEMONSTRATED (internal)
Key sovereignty	OpenBao KMS; customer-held keys	SPECIFIED
Identity sovereignty	Self-hosted WSO2 identity & agent ID	SPECIFIED
Model sovereignty	Self-hosted open-weight models	UPSTREAM (Ollama/vLLM)
Operational sovereignty	Customer-controlled operations	HYPOTHESIS (managed option)

Portable deployment, and the "zero trace" correction

The Platform Scope describes booting the full stack from an encrypted external drive (Podman, LUKS, OpenBao, WireGuard, PostgreSQL, RustFS) with, in its words, "zero trace on the host." This paper does not use that phrase, because literal forensic zero-trace cannot be guaranteed: residual artefacts remain outside the encrypted volume — USB device-registry and kernel/udev logs, swap and memory contents, filesystem and mount metadata, crash dumps, and network traces. The defensible and still-valuable objective is: **no application data written to host storage; encrypted, portable application state; customer-controlled credentials; and minimised host persistence, with residual OS-level**

device metadata addressed by host policy. Stated that way, the capability is real, differentiated, and survives a security review; stated as "zero trace," it does not.

13. Security & Compliance

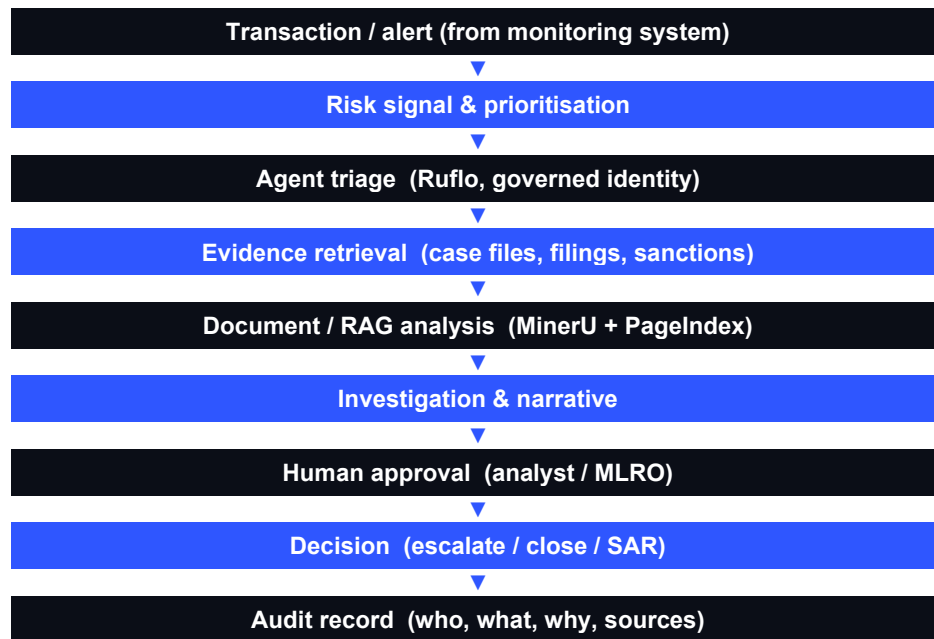
ARMFast should never claim to be compliant; compliance is a status only an audited deployment holds, and much of it remains the customer's responsibility. What ARMFast can credibly claim is that it is **designed to support** specific compliance objectives. The mapping below is the honest form, and it names the gap and the customer's share.

Requirement	ARMFast capability (status)	Gap / customer responsibility
ISO 27001 / 42001	Hardened base, RBAC, audit (SPECIFIED)	Independent assessment; SoA; customer ISMS
NIST AI RMF / OWASP LLM	Agent identity, SkillSpectre (SPECIFIED)	Red-team; customer risk governance
DORA	Two-site DR, RTO/RPO tiers (SPECIFIED)	Tested drills; customer resilience programme
GDPR / Privacy Act / PDPL	Residency zones (SPECIFIED)	Live regional nodes; customer DPA & lawful basis
AUSTRAC / FATF AML-CTF	AML/KYC workflows via ARMreview (DEMONSTRATED)	Reference deployment; customer AML programme
CDR (Australia)	Not addressed in scope	Design + assessment (both sides)

The security stack — WSO2 identity, OpenBao secrets, WireGuard networking, Wazuh/Auditd/AIDE monitoring and integrity, hardened Ubuntu base — is a sound foundation built on genuine primitives. The distinction the paper maintains is between security *design* (present, specified), security *implementation* (to be built and verified), and independent *assurance* (a third-party assessment, not yet obtained). Regulated buyers audit the third of these first; Section 28 makes obtaining it the near-term priority.

14. AML Investigation Use Case

The recommended first product is a single, high-value, legally-driven workflow: AML alert triage and investigation with auditable document intelligence. It is the right beachhead because it uses ARMFast's genuinely strong capability (document intelligence), targets a mandated pain, and produces an outcome a regulator understands — an auditable decision with a complete evidence trail.



Where ARMFast participates: it does not replace the transaction-monitoring system that raises the alert; it **governs and accelerates the investigation** that follows. The Core supplies the governed agent identity, the durable workflow, the retrieval over documents and case files, the human-approval gate, and the complete audit record. The upstream document-intelligence components supply the retrieval accuracy over structured filings.

Customer outcome

Dimension	Detail
Customer / buyer	Regulated FI or VASP; buyer = MLRO / Head of Financial Crime / CISO
Existing process	Manual analyst triage across siloed tools; document review by hand
Pain	Alert backlogs, slow investigations, inconsistent evidence trails, audit friction
ARMFast intervention	Governed agent triage + document intelligence + auditable workflow
Expected outcome	Faster, more consistent investigations with a complete evidence record (potential value driver — to be validated per deployment)
Evidence required	Design-partner deployment; measured triage-time and evidence-completeness

[STRATEGIC HYPOTHESIS] No efficiency figure is claimed here. Any savings are an illustrative hypothesis until a design partner measures them; the paper commits to producing that measurement rather than asserting a number.

15. Other FinTech Opportunities

Once the AML beachhead is proven, adjacent modules reuse the same Core with high marginal leverage. They are sequenced deliberately — the discipline of Section 37 ("what not to do") is to prove one before selling many.

Module	Reg. driver	Reuse of Core	Priority
KYC / onboarding orchestration	AML-CTF, identity rules	Very high	2
Transaction monitoring triage	AML-CTF	High	2
Sanctions / travel-rule (VASPs)	FATF travel rule	High	3
Regulatory reporting	Local reporting regimes	Medium	3
Wealth / income profiling (ARMF)	Suitability, KYC	Medium	4

16. ARM Technology Holding Ecosystem

The ecosystem is ARMFast's strongest moat candidate — and the paper is careful not to overstate it. A moat exists only to the extent that integrations are operational and create genuine switching costs; the mere existence of many products is not a moat. The table classifies each relationship honestly.

ARM product	Role for ARMFast	Integration status
ARMUP (crypto exchange)	First customer; travel-rule / wallet-monitoring agents	In development
ARMF (wealth / FinTech)	First customer; profiling analytics	In development
ARMreview (compliance)	AML/KYC investigation app; reference workflows	Demonstrated (internal)
theArmID (identity/KYC)	Identity & KYC agent source	Planned
ARMchain	Provenance / PQC crypto team	Conceptual / planned
ARMcloud / JoinMail	Productivity / email built on Core	In development
ARM Audit	Audit-trail generation	Planned

[STRATEGIC HYPOTHESIS] The strategic value is real but conditional: ARMUP and ARMF are genuine regulated operators that can be first customers and reference deployments — a distribution advantage a standalone startup does not have. The switching-cost moat, however, is built only when identity (theArmID) and compliance (ARMreview) integrations are live and generating shared data. Until then, the ecosystem is a distribution advantage and a moat *candidate*, not a moat.

17. Competitive Landscape

The purpose of competitive analysis is credibility, not victory. ARMFast is compared here at its true, present maturity — pre-release — against competitors' production capability, with maturity stated explicitly. No competitor offers the exact bundle; the honest reading is that each capability is available elsewhere, more mature, and ARMFast's claim must be the governed, sovereign, FinTech-tuned *combination*, proven.

Category / player	What it offers	Maturity	Relationship to ARMFast
Agent frameworks (LangGraph, CrewAI, AutoGen, ADK, Semantic Kernel)	Agent orchestration	Production	Substitute for the engine; ARMFast uses Rufflo (same class)
Workflow (Temporal, Conductor, Prefect, n8n)	Durable / visual workflow	Production	Components ARMFast integrates
Hyperscalers (AWS/Azure/GCP)	Managed agent + AI infra	Production	Primary alternative; not sovereign
Databricks / Snowflake	Governed data + AI	Production	Adjacent; not self-hosted/agent-native
Sovereign-AI infra (e.g. VAST)	On-prem AI factories	Production	Complement below ARMFast
RegTech (KYC/AML/case mgmt)	Domain compliance tools	Production, referenced	Integrate & orchestrate, not replace
ARMFast	Governed sovereign agent control + FinTech Suite	Pre-release	—

18. Build vs Buy vs Cloud

Dimension	ARMFast	DIY on OSS	Hyperscaler	Specialist RegTech
Sovereignty / residency	High (self-hosted)	High	Limited	Varies
Time to value	Medium (pre-integrated)	Low (months of work)	High	High (narrow)
Agent governance	Designed-in	Build yourself	Improving	Limited
Operational burden	Vendor-managed (goal)	Entirely yours	Low	Low
Breadth (agent+workflow+RAG)	Unified (goal)	Assemble	Managed	Narrow
Maturity today	Pre-release	Proven parts	Highest	Proven
Best when	Regulated + sovereign + agentic	Deep in-house team	Cloud-permitted	Single point need

The paper does not claim ARMFast wins every comparison. Hyperscalers are better where the cloud is permitted and scale and support dominate; DIY is better for teams with deep in-house capability and time; specialist RegTech is better for a single, well-defined point need with live references. ARMFast's honest edge is the *intersection*: regulated + sovereign + agent-native + pre-integrated + governed. Its answer to "why not build it?" is the 6–12 months of integration and the governance/audit fabric a customer would otherwise build and still have to secure; its answer to "why not cloud?" is data residency and vendor independence; its answer to "why not RegTech?" is that it *orchestrates* those tools rather than replacing them.

19. Market Gap

The gap is validated, not assumed. The evidence: 95–97% of senior decision-makers prioritise private/sovereign AI and keep critical workloads on-premises; integration complexity is the #1 hybrid obstacle; DORA and peers make data control a procurement gate; and no incumbent offers a self-hosted,

agent-native, governed, FinTech-compliance-tuned bundle. The underserved problem is specific: **running auditable AI agents on regulated financial data, on infrastructure the institution controls, without assembling and securing a dozen tools.** The gap is real and emerging rather than a proven, contested category — which is an opening, provided ARMFast treats it as a hypothesis to be proven by design-partner revenue.

20. Ideal Customer Profile

Attribute	ARMFast initial ICP
Institution type	Regulated FI, payments/remittance firm, or crypto/VASP
Size	200–5,000 staff (mid-market; large enough to have an MLRO, small enough to move)
Geography	Australia first; then GCC/UAE
Regulation	Active AML-CTF + data-residency obligations (AUSTRAC/APRA, PDPL)
Data sensitivity	High; cloud-restricted financial-crime and customer data
Infrastructure	Hybrid / on-premises capable; wary of hyperscaler lock-in
Buyer / champion	MLRO / Head of Financial Crime / CISO
Buying trigger	Alert backlog, audit finding, DORA/AUSTRAC pressure, cloud-restriction
Sales cycle	6–12 months (regulated procurement + security review)
First instances	ARM ecosystem operators (ARMUP, ARMF)

21. Beachhead Market

Region	Reg. fit	FinTech density	Sovereignty demand	ARM advantage	Priority
Australia	High (APRA/AUSTRAC)	Medium	High	A100 in AU; entity	1 Primary
UAE / GCC	High (PDPL)	High	Very high	ARM ME / KSA	2 Secondary
Pakistan	Medium	Medium	Medium	Team + ops	3 Build/pilot
Singapore	High (MAS)	Very high	High	Limited	4
UK / EU	High (DORA/FCA)	High	High	Limited	5 Later

[RECOMMENDATION] First market Australia — regulatory fit, sovereign A100 capacity in-country, and a legal entity give the shortest path to a credible first deployment. Second GCC/UAE — the highest sovereignty demand plus ARM’s Middle East presence. Pakistan is the build-and-pilot base, not the first commercial market. This sequence should change only if a design partner emerges faster elsewhere.

22. Market Opportunity

Market-sizing confidence is low given ARMFast’s pre-revenue stage and the wide dispersion of published estimates; the figures below are scenario boundaries built bottom-up with visible assumptions, not forecasts. The paper distinguishes the broad market from ARMFast’s realistically addressable slice.

Scenario (Year 3)	Paying institutions	Blended ACV	ARR	Assumptions
Conservative	12	USD 70,000	~USD 0.8M	Ecosystem + few design partners; slow proof
Base	40	USD 120,000	~USD 4.8M	Beachhead traction; 2–3 managed deals; refs published
Aggressive	110	USD 190,000	~USD 20.9M	Category validated; GCC + adjacent modules

Layer	Indicative value	Basis
TAM (2026)	~USD 9–12B	Self-hostable share of agentic AI + orchestration + vector tooling
SAM	~USD 1.5–2.5B	Self-hosted/sovereign + regulated-FinTech subset, target regions
SOM (Yr 3, base)	~USD 4.8M ARR	Bottom-up: 40 institutions × ~USD 120k ACV

23. Business Model

Open-core (NetHSM-style: source-available and auditable, production under licence) fits the buyer — who wants to read the code for trust and pay for production, support, and indemnity — but only if the open tier actually ships. Generic self-hosted licences compete with free assembly and with the underlying open-source projects directly, so the defensible revenue is vertical and managed.

- **Flagship:** ARMFast FinTech Compliance Suite — priced per institution.
- **Attach:** Managed Sovereign Deployment — ARMFast operated on the customer's or a sovereign-region's infrastructure, priced on capacity + support.
- **Attach:** Enterprise Assurance — SLA, security advisories, indemnity, compliance-evidence packs.
- **Funnel, not revenue:** the open/developer tiers.

Pricing should be as simple as the product is focused: an annual per-institution licence for the Suite, a capacity-based fee for managed deployment, and a support/assurance tier — not a per-agent or per-workflow meter that adds friction to a regulated sale.

24. Product Strategy

Sell two things, in order: a deliberately minimal **ARMFast Core** (Section 7 MVP) and, on top of it, the **FinTech Compliance Suite** with AML triage as the first module. Add Managed Sovereign Deployment and Enterprise Assurance as attach. This is the whole product strategy; its discipline is as much about refusal as ambition.

What ARMFast should not do

- Do not position as a generic AI platform for everyone.
- Do not ship three workflow engines or three agent frameworks; run one of each.
- Do not build infrastructure that mature open source already provides.
- Do not present upstream benchmarks as ARMFast results.
- Do not claim compliance certification or "zero trace" before they are proven.

- Do not attempt to replace every RegTech platform; orchestrate them.
- Do not target every geography at once, or sell dozens of use cases before proving one.
- Do not build complexity ahead of customer validation.

25. Differentiation & Moat

The paper is direct about this, because a credible reader will be. ARMFast has **no proprietary technology moat today**: its components, including the Ruflo agent engine, are third-party open source that any competent team can also use. Differentiation and defensibility must therefore come from elsewhere, and must be built rather than claimed.

Moat source	Now	Assessment
Proprietary technology	None	Stack is third-party OSS incl. agent engine
ARM ecosystem apps + regulated data	Potential	Best candidate; requires live integrations
Sovereign operations (A100, 2-site, residency)	Emerging	Genuine early advantage; hard to replicate cheaply
Switching costs (identity/compliance)	Future	Follows from ecosystem integration + data
Distribution via ARM operators	Emerging	Real internal channel (ARMUP/ARMF)
Governance + compliance workflow depth	Potential	Buildable domain advantage in AML
Community / brand	None	Empty repo; brand-confused today

The honest formulation: if ARMFast disappeared tomorrow, ARM Technology Holding could rebuild the *stack* from open source in months; what it could not quickly rebuild is live regulated customers, integrated identity and compliance, audited sovereign operations, and accumulated AML-workflow depth. That is precisely where the moat must be formed — in the ecosystem, the regulated data, and the operations, not the technology.

26. Product Maturity & Evidence

This is the paper's central credibility table. It states, per capability, what is implemented, demonstrated, in production, and independently evidenced — today.

Capability	Implemented	Demonstrated	Production	Independent evidence
Agent identity (WSO2 Agent ID)	Partial	No	No	None
Agent governance lifecycle	Partial	No	No	None
Durable workflow (Temporal)	Yes (upstream)	Internal	No (as ARMFast)	Temporal itself
Document intelligence (PageIndex)	Yes (upstream)	Internal	No (as ARMFast)	VectifyAI benchmark
Vector memory (TurboVec)	Yes (upstream)	Internal	No (as ARMFast)	Upstream reports
Self-hosted / residency	Partial	Internal (AU)	No	None
Portable deployment	Specified	No	No	None
Security controls / assurance	Partial	No	No	None (assessment pending)
Open-source / public repo	No	No	No	Repo currently empty
FinTech Suite (AML triage)	Specified	No	No	None

Read plainly, the table says ARMFast is **early**: strong upstream components, a sound design, and no independent proof yet of the platform, its security, or a customer deployment. That is not a criticism of the strategy; it is the definition of the work ahead, itemised in Sections 28–29.

27. Risks & Limitations

- **Evidence deficit (critical):** no public code, reference customers, independent security assessment, or platform benchmarks.
- **Claim integrity (critical):** every headline number is upstream; presenting any as ARMFast's fails due diligence.
- **Architecture complexity (critical):** the specified stack is not operable by a small team; must be cut to the MVP Core.
- **No technology moat (high):** all components, including Ruflo, are free to competitors.
- **Sovereignty contradictions (high):** Ruflo's Claude-Code heritage and Aibrix's burst-to-cloud default must be resolved and documented.
- **Dependency & licensing exposure (medium):** ~50 upstream projects mean ~50 CVE/upgrade streams and licence obligations (GPL/MPL/AGPL-avoidance) requiring legal review.
- **Brand confusion (medium):** "ARMFast" collides with Arm Holdings plc in search and procurement; recommend consistent "ARMFast by ARM Technology Holding" descriptor and disambiguation copy on every asset (a strategic, not legal, recommendation).

28. Proof Agenda

The path forward is proof, not features. This is the itemised agenda — the artifacts that convert design and integration into evidence a CTO, CISO, and regulator will accept.

Proof area	Current evidence	Missing evidence	Validation method
Product	Design + integrations (internal)	Running MVP Core; reference architecture	Public reference deployment
Security	Design + genuine primitives	Assessment, SBOM, signed releases, red-team	Independent pen test + assessment
Performance	Upstream component benchmarks	ARMFast platform benchmark under real load	Own reproducible evaluation
Compliance	Control design	Objective mappings; tested DR drills	Third-party review + drill evidence
Customer	None (pre-release)	1 internal + 2 external references	Design-partner deployments
Ecosystem	Apps exist	Live theArmID / ARMreview integrations	Operational integration + shared data

29. 12-Month Roadmap

Window	Objective	KPI / success threshold	Evidence produced
0–90 days	Ship MVP Core; open repo + SDK; correct all claims to upstream attribution; publish benchmark methodology	Repo live; claim discipline enforced	Repo, SDK, API docs, corrected claims
0–90 days	Reference deployment + portable-deployment demo (defensible wording)	MVP runs end-to-end; demo recorded	Reference architecture + demo
90–180 days	Independent security assessment + pen test; SBOM; signed releases	Assessment passed; SBOM published	Security evidence pack
90–180 days	First design partner — ARM operator (ARMUP/ARMF), AML triage	1 live internal deployment	Internal case study + metrics
180–365 days	2–3 FinTech references (AU + GCC); live theArmID/ARMreview integration	2–3 signed; 1 external reference	Case studies, references
180–365 days	Compliance-objective mappings + ARMFast's own document-pipeline evaluation	Mappings published; eval reproducible	Compliance + performance evidence

30. Strategic Outlook

Tested from the six perspectives that decide a regulated infrastructure purchase, ARMFast's proposition holds where the buyer values sovereignty and governance and is honest about where evidence is still owed.

Perspective	Objection	Response	Remaining gap
CTO — why deploy?	"Show me the running platform."	Pre-integrated governed Core; saves 6–12 mo of assembly	Public reference deployment (Phase 1)
CISO — why trust?	"No assessment, no SBOM."	Self-hosted, owned keys, audited actions, SkillSpectre	Independent assessment (Phase 1–2)
CFO — why pay?	"Value vs DIY?"	Lower integration cost + regulatory risk; per-institution price	Measured ROI from design partner
Procurement — who supports?	"Pre-release, no SLA."	Enterprise Assurance tier; data/workflow export; escrow option	Tier + references to stand up
FinTech exec — what outcome?	"What does it solve?"	Faster, auditable AML investigations with full evidence	Design-partner metrics
Investor — where's the moat?	"Components are free."	Moat = ecosystem + regulated data + sovereign ops, to be built	Live integrations + switching costs

Investor logic, briefly: **why now** — sovereignty became a procurement gate in 2025–26; **why this market** — regulated finance has legal, non-discretionary demand; **why not hyperscalers** — they are structurally non-sovereign for this data; **why not open source alone** — assembly and governance are the unmet work; **what must become true** — proof, references, and ecosystem lock-in; **what could kill it** — failure to ship a simple Core, a hyperscaler sovereign-agent offering, or an inability to convert the ecosystem into switching costs.

Conclusion, Scorecard & Recommendation to the Board

ARMFast has chosen a real problem in a market moving toward it, with a clean product taxonomy and a concrete, demonstrable FinTech story. It also has no technology moat today, a set of headline numbers that belong to upstream projects, an architecture that must be simplified before it can ship, and a code base that is not yet public. Both halves are true, and the strategy that follows from holding both is not more features — it is proof, focus, and honest language.

Final strategic scorecard

Dimension	Rating	Basis
Product	Developing	Sound design; pre-release; must ship MVP Core
Market	Attractive	Sovereignty-as-procurement; regulated-finance demand
Technology	Adequate	Strong upstream components; no proprietary core
Differentiation	Emerging	Governed + sovereign + FinTech combination, unproven
Security	Developing	Good design; no independent assurance yet
Commercial model	Viable	Open-core + vertical Suite + managed/assurance
Distribution	Emerging	ARM operators as first customers
Moat	Potential	Ecosystem + regulated data + ops, to be built

Dimension	Rating	Basis
Overall	Promising	Real opportunity, conditional on execution & proof

Recommendation to the board

Should ARMFast proceed?

PROCEED, WITH CONDITIONS. Build a minimal ARMFast Core and one product — the FinTech Compliance Suite, AML alert triage and investigation first. Sell to regulated financial institutions and VASPs, starting with ARM ecosystem operators, in Australia, then the GCC. Prove, within twelve months: a running open Core, an independent security assessment, ARMFast’s own reproducible benchmark, a portable deployment with defensible claims, and one internal plus two external references. Stop doing everything else — the extra engines, the generic-platform ambition, the upstream benchmarks presented as ARMFast’s, and the "zero-trace" and "compliant" language. The moat is not in the technology, which anyone can assemble; it is in the ecosystem, the regulated data, and the sovereign operations — build there. The single risk that would invalidate this plan is failing to ship a simple, proven Core before a hyperscaler packages an equivalent sovereign-agent offering. On the evidence, the opportunity is real and the direction is right; the work that remains is the work of earning trust, which is exactly the product ARMFast intends to sell.

Appendices

The appendices are the reference pack behind the paper: the registers, matrices, and methodology a technical or commercial reviewer needs to trace any claim. They are deliberately compact and decision-oriented.

Appendix A — Master Claim Verification Register

Claim	Owner	Status	Allowed wording
16× index / 10M→4GB / 12–20% vs FAISS	TurboVec (RyanCodrai)	UPSTREAM verified	"Integrates TurboVec; ~16×; on Arm CPUs ~12–20% over a FAISS baseline"
98.7% FinanceBench	PageIndex / Mafin 2.5 (VectifyAI)	UPSTREAM (vendor SOTA)	"Uses PageIndex, which reports 98.7% (VectifyAI)"; not ARMFast's
100% 10-K at k=5	Proxy-Pointer RAG	UPSTREAM claimed	"Evaluates Proxy-Pointer RAG, which reports 100% at k=5"
14× TTFT / 90% compute	LMCache (H200)	UPSTREAM (specific HW)	"LMCache reports up to 14× TTFT on H200-class hardware"
40–85% cost / 2–10×	cascadeflow	UPSTREAM claimed	"cascadeflow reports 40–85% model-cost reduction in its own tests"
100+ agents / SONA	Ruflo (ruvnet)	UPSTREAM	"Built on Ruflo (MIT)"; not ARM-built
Post-quantum / zero-trust	ARMFast (design)	SPECIFIED	"Designed for MLDSA / zero-trust"; implementation unverified
Zero trace on host	ARMFast	UNVERIFIED	"No application data on host; residual OS metadata may remain"
Open source	ARMFast	CONTRADICTED	"Source-available / open-core (NetHSM-style)"
Compliance-ready	ARMFast	SPECIFIED	"Supports ISO 27001/42001, DORA, AML/KYC objectives"

Appendix B — V1 / V2 / V3 / HackMD Reconciliation

Topic	V1 / V2	HackMD scope	Final V3 position
Definition	Governed self-hosted agent middleware	Infra layer powering all ARM apps	Infra/control layer; Core + FinTech Suite
Agent engine	Rufio = ARM IP (moat candidate)	Ruflo = ruvnet/ruflo, MIT	UPSTREAM; not ARM IP (corrected)
98.7% FinanceBench	V2: "not credible"	PageIndex figure	UPSTREAM vendor SOTA; attribute (corrected)
Taxonomy	Blurred	ARMFast / ARMcloud / JoinMail	Adopt clean 3-layer taxonomy
Open source	Contradicted (empty repo)	NetHSM-style source-available	Source-available / open-core
Architecture	Composed OSS	~50 components, 3 workflow engines	Cut to MVP Core
Sovereignty	Deployment characteristic	Residency zones; A100 AU	Purchasing requirement; strong pillar

Topic	V1 / V2	HackMD scope	Final V3 position
Moat	None verifiable	Implied via ecosystem	No tech moat; ecosystem+data+ops only

Appendix C — Technology Provenance Matrix

Component	Origin	Licence	ARMFast contribution
Ruflo (agents)	ruvnet / Reuven Cohen	MIT	Integration + config
Temporal (workflow)	Temporal	MIT	Selection + governed wrap
Conductor / Prefect	Orkes / Prefect	Apache 2.0	Deferred in MVP
TurboVec (vector)	RyanCodrai / Google TurboQuant	MIT	Integration layer (closed)
PageIndex (RAG)	VectifyAI	MIT	Integration
MinerU / Hyper-Extract	opendatalab / others	Apache/MIT	Pipeline assembly
LMCache / cascadeflow / Aibrix / Exo	various OSS / Linux Fdn	Apache/MIT	Config; mostly deferred
Ollama / vLLM	Ollama / vLLM project	MIT/Apache	Model serving
WSO2 (IS/Agent ID/API/MI/GW)	WSO2	Apache 2.0	Integration
PostgreSQL / Patroni	PostgreSQL / Zalando	PostgreSQL/MIT	Ops + HA
OpenBao / WireGuard / RustFS	OpenBao / WireGuard / RustFS	MPL/GPL/Apache	Ops + config
konstruktoid / Auditd / AIDE / Wazuh	respective projects	MIT/GPL	Build-time hardening
Prometheus / Grafana / Loki	Prometheus / Grafana	Apache 2.0	Observability

Appendix D — Third-Party Licensing Matrix

Indicative only; not legal advice. Items flagged require legal review before commercial release.

Licence family	Examples	Consideration	Flag
MIT / Apache 2.0	Ruflo, Temporal, TurboVec, PageIndex, WSO2, MinerU	Permissive; attribution; patent grant (Apache)	Low
MPL 2.0	OpenBao	File-level copyleft; keep modifications open	Low–medium
GPL / GPLv2	WireGuard, Auditd, AIDE, Barman, Keepalived	Copyleft; distribution obligations	Review distribution model
AGPL	Windmill (excluded), some tools	Network copyleft; risky for SaaS	Avoid / already excluded
Llama licence	LLaMA models	Use restrictions / acceptable-use terms	Review; prefer permissive models
"Open-source" (unspecified)	RustFS, PageIndex tier	Confirm exact licence + production terms	Verify before adoption

Legal-review triggers

Confirm the NetHSM-style production-restriction model is enforceable; verify exact licences on components marked only "open-source"; confirm GPL distribution obligations against the portable-deployment model; and review model-licence acceptable-use terms. These are matters for qualified counsel; this paper draws no legal conclusions.

Appendix E — Security Control Matrix

Control	Technology	Purpose	Status
Identity / SSO	WSO2 Identity Server + SoloKeys	AuthN/AuthZ, passkeys	SPECIFIED
Agent identity	WSO2 Agent ID	Cryptographic agent principals	SPECIFIED
Secrets / KMS	OpenBao	Keys & secrets per region	VERIFIED primitive
Network	WireGuard, Traefik	Encrypted transport, gateway	VERIFIED primitive
Skill security	SkillSpectre	Pre-deployment agent-skill scan	SPECIFIED
Host hardening	konstruktoid (CIS)	Build-time baseline	SPECIFIED
Audit / integrity	Auditd + AIDE + Wazuh	Kernel audit, file integrity, SIEM	SPECIFIED
Observability	Prometheus/Grafana/Loki	Metrics, logs	SPECIFIED
DR / HA	Patroni, Keepalived, Velero, Barman	Two-site failover, backup	SPECIFIED

Appendix F — Compliance Mapping

Requirement	ARMFast capability	Evidence	Gap / customer share
ISO 27001 / 42001	Hardened base, RBAC, audit	Pending	Assessment; customer ISMS
NIST AI RMF / OWASP LLM	Agent identity, SkillSpectre	Pending	Red-team; customer governance
DORA	Two-site DR, RTO/RPO tiers	Pending	Tested drills; customer resilience
GDPR / Privacy Act / PDPL	Residency zones	Pending	Regional nodes; customer DPA
AUSTRAC / FATF	AML/KYC workflows (ARMreview)	Internal only	Reference deployment; AML programme
PCI DSS (if card data)	Segmentation, secrets, audit	Pending	Scope + assessment

Appendix G — Competitive Matrix

Capability	ARMFast	DIY OSS	Hyperscaler	RegTech
Self-hosted / sovereign	Yes (goal)	Yes	Limited	Varies
Agent-native + governed	Designed	Assemble	Improving	No
Durable workflow	Via Temporal	Yes	Managed	Partial
Document intelligence	Via PageIndex	Assemble	Managed	Domain
FinTech compliance depth	Suite (goal)	No	Services	Yes
Maturity today	Pre-release	Proven	Highest	Proven

Appendix H — Market-Sizing Methodology

Confidence is low and stated as such. TAM is anchored to the self-hostable share of independent agentic-AI, orchestration, and vector-tooling estimates (~USD 7–8.5B agentic in 2025, 40–46% CAGR; sovereign cloud ~USD 80B in 2026), treated as a band. SAM narrows to the self-hosted/sovereign + regulated-FinTech subset in target regions (AU, GCC). SOM is bottom-up: paying institutions × blended ACV × adoption, across conservative/base/aggressive scenarios (Section 22). ACV assumptions (USD 70k–190k) reflect per-institution self-hosted licence + support norms for comparable open-core infrastructure and are illustrative until replaced with pipeline data. CAC (USD 40k–80k), 6–12-month cycles, and 70–85% gross margin are planning assumptions, not measured figures. No figure in this paper should be read as a forecast.

Appendix I — Product Maturity Matrix

Full detail in Section 26. Roll-up: no capability is yet in production as ARMFast or independently evidenced; the strongest-implemented capabilities are upstream components (Temporal, PageIndex, TurboVec) used internally; identity, governance, security assurance, the public repo, and the FinTech Suite are specified or partial. Overall maturity: **pre-release** / **early**.

Appendix J — Technical Dependency Register

Dependency	Role	Criticality	Dependency risk
Ruflo	Agent orchestration	Critical	Single-maintainer heritage; Claude-Code lineage
Temporal	Durable workflow	Critical	Low; mature, MIT
PageIndex	Document RAG	High	Young project; verify production terms
TurboVec	Vector index	High	Young; single-maintainer
WSO2 suite	Identity/gateway	Critical	Vendor-led OSS; integration depth
PostgreSQL	System of record	Critical	Low
OpenBao	Secrets	Critical	Low–medium (fork maturity)
~50 total components	Full stack	—	~50 CVE/upgrade streams; needs SBOM + policy

Appendix K — Risk Register

Risk	Severity	Mitigation	Owner area
Evidence deficit	Critical	Ship MVP; assessment; references (Phase 1–2)	Eng / GTM
Claim integrity	Critical	Enforce claim register site-wide	Product / Marketing
Architecture complexity	Critical	Cut to MVP Core	Eng
No technology moat	High	Build ecosystem + data + ops moat	Strategy
Sovereignty contradictions	High	Disable burst-to-cloud; document model paths	Eng / Security
Licensing exposure	Medium	SBOM; legal review of GPL/model terms	Legal / Eng
Brand confusion	Medium	"ARMFast by ARM Technology Holding"; disambiguation	Marketing
Hyperscaler pre-empts	Medium–High	Speed to a proven, referenced beachhead	Leadership

Appendix L — Moat Formation Roadmap

Moat	Now	0–12 months	12–24 months
Ecosystem integration	Apps exist	Live theArmID/ARMreview integration	Shared identity/compliance data across apps
Regulated data / workflow depth	None external	First AML deployments	Accumulated AML case data & templates
Sovereign operations	A100 (AU)	AU + GCC managed deployments	Multi-region audited operations
Switching costs	None	Identity + workflow lock-in begins	High re-integration cost for customers
References / trust	None	1 internal + 2 external	Category credibility in AU/GCC finance

Appendix M — ARMFast Proof Agenda

Detailed in Section 28. Summary of the seven proofs ARMFast must produce, in priority order: (1) **product** — a running, open MVP Core with reference architecture; (2) **security** — independent assessment, SBOM, signed releases; (3) **performance** — ARMFast’s own reproducible platform benchmark (distinct from upstream numbers); (4) **compliance** — objective mappings and tested DR drills; (5) **customer** — one internal plus two external references; (6) **ecosystem** — live, operational integrations creating switching costs; (7) **commercial** — signed per-institution contracts with measured outcomes. The white paper’s central thesis is that delivering these proofs, not adding features, is what converts ARMFast from a credible design into a defensible business.

End of White Paper

ARMFast — Governed Agent Infrastructure for Regulated Finance · V3 · ARM Technology Holding · August 2026