



RIHUUM INTERCONTINENTAL LIMITED

CONTROLLED CONSOLIDATED MASTER BLUEPRINT EDITION

Master Corporate, Technology and Product Development Document

Including Rihuum Master Enterprises, the Rihuum Digital Ecosystem, Rihuum OS, Rihuum Intelligence Architecture, Rihuum Sentinel AI Cybersecurity Suite, RAHIS and the long-term commercialisation roadmap

Version 3.1 | 26 July 2026 | Controlled consolidated edition

RC 1476119 | Incorporated 6 March 2018

www.rihuum.com | www.rihuum.tech | www.rihuum.net

Registered locality: Abuja, Nigeria

info@rihuum.com | info@rihuum.tech | info@rihuum.net | rihuumconsult@gmail.com

Finance: finance@rihuum.com | Payments: payment@rihuum.com | Approval: account@rihuum.com
09162102777 | 08082407830 | 07031321663

CONFIDENTIAL - GOVERNANCE, EXECUTION AND INVESTMENT PLANNING

Document Control and Authority

Authority: This document is the controlled strategic and operating blueprint for Rihuum Intercontinental Limited. Business plans, product roadmaps, architecture decisions and departmental plans must align with it unless a documented board-approved exception is recorded.

Table 1. Controlled document record

Field	Controlled value
Legal entity	Rihuum Intercontinental Limited (RC 1476119)
Document	Master Corporate, Technology and Product Development Blueprint
Version / date	3.1 / 26 July 2026
Status	Executive-authorized controlled consolidated successor to v3.0; formal Board ratification must be recorded separately. It establishes the governed architecture and release candidates without claiming that pending providers, credentials, tests or production integrations are commissioned.
Business owner	Board of Directors and Managing Director/Chief Executive Officer
Technology owner	Chief Technology Officer / designated technology leader
Review cycle	At least annually and after material legal, product, security, funding or market change
Distribution	Controlled internal copy; approved extracts may be issued to investors, partners, staff and clients
Change summary	Version 3.1 consolidates the current Sites/D1 application runtime, Namecheap DNS/email boundary, RME 0.3 Configuration Centre, Sentinel AI staging candidate and RAHIS v8.3 controlled candidate. RETP is retained only as a superseded historical alias.

Approved corporate identity

Table 2. Identity and contact data to be used across documents and solutions

Element	Approved value
Official company name	Rihuum Intercontinental Limited
CAC registration number	RC 1476119
Date of incorporation	6 March 2018 (company-supplied and board-approved fact)
Email	Corporate: info@rihuum.com admin@rihuum.com Technology: info@rihuum.tech admin@rihuum.tech Operations: info@rihuum.net admin@rihuum.net Finance control: finance@rihuum.com payment@rihuum.com account@rihuum.com Continuity: rihuumconsult@gmail.com
Telephone	09162102777 08082407830 07031321663
Domains / registered locality	www.rihuum.com www.rihuum.tech www.rihuum.net Abuja, Nigeria
Attribution	Built and Developed by Rihuum Intercontinental Limited - www.rihuum.tech
Official logo	Only the board-approved gold Rihuum emblem supplied by the company

Evidence and claims discipline

- **Company facts:** Facts supplied and approved by the board are treated as company records; they should still be reconciled to the current CAC profile and statutory registers.
- **Recommendations:** Targets, structures, controls and timelines in this blueprint are management recommendations until adopted through budget, policy, contract or board resolution.
- **No implied certification:** Alignment to a framework or standard does not mean Rihuum is certified. Certification may be claimed only after an accredited assessment and current certificate.
- **Legal review:** The compliance section is an operating checklist, not legal or tax advice. Qualified Nigerian counsel, tax advisers and sector specialists must validate obligations before launch or market entry.
- **Open facts:** Rihuum Technology and Digital Hub is confirmed as CAC-registered, but its exact registration number/legal form remains unverified. Abuja, Nigeria is the confirmed registered-office locality; the exact street/public correspondence address and Google Maps Place ID remain verification items and are not guessed.

How to Use This Blueprint

Operating rule: Strategy becomes real only when each recommendation has an accountable owner, approved funding, measurable completion evidence and a review date.

Decision hierarchy

1. **Board direction:** Vision, risk appetite, annual priorities, capital allocation, major partnerships and entry into regulated or new markets.
2. **Executive portfolio:** Which products and services receive investment; which are incubated, partnered, paused or retired.
3. **Product and architecture governance:** Product outcomes, shared platform contracts, data rules, security requirements and technical exceptions.
4. **Delivery governance:** Backlogs, releases, quality gates, migration plans, service operations and measurable benefits.
5. **Continuous review:** Monthly operating review, quarterly portfolio review and annual strategy refresh, with immediate review after a material incident or legal change.

Five mandatory gates

Table 3. Gate model applied to every product, service and expansion

Gate	Question	Required evidence
Value	Does a defined customer problem justify investment?	Discovery evidence, customer segment, outcome metric, commercial hypothesis
Feasibility	Can Rihuum deliver and operate it responsibly?	Architecture, skills, vendor, cost and support assessment
Trust	Is it secure, private, lawful and governable?	Threat model, privacy assessment, controls, contracts and approvals
Readiness	Can it be deployed, supported and recovered?	Test evidence, runbook, monitoring, backup/restore and rollback rehearsal
Scale	Should it receive more capital and market exposure?	Adoption, retention, margin, service quality, risk and capacity data

Interpretation of Rihuum OS

Rihuum OS is defined in this blueprint as Rihuum's unified enterprise and industry operating experience and product family. Its initial product is not a replacement for Windows, macOS, Linux, Android or iOS. It is the secure digital operating layer through which Rihuum and its clients use RME-powered workflows, records, business modules, subscriptions, intelligence, support and integrations. This definition creates a commercially credible starting point while preserving future options.

Interpretation of Rihuum Master Enterprises

Rihuum Master Enterprises (RME) is Rihuum's shared multi-tenant enterprise core and product control plane. RME 0.3 Configuration Centre governs manual registration of public identifiers, provider references, environment settings, activation evidence and safe feature state. Secret credentials remain protected server-side and outside public records.

Contents

The page references below reflect this final rendered document.

1. Executive Summary.....	8
2. Company Overview.....	10
3. Vision, Mission, Values, and Strategic Objectives.....	12
4. Corporate and Departmental Structure.....	14
5. Brand and Domain Strategy.....	16
6. Products, Services, and Business Units.....	18
7. Technology Architecture.....	21
8. Software Development Framework.....	24
9. Product Roadmap.....	26
10. AI, Machine Learning, Data Science, and Automation Strategy.....	28
11. Cybersecurity and Data-Protection Framework.....	31
12. Hosting, Infrastructure, and Migration Strategy.....	33
13. Development, Testing, Staging, and Production Processes.....	35
14. Version Control and Release Management.....	37
15. Feature-Development Framework.....	39

Contents - continued

The page references below reflect this final rendered document.

16. Feature Updates and Upgrades.....	41
17. New Feature Releases.....	42
18. Software Versioning.....	43
19. Database and System Migrations.....	44
20. Backup, Rollback, Recovery, and Disaster-Management Procedures.....	46
21. Maintenance and Technical-Support Framework.....	48
22. Quality Assurance and Software-Testing Procedures.....	50
23. Documentation and Change-Management Processes.....	52
24. Emerging Technologies and Market Opportunities.....	54
25. Technology Research and Innovation Roadmap.....	56
26. Market Expansion and Commercialisation Strategy.....	57
27. Pricing, Licensing, Subscription, and Revenue Models.....	59
28. Client Onboarding and Deployment Procedures.....	61
29. Staff Recruitment, Training, and Performance Management.....	63
30. Risk Management and Business Continuity.....	65

Contents - continued

The page references below reflect this final rendered document.

31. Legal, Regulatory, and Compliance Requirements.....	67
32. Financial and Investment Planning.....	69
33. Marketing, Branding, and Customer-Acquisition Strategy.....	71
34. Key Performance Indicators and Reporting Framework.....	73
35. Implementation Phases, Timelines, and Milestones.....	75
36. Short-, Medium-, and Long-Term Growth Plans.....	77
37. RAHIS Hospitality Platform and Digital Ecosystem Expansion.....	79
38. Rihuum Sentinel AI Cybersecurity Suite and Integrated Defence Platform.....	91
Appendix A. First 90-Day Action Register.....	98
Appendix B. Governance and RACI Matrix.....	100
Appendix C. Architecture Principles and Decision Standards.....	101
Appendix D. Policy, Process, and Documentation Register.....	102
Appendix E. Source and Evidence Register.....	103
Appendix F. Glossary.....	104
Appendix G. Open Decisions and Verification Register.....	106
Appendix H. Nigeria and Africa Market and Portfolio Expansion.....	108
Appendix I. Corporate Communications, Email and Visual Media Register.....	112

SECTION 01 | Executive Summary

Strategic conclusion: Rihuum should operate as one technology-first company with a disciplined portfolio of connected business units, not as a collection of unrelated services. Rihuum Master Enterprises becomes the shared enterprise core that powers Rihuum OS and every authorised product; the three domains become distinct digital front doors; and Rihuum Intelligence Architecture governs every AI and Agentic AI capability.

Rihuum Intercontinental Limited has the breadth to serve enterprises, governments, SMEs, startups, education, hospitality, logistics, agriculture, healthcare, financial services, manufacturing and other sectors. Breadth is valuable only when it is supported by a common operating model. This blueprint therefore separates the company into market-facing business units while centralising brand, identity, security, data, product engineering, finance, people, legal, customer success and technology governance.

The recommended technical foundation is a portable modular monolith for the first production version of Rihuum Master Enterprises, with Rihuum OS and authorised products consuming its shared capabilities through explicit module, API and event contracts. This is the most practical architecture for the current Namecheap shared-hosting constraint because it minimises operational complexity while preserving boundaries, migrations and deployment contracts. Components should become independent services only when measured scale, isolation, compliance, availability or team ownership requires separation.

The six enterprise decisions

Table 4. Decisions that define the Rihuum foundation

Decision	Approved direction	Business result
One company, managed portfolio	All units share governance, platform services, data rules and commercial standards.	Lower duplication; a coherent client proposition.
Three-domain ecosystem	rihuum.com for corporate trust; rihuum.tech for products, AI and the Academy; rihuum.net for operations, support and infrastructure.	Clear journeys with one brand and shared analytics.
RME-powered Rihuum OS	Build RME as the shared multi-tenant enterprise core, then deliver Rihuum OS as the unified operating experience and product family above it.	One reusable foundation, faster products and recurring revenue.
Governed Agentic AI	Use RIA to control models, knowledge, tools, memory, approvals, evaluation and audit.	AI value without uncontrolled autonomy.
Portable delivery	Environment-based configuration, database migrations, storage adapters, documented APIs, automated tests, backup and rollback from day one.	Migration from shared hosting without rebuilding products.
Evidence-gated growth	Invest further only after value, trust, readiness, unit economics and capacity evidence.	Capital discipline and lower execution risk.

First 90-day mandate

1. **Govern:** Appoint accountable executive, product, security, privacy, finance and service owners; approve the decision and risk registers.
2. **Verify:** Reconcile CAC records, shareholding, registered office, tax status, trademarks, domain control, Academy registration and existing contracts.

3. **Control the portfolio:** Inventory every active website, repository, product, client deployment, vendor, dataset, credential, licence and commitment; pause unapproved new builds.
4. **Launch the digital front doors:** Establish the three-domain information architecture, common design system, consent controls, analytics and central content workflow.
5. **Establish engineering:** Create version-controlled repositories, development/staging/production separation, security scanning, test gates, release records and restore-tested backups.
6. **Prototype RME and Rihuum OS:** Deliver the RME identity, organisation/tenant, role, policy, audit and support foundation; validate it through one end-to-end Rihuum OS client workflow before broad module expansion.
7. **Commercialise one narrow offer:** Select an ideal customer segment, run a paid pilot, measure time-to-value, support effort, gross margin and adoption.

Definition of success

- Clients can understand what Rihuum does, obtain a proposal, onboard securely, receive support and expand their relationship through one coherent experience.
- Every production system has a named owner, repository, deployment record, data classification, security baseline, monitoring, backup, restoration test and lifecycle status.
- RME provides common enterprise capabilities once; Rihuum OS and every authorised product reuse them through governed contracts rather than rebuilding isolated foundations.
- AI systems have authorised purposes, approved data, least-privilege tools, human approval for material actions, evaluation evidence and complete audit trails.
- Revenue increasingly combines recurring subscriptions, licences and managed services with implementation, training, hardware and advisory income.
- Growth decisions are made from reconciled operational and financial data rather than activity alone.

SECTION 02 | Company Overview

Positioning: Rihuum Intercontinental Limited is a diversified, technology-first enterprise that designs, commercialises, deploys and operates secure digital products and technology-enabled services across industries.

Table 5. Corporate profile

Item	Current foundation
Legal name	Rihuum Intercontinental Limited
CAC number	RC 1476119
Incorporation	6 March 2018
Primary markets	Nigeria first; phased West African, African and selected international expansion
Corporate domains	rihuum.com, rihuum.tech and rihuum.net
Training academy	Rihuum Technology and Digital Hub - CAC-registered; separate registration number pending verified insertion
Strategic identity	Technology and digital transformation; software and AI; cybersecurity and infrastructure; skills; smart systems; research and commercialisation
Shared enterprise core	Rihuum Master Enterprises (RME) - multi-tenant enterprise core and product control plane
Flagship product family	Rihuum OS - unified enterprise and industry operating experience powered by RME

Business thesis

Rihuum will create value in three connected ways. First, it will build repeatable digital products that can be licensed or subscribed to. Second, it will implement, integrate and manage those products for clients. Third, it will develop the skills, research and partner ecosystem required to sustain delivery. Hospitality, smart security, telematics, networking and training remain important businesses, but they should be digitally enabled through the same commercial, data and service platform.

Priority customer groups

Table 6. Customer groups and initial value propositions

Customer group	High-value problems	Rihuum entry offer
SMEs and growth companies	Fragmented operations, weak records, inconsistent customer service and limited automation	Rihuum OS starter modules, managed website, CRM, billing and digital-skills support
Enterprises	Integration, security, data governance, service reliability and workforce capability	Enterprise deployment, integrations, cybersecurity, analytics and managed services
Government and public institutions	Citizen/service workflows, accountability, data protection, skills and infrastructure	Discovery and pilot programmes with procurement, hosting and data-sovereignty controls
Education and workforce programmes	Market-relevant skills, delivery platforms and measurable outcomes	Academy programmes, LMS, labs, assessments and employer partnerships

Customer group	High-value problems	Rihuum entry offer
Hospitality and property operators	Guest experience, bookings, operations, security and asset visibility	Hospitality modules, smart access, CCTV, networks, events and service automation
Logistics, mobility and field operations	Fleet visibility, safety, routing, maintenance and proof of service	Telematics, IoT integration, dashboards and operational workflows

Operating boundaries

- **Build:** where Rihuum owns differentiated workflows, reusable intellectual property or strategic data capability.
- **Buy:** for commodity functions such as email delivery, payment processing, payroll, commodity monitoring or conferencing when an accountable vendor is more efficient.
- **Partner:** where licences, market access, specialist expertise, hardware warranties or regulated capability are required.
- **Integrate:** through documented contracts so a vendor or hosting change does not force a product rewrite.
- **Decline:** work that cannot meet minimum margin, security, legal, support, ethical or strategic-fit requirements.

SECTION 03 | Vision, Mission, Values, and Strategic Objectives

Vision

Vision: To become one of Africa's most respected technology companies, recognised for secure, intelligent, scalable and commercially successful products and solutions that solve real business and societal problems.

Mission

Mission: To combine software engineering, responsible AI, digital skills, data, cybersecurity, infrastructure and industry knowledge to bridge gaps, improve organisations, create opportunities and deliver measurable, sustainable value.

Core values

Table 7. Values translated into observable behaviour

Value	Expected behaviour
Integrity	Represent capabilities, evidence, prices, risks and delivery status truthfully; protect entrusted information.
Customer value	Start with a defined problem and measure adoption, outcome, satisfaction and total cost.
Security and privacy	Design safe defaults, least privilege, data minimisation, traceability, recovery and responsible disclosure.
Engineering excellence	Use documented standards, reviews, tests, version control, observability and maintainable architecture.
Responsible intelligence	Use AI when it improves an outcome; keep humans accountable for material decisions and actions.
Learning and inclusion	Grow local capability, make products accessible and create pathways from training to meaningful work.
Ownership	Give every commitment an accountable owner and escalate early when evidence shows risk.
Sustainable innovation	Prefer durable value, reuse and lifecycle stewardship over novelty or ungoverned expansion.

Strategic objectives

Table 8. Strategic objectives and outcome evidence

Objective	2026-2027 outcome	Longer-term direction
Build the operating foundation	Controlled corporate records, policies, finance, CRM, repositories, environments and governance	Auditable management systems that scale across markets
Commercialise RME-powered Rihuum OS	Validated RME core, Rihuum OS thin slice and paid lighthouse deployments	Configurable platform with partner and module ecosystem
Make AI governable and useful	RIA control plane, evaluated assistants and approved low-risk agents	Sector-specific, auditable multi-agent solutions

Objective	2026-2027 outcome	Longer-term direction
Create recurring revenue	Subscriptions, support retainers and managed services added to project income	Majority of gross profit from repeatable products and contracted services
Build digital talent	Academy pathways linked to internal apprenticeships and employer needs	Recognised African workforce-development and certification partnerships
Earn trust	Security, privacy, quality, support and incident processes implemented and measured	Appropriate independent assurance and certifications when commercially justified
Expand deliberately	Nigeria reference clients and repeatable sector plays	Phased West African, African and selected global operations
Institutionalise innovation	Research backlog, experiments, evidence gates and IP register	Venture builder and commercialisation engine

Targets are intentionally outcome-based. Numeric targets must be set after the first 90-day baseline and annual budget are reconciled; unsupported numbers would create false precision.

SECTION 04 | Corporate and Departmental Structure

Organisation design: Use a lean matrix: market-facing business units own customers and commercial outcomes; shared enterprise functions own standards, scarce capability and common platforms; cross-functional product teams deliver end-to-end outcomes.

Governance and executive structure

- **Board of Directors:** Strategy, risk appetite, capital, statutory oversight, executive accountability and reserved decisions.
- **Managing Director/CEO:** Enterprise performance, portfolio priorities, culture, external relationships and execution of board direction.
- **Executive Leadership Team:** Technology, product, finance, operations, commercial, people, legal/compliance and customer-success decisions.
- **Company Secretary/Legal:** Statutory registers, filings, board governance, contracts, IP and regulator coordination.
- **Portfolio and Investment Committee:** Prioritisation, stage-gate funding, product retirement and partnership decisions.
- **Technology, Data and AI Council:** Architecture, security, privacy, AI governance, platform standards and material exceptions.

Departments and business units

Table 9. Target organisational structure

Group	Core accountability	Initial accountable lead
Strategy, PMO and Corporate Development	Strategy deployment, portfolio, partnerships, investors, research and performance reporting	CEO / Strategy lead
Product and Experience	Discovery, product management, UX, portfolio lifecycle and commercial packaging	Head of Product
Engineering, RME and Rihuum OS	Shared-core architecture, software, integrations, DevSecOps, reliability and technical documentation	CTO / Engineering lead
AI, Data and Automation	RIA, AI/ML, analytics, knowledge systems, evaluation and automation	AI/Data lead
Cybersecurity and Digital Trust	Security, privacy engineering, GRC, incident response and assurance	Security/Privacy lead
Commercial and Marketing	Market research, sales, pricing, proposals, brand, content, social and partner channels	Commercial lead
Customer Success and Service Operations	Onboarding, adoption, support, SLAs, renewals, managed services and knowledge base	Service lead
Rihuum Technology and Digital Hub	Curriculum, instructors, learning operations, labs, certifications and employer outcomes	Academy director
Smart Infrastructure and Security Solutions	CCTV, access control, networking, IoT, telematics, automation and field services	Solutions lead

Group	Core accountability	Initial accountable lead
Hospitality and Events Solutions	Hospitality technology, property operations, events and service design	Business-unit lead
Finance, Procurement and Administration	Accounting, treasury, budgeting, tax coordination, procurement, assets and controls	CFO/Finance lead
People and Culture	Workforce plan, recruitment, performance, learning, wellbeing and conduct	People lead

Lean staffing sequence

Table 10. Capability growth by stage

Stage	Core internal roles	Use specialists/partners for
Foundation	CEO, product/portfolio owner, senior full-stack engineer, commercial lead, finance/admin, client-support coordinator	Company secretarial, legal, tax, security testing, brand production and specialist infrastructure
Pilot	Add UX/product design, QA, implementation, data/AI engineering, Academy operations and field solutions	Penetration testing, cloud architecture, curriculum accreditation and regulated-sector advice
Scale	Dedicated security/privacy, platform/SRE, customer success, regional sales, HR and financial control	Independent assurance, international legal/tax and specialised hardware/vendor ecosystems
Enterprise	Product-line leaders, platform teams, research, partner engineering and regional operations	Market-entry advisers, accredited certification bodies and strategic delivery partners

Management cadence

- Weekly: delivery, service, cash/collections and critical risk review.
- Monthly: executive operating review covering financials, pipeline, products, clients, people, security and incidents.
- Quarterly: board and portfolio review; investment gates; risk appetite; commercial and technology roadmap.
- Annually: strategy, budget, workforce, control effectiveness, business-impact analysis and blueprint refresh.
- Event-driven: immediate review after a major incident, regulatory change, acquisition, new country, material contract or architecture exception.

SECTION 05 | Brand and Domain Strategy

Brand rule: The supplied gold Rihuum emblem is the only corporate logo. Business units and products use endorsed wordmarks and descriptors beneath it; they do not create competing corporate identities.

One brand. Three connected digital front doors.

Clear purpose, shared identity, unified data and client journey

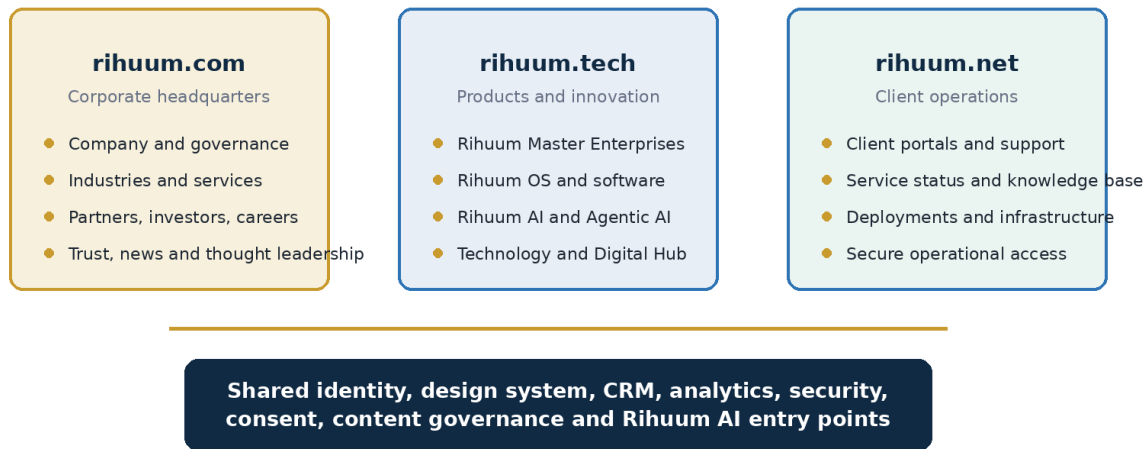


Figure 1. Rihuum three-domain ecosystem

Domain assignments

Table 11. Purpose and governance of each owned domain

Domain	Primary purpose	Key content and services	Governance
rihuum.com	Corporate headquarters and trust	Company, governance, industries, services, partnerships, investors, careers, newsroom and corporate blog	Corporate Communications + Legal; canonical corporate identity
rihuum.tech	Products, innovation and learning	Rihuum Master Enterprises, Rihuum OS, Rihuum AI, software, product documentation, developer resources, Academy, labs and technology blog	Product + Technology + Academy; primary lead generation for digital products
rihuum.net	Client operations and service delivery	Client portal, support, knowledge base, deployment access, service status, infrastructure and operational notices	Service Operations + Security; authenticated and high-trust workflows

Recommended service addresses

- www.rihuum.com:** Primary corporate site; root domain redirects consistently to www or the chosen canonical host.

- **app.rihuum.tech:** RME-powered Rihuum OS and product sign-in; use a separate application origin from marketing content.
- **academy.rihuum.tech:** Rihuum Technology and Digital Hub programmes, LMS and learner services.
- **docs.rihuum.tech:** Versioned product, API, security and developer documentation.
- **portal.rihuum.net:** Client projects, assets, subscriptions, tickets, reports and authorised operations.
- **status.rihuum.net:** Public service status hosted independently from the primary production stack when feasible.
- **support.rihuum.net:** Knowledge base and ticket entry with safe public/private separation.

Unified design and content system

- Create a versioned design system with official logo assets, colour tokens, typography, spacing, components, accessibility rules and usage examples.
- Display the legal company name and RC number on corporate and product sites, legal pages, invoices, proposals, contracts and official communications as applicable.
- Use one content-management workflow with role-based drafting, legal/technical review, scheduled publishing, revision history, ownership and review dates.
- Use canonical URLs, XML sitemaps, robots controls, structured metadata and redirect maps; avoid duplicating the same article across domains.
- Maintain distinct privacy notices, cookie/consent controls and terms for public sites, the Academy, client portals and each product where processing differs.
- Use one CRM identity and campaign taxonomy so a prospect can move across the ecosystem without fragmented records or excessive tracking.

Brand architecture

Use an endorsed architecture: 'Rihuum' is the master brand; 'Rihuum Master Enterprises', 'Rihuum OS', 'Rihuum AI', and 'Rihuum Technology and Digital Hub' are endorsed platform, product or business-unit names. Sector modules use descriptive names, for example 'Rihuum OS Hospitality' or 'Rihuum OS Fleet', until evidence justifies a standalone brand. All external names require legal, domain, trademark and customer-confusion checks before launch.

SECTION 06 | Products, Services, and Business Units

Portfolio principle: Products create repeatability; services create adoption; managed operations create durable outcomes; training creates capability. Each offer must have a clear owner, customer, margin model, support model and lifecycle status.

Table 12. Rihuum portfolio and commercial role

Portfolio area	Core offers	Primary revenue
Rihuum Master Enterprises	Shared enterprise core and product control plane: identity, tenancy, master records, workflow, commercial controls, integration, audit, support and lifecycle operations	Platform subscription/licence, implementation, managed hosting and internal shared-platform allocation
Rihuum OS	Unified enterprise and industry operating experience, modules, portals and analytics powered by RME	Subscription, tenant/module licence, implementation, support and managed hosting
Rihuum AI and Agentic AI	Knowledge assistants, governed agents, analytics, automation and model integration	Subscription/usage, implementation, evaluation, support and private deployment
Software and Digital Transformation	Custom applications, integrations, websites, process redesign and managed product teams	Projects, retainers, licences and support
Cybersecurity and Digital Trust	Assessments, secure architecture, privacy, awareness, monitoring coordination and incident readiness	Assessment, managed service, training and retainers
Cloud, Infrastructure and Networking	Hosting, migration, networks, backup, monitoring and operations	Projects, hardware margin, managed service and support
Smart Security, IoT and Telematics	CCTV, access control, sensors, fleet/asset visibility and automation	Hardware, installation, subscription, maintenance and analytics
Technology and Digital Hub	Courses, bootcamps, enterprise training, labs, apprenticeships and workforce programmes	Tuition, corporate cohorts, grants, sponsorship and platform licences
Hospitality and Events	Hospitality technology, guest/service workflows, property systems, event delivery and smart facilities	Projects, subscriptions, operations fees and vendor margin
Research, Analytics and BI	Market/operational research, dashboards, data engineering, forecasting and decision support	Projects, data products, subscriptions and advisory
Venture Builder and Innovation Lab	Discovery, prototypes, incubation, IP commercialisation and partnerships	Equity/options, royalties, licences, programme fees and co-investment

Product-platform hierarchy

- Rihuum Master Enterprises:** The shared enterprise core and product control plane. All authorised Rihuum products consume its identity, tenancy, master-record, workflow, commercial, audit, support, integration and lifecycle contracts.
- Rihuum OS:** The unified enterprise and industry operating experience and product family built on RME.

3. **Rihuum Intelligence Architecture:** The governed intelligence layer that uses RME identity, data, policy, approvals and audit; it never bypasses them.
4. **Products and sector modules:** Academy, hospitality, smart operations, CRM/ERP and future solutions reuse RME services and RIA controls rather than create isolated foundations.

RME-powered Rihuum OS product family

- **RME Core:** Identity, organisations/tenants, roles and policies, master records, workflow, notifications, audit, billing, subscription/licensing, entitlements, support, product registry and configuration.
- **Rihuum OS shell:** Responsive navigation, workspaces, dashboards, search, command experience and module composition over RME capabilities.
- **Business modules:** CRM, sales, projects, inventory/procurement, HRIS, finance interfaces, service desk and reporting.
- **Learning module:** Programmes, enrolment, content, cohorts, assessments, credentials, instructor operations and employer outcomes.
- **Hospitality module:** Bookings/inquiries, guest profile, service requests, events, facilities, maintenance, access and management reporting.
- **Smart operations module:** Devices, sites, assets, telemetry, alerts, maintenance, evidence and field-service workflows.
- **RIA intelligence layer:** Knowledge, assistants, governed agents, analytics, automation, evaluation and audit across authorised modules.

Nigeria and Africa portfolio expansion

The v2.3 controlled reproduction defines eight shared application suites, 31 named industry directions plus a custom-sector route, 16 platform/product directions and 14 service lines. These are portfolio architecture and discovery scopes—not claims of general availability. Investment follows customer evidence, specialist validation, regulatory review, delivery capacity and the existing lifecycle gates.

Portfolio lifecycle

Table 13. Required lifecycle states

State	Meaning	Allowed commitment
Explore	Problem and market research; no product commitment	Time-boxed discovery only
Incubate	Prototype with named hypothesis, owner and budget	Controlled users and non-production data
Pilot	Operational trial with support, controls and success measures	Limited contract and explicit pilot terms
General availability	Supported, documented, priced and production-ready	Standard commercial contracts and SLAs
Maintain	Stable product with controlled enhancements	Renewals, patches and planned upgrades
Sunset	End-of-sale/end-of-support plan with migration path	No new commitments outside approved exception

CYBERSECURITY PRODUCT INTEGRATION: Section 38 establishes Rihuum Sentinel AI as the shared cybersecurity control plane consuming RME identity, licensing and audit plus RIA-governed intelligence contracts. All future Rihuum products register security integrations through these contracts rather than create isolated silos.

PRODUCT PORTFOLIO DECISION: The Rihuum Cybersecurity Suite is an official RME/Rihuum OS product family. Sentinel AI is the central platform; 40 defensive modules are separately licensable and may be configured into SME, Enterprise, Hospitality, Academy and Managed Detection and Response editions.

SECTION 07 | Technology Architecture

Architecture choice: Start Rihuum Master Enterprises as a well-structured modular monolith with strict internal and external contracts. Rihuum OS and every authorised product consume those shared contracts. Do not adopt microservices as a prestige decision; extract a service only when independent scale, security isolation, availability, data ownership or team autonomy is demonstrably required.

Rihuum OS and RME - Target Logical Architecture

RME powers the operating experience, products and governed intelligence

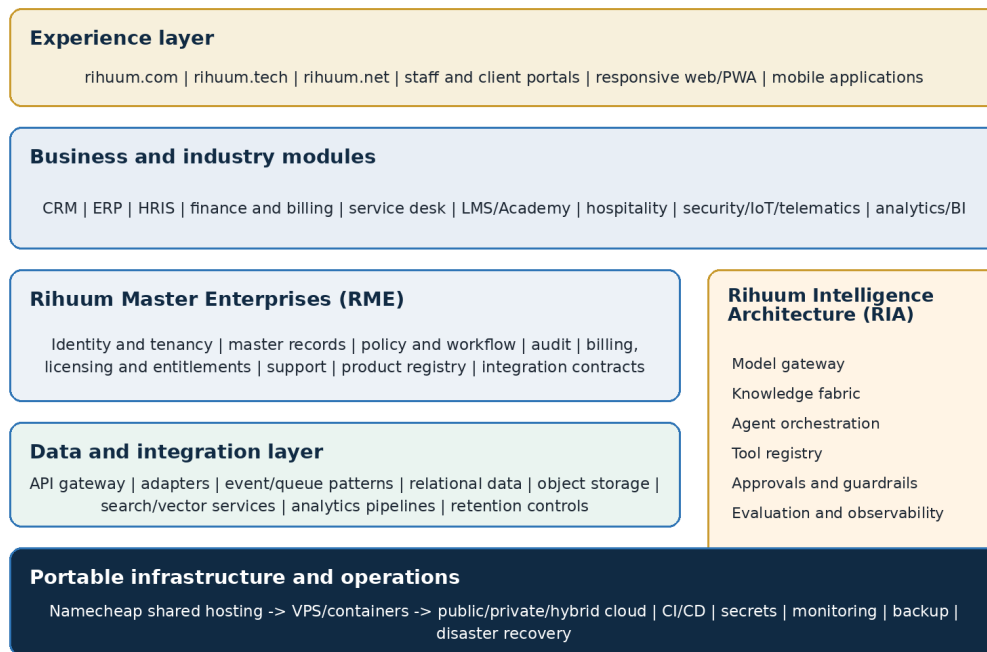


Figure 2. RME-powered Rihuum OS target logical architecture

RME platform contracts

Table 14. Shared enterprise contracts required across every product

Capability	Shared contract	Mandatory rule
Identity and tenancy	Users, organisations, roles, policy, sessions, SSO and delegated administration	Every request and record resolves an authenticated actor, tenant, purpose and authority.
Master records	Customers, people, sites, assets, products, catalogues and stable identifiers	A product references governed records; it does not create incompatible duplicates without an approved mapping.
Workflow and events	States, tasks, approvals, notifications, jobs and domain events	Effects are idempotent, traceable and safe to retry or compensate.

Capability	Shared contract	Mandatory rule
Commercial controls	Plans, prices, subscriptions, licences, entitlements, usage and invoices	Access follows approved entitlement and contract state; finance remains reconcilable.
Audit and support	Immutable audit events, consent/evidence, tickets, incidents and service history	Material user, system and AI actions are attributable and reviewable.
Integration	Versioned APIs, webhooks, adapters, schemas and event catalogue	No direct database coupling between products or unmanaged third-party credentials.
Product lifecycle	Product/module registry, configuration, feature flags, release and compatibility records	Every deployed module declares owner, version, dependencies, support state and migration path.

Architecture principles

- **Secure and private by design:** Threat modelling, least privilege, safe defaults, minimised data, encrypted transport, audited actions and tested recovery.
- **Modular before distributed:** Clear bounded modules, dependency direction and interfaces inside one deployable unit before service extraction.
- **API and event ready:** Documented interfaces and stable identifiers; asynchronous patterns only where they improve reliability or isolation.
- **Tenant aware:** RME-enforced organisation-scoped identity, authorisation, data access, configuration, billing, audit and exports from the first schema.
- **Portable:** Configuration outside code; storage, email, payment, AI and hosting adapters; repeatable builds and migrations.
- **Observable:** Structured logs, metrics, traces where feasible, audit records, health checks and service-level indicators.
- **Accessible and responsive:** Mobile-first responsive experiences, keyboard support, semantic structure, readable content and tested assistive-technology paths.
- **Replaceable intelligence:** Models and providers sit behind an approved gateway; business rules and source data are not trapped in prompts.

Initial deployable architecture

Table 15. Foundation components and migration contracts

Capability	Shared-hosting implementation	Migration-ready contract
Web/application	Server-rendered, responsive PHP application using the hosting plan's supported runtime; static assets via CDN where available	Container-ready build, stateless request handling and environment configuration
Database	Separate MySQL/MariaDB databases for staging and production	Versioned migrations, portable SQL patterns, exports and data-access layer
Jobs	Cron-driven database job queue with idempotent workers	Queue interface that can move to Redis or managed messaging
Files	Protected local storage outside public paths; controlled downloads	Storage adapter supporting S3-compatible object storage and lifecycle rules

Capability	Shared-hosting implementation	Migration-ready contract
Email/SMS	Approved external providers through adapters	Provider-neutral notification service, templates and delivery logs
Payments	Hosted checkout/API from licensed payment service providers	Payment adapter, webhook verification, reconciliation and no storage of prohibited card data
AI	External model services through RIA gateway using RME identity, tenancy, data and approval context; no direct model calls from business modules	Multi-provider routing, private models later, policy/evaluation layer and RME controls retained
Monitoring	External uptime checks plus structured application/error/audit logs	Central telemetry and alert routing on VPS/cloud

Multi-tenancy and data isolation

The recommended first model is logical multi-tenancy with a tenant identifier enforced in every tenant-owned record, request context, query policy, cache key, file path, job and audit event. High-risk or enterprise clients may require a dedicated database, deployment or infrastructure account. That option must be supported through configuration and deployment automation, not a fork of the product code.

Architecture governance

Record consequential decisions and alternatives in Architecture Decision Records (ADRs) with an owner and review trigger. Maintain current context, module, data-flow, threat and deployment diagrams. Govern approved technology, dependency, integration and data patterns through time-bounded exceptions. Review at discovery, pre-build, pre-production and after material incidents or scale changes.

SECTION 08 | Software Development Framework

Delivery model: Use product discovery to choose the right problem, iterative delivery to reduce risk, and DevSecOps controls to make every release reproducible, testable, secure and recoverable.

Table 16. Product and software lifecycle

Stage	Core activities	Exit evidence
Discover	Customer interviews, process/data mapping, alternatives, risk and commercial hypothesis	Problem statement, segment, outcome metric and decision to stop or continue
Define	PRD, journey, scope, acceptance criteria, architecture, threat/privacy review and support model	Approved thin slice, owner, plan, controls and budget
Design	UX prototype, data/API contracts, test strategy, migration and observability	Reviewed design and testable acceptance criteria
Build	Small changes, peer review, automated checks, documentation and feature flags	Merged code with traceability and clean quality gates
Verify	Functional, integration, security, accessibility, performance, migration and recovery tests	Test evidence, accepted residual risk and release candidate
Release	Approval, backup, deployment, smoke test, monitoring, communications and rollback readiness	Signed release record and stable production health
Learn	Adoption, outcomes, support, defects, cost and customer feedback	Decision to iterate, scale, maintain or retire

Definition of Ready

- A named customer/user and problem are documented.
- The outcome metric, scope and non-goals are explicit.
- Acceptance criteria are testable; dependencies and data are understood.
- Security, privacy, legal, accessibility, support and migration impacts have been screened.
- Design and architecture are proportionate to risk; owner and capacity are available.

Definition of Done

- Code is reviewed, version-controlled and linked to the requirement and decision record.
- Automated and manual tests pass; critical/high vulnerabilities are resolved or formally accepted by authorised risk owners.
- Documentation, runbooks, release notes, migrations, monitoring and support knowledge are current.
- Deployment and rollback are tested at the appropriate level; data/AI evaluation evidence is retained.
- The feature is released safely, measured in production and assigned a post-release review date.

Planning and workflow

Use a prioritised product backlog with short planning horizons. Product teams may use Scrum or Kanban according to work type, but must maintain flow limits, explicit priorities, visible blockers and a release forecast. Urgent work

must not silently bypass controls: an emergency path records the reason, approver, tests performed, rollback plan and required follow-up.

Engineering health measures

- Lead time from approved change to production and deployment frequency.
- Change failure rate, rollback rate and time to restore service.
- Escaped defects, vulnerability age, test reliability and dependency freshness.
- Build/release success, review time, documentation currency and operational toil.
- Product adoption and outcome measures; delivery speed without customer value is not success.

SECTION 09 | Product Roadmap

Roadmap rule: The roadmap is a sequence of validated capabilities and business outcomes, not a promise to build every listed feature. Quarterly portfolio review can re-order, pause or retire work as evidence changes.

Execution roadmap and gated scale



No phase advances without evidence: product value, security, operability, commercial readiness and funding capacity.

Figure 3. Phased execution roadmap

RME and Rihuum OS capability roadmap

Table 17. RME and Rihuum OS releases and outcome gates

Horizon	Minimum capability	Gate to advance
Foundation - 0 to 90 days	RME identity, organisations/tenants, roles, policy, audit, configuration, support, product registry, platform contracts and secure environments; Rihuum OS shell	End-to-end demonstrator; threat model; restore test; named pilot
Pilot - months 4 to 6	RME workflow, notifications, subscriptions/licensing and reporting exposed through a Rihuum OS CRM/client-portal thin slice	Paid pilot; adoption; contract compatibility; support and migration evidence
Commercial - months 7 to 12	Billing integration, service desk, Academy/LMS or one priority sector module, self-service onboarding and operations dashboard	Repeatable deployment; support capacity; acceptable unit economics
Scale - months 13 to 24	API catalogue, integration adapters, advanced analytics, additional sector modules, regionalisation and stronger isolation options	Multiple reference clients; cloud migration triggers met; partner readiness
Platform - months 25 to 36	RME extension framework, partner modules, marketplace controls, private/enterprise deployment and advanced RIA services	Governed ecosystem, stable contracts, assurance and sustainable partner economics

Portfolio sequence

1. Stabilise corporate identity, domains, sales/service workflows and engineering controls.

2. Build RME Core first, then deliver a Rihuum OS thin slice and use Rihuum internally as the first operational client.
3. Select one external lighthouse workflow with a defined buyer, measurable pain and short implementation path.
4. Commercialise the Academy platform and one smart-operations or hospitality module only after core reuse is proven.
5. Add Agentic AI first to bounded knowledge, triage and drafting tasks; expand tool authority only after evaluation and approval evidence.
6. Create partner/marketplace capability only after API stability, tenant isolation, support processes and commercial governance are mature.

Roadmap dependencies

- **Legal and identity:** Verified corporate records, IP assignments, client terms, privacy documents and Academy registration details.
- **Platform:** RME identity, tenant, master-record, audit, notification, commercial and lifecycle contracts before multiple modules.
- **Operations:** CRM, finance, support, asset and knowledge records before rapid acquisition.
- **Trust:** Security baseline, privacy governance, incident response and restore-tested backup before production data.
- **Commercial:** Pricing research, unit economics, implementation playbooks, partner terms and customer-success ownership.
- **People:** Senior product/engineering leadership, QA, implementation and service capacity; Academy used as a controlled talent pipeline.

SENTINEL AI POSITION: Rihuum Sentinel AI is the cybersecurity implementation of governed RIA. It may classify, correlate, explain and prepare bounded response actions; it cannot expand scope, alter evidence, accept risk or perform irreversible autonomous actions.

SECTION 10 | AI, Machine Learning, Data Science, and Automation Strategy

AI policy: Rihuum will use AI only for an authorised purpose with measurable value, approved data, proportionate human oversight, constrained tools, evaluation evidence, monitoring and a safe way to stop or reverse actions.

Rihuum Intelligence Architecture (RIA)

RIA is the cross-product control plane for artificial intelligence. It integrates through RME and must use RME identity, tenancy, master data, policies, entitlements, tool/action permissions, approvals and audit. Business modules must not connect independently to models, give agents unrestricted credentials or permit RIA to bypass RME controls. RIA separates business intent from model/provider choice and provides common controls for model routing, knowledge retrieval, prompt/instruction management, tools, memory, approvals, evaluation, audit and cost.

Table 18. RIA components and minimum controls

Component	Purpose	Minimum control
Model gateway	Route approved requests across models/providers	Allowlist, purpose tags, data rules, rate/cost limits, logging and failover
Knowledge fabric	Retrieve governed enterprise knowledge	Source ownership, access filtering, version/date, citation, retention and removal workflow
Agent orchestrator	Plan and execute bounded workflows	Explicit goal, step/time/cost limits, approved tools, state control and termination
Tool registry	Expose business actions to agents	Schema validation, least privilege, environment scope, approval class and audit
Memory service	Retain authorised context	Purpose, tenant isolation, poisoning controls, expiration, correction and deletion
Policy and approval	Enforce human and system controls	Risk tier, separation of duties, transaction thresholds and deny-by-default
Evaluation service	Measure quality, safety and task outcomes	Versioned datasets, test suites, regression thresholds and sign-off
Observability	Trace decisions, cost, errors and actions	Prompt/model/tool versions, source links, latency, spend, incidents and user feedback

Agent autonomy levels

Table 19. Authority model for Rihuum Agentic AI

Level	Permitted behaviour	Typical control
0 - Inform	Search, summarise, explain and answer without changing a system	Grounded sources, access controls, citations and feedback
1 - Draft	Prepare content, plans, tickets or transactions for a person	Human review before any external or system effect
2 - Recommend	Compare options and recommend a decision	Named accountable decision-maker; rationale and evidence retained

Level	Permitted behaviour	Typical control
3 - Execute with approval	Take a bounded action after explicit approval	Least-privilege tool, strong confirmation, limits, idempotency and audit
4 - Execute within policy	Perform repetitive low-risk actions inside approved rules	Continuous monitoring, exception queues, kill switch and periodic review
5 - High autonomy	Adapt plans across multiple tools and agents	Not a default Rihuum production mode; requires executive risk approval and specialised assurance

Priority AI use cases

- **Internal knowledge:** Policy, product, proposal and support retrieval with source citations and role-based access.
- **Customer service:** Triage, suggested responses, knowledge retrieval, sentiment and routing; humans retain ownership of disputes and material commitments.
- **Sales and delivery:** Discovery summaries, proposal drafts, requirements traceability, project risk and meeting actions.
- **Academy:** Tutor support, adaptive practice, content assistance and assessment analytics with academic-integrity and learner-safety controls.
- **Operations:** Invoice/document extraction, reconciliation suggestions, scheduling, exception detection and management summaries.
- **Smart systems:** Computer-vision or telemetry alerts where lawful and accurate enough, with human verification before consequential action.
- **Analytics:** Forecasting, segmentation, anomaly detection and decision support using governed datasets and reproducible methods.

AI product lifecycle

1. Define the user, purpose, prohibited use, decision/action impact and measurable baseline.
2. Classify data, legal basis, rights, vendor use, cross-border transfer and retention; complete a DPIA where risk warrants it.
3. Choose the simplest effective technique: rules, workflow, analytics, conventional ML, generative AI or an agent.
4. Threat-model prompts, knowledge, memory, identity, tools, inter-agent communication, supply chain and human trust.
5. Create representative evaluation datasets and thresholds for task quality, grounding, safety, bias, privacy, security, latency and cost.
6. Pilot with bounded users and authority; red-team and test failure handling, approvals, logging, rollback and kill switch.
7. Approve release, monitor production drift/incidents and re-evaluate after model, prompt, knowledge, tool, policy or user changes.

AI governance and prohibited patterns

- No agent receives administrator credentials, unrestricted network access or a broad shared service account.
- No unreviewed AI output creates a legal commitment, changes payroll/financial records, makes a high-impact employment/credit/health decision, or controls physical access/safety.
- No client, employee or learner data is used to train a model without documented authority, purpose, contract and rights controls.
- No hidden AI interaction: users are informed when they are interacting with AI and how to reach a person for material matters.
- No claim that an AI system is accurate, autonomous, secure or compliant without documented scope and current evaluation evidence.

Governance references include NIST AI RMF and the Generative AI Profile, ISO/IEC 42001:2023, and current OWASP Agentic AI guidance. See Appendix E.

UNIFIED CYBERSECURITY PRODUCT FAMILY: Section 38 converts this enterprise framework into a commercial, separately licensable suite with Sentinel AI as its central platform. The framework remains the corporate minimum; the suite provides governed implementation workflows and evidence.

SECTION 11 | Cybersecurity and Data-Protection Framework

Trust objective: Rihuum must make product and client security an executive-owned quality outcome. Security features essential to safe operation are baseline capabilities, not optional decoration.

Cybersecurity management model

Table 20. NIST CSF 2.0 functions applied at Rihuum

Function	Rihuum implementation	Example evidence
Govern	Risk appetite, policies, roles, supply-chain oversight, legal mapping and board reporting	Risk register, control owners, exceptions and quarterly dashboard
Identify	Assets, data, systems, dependencies, threats, business impact and vulnerabilities	Inventories, data maps, classifications, BIA and threat models
Protect	Identity, secure configuration, encryption, training, backups, application security and data controls	MFA, access reviews, baselines, test results and protected backups
Detect	Logs, monitoring, alerting, anomaly detection and reporting channels	Coverage map, alert tests, vulnerability findings and security contact
Respond	Triage, containment, communications, legal/privacy assessment and lessons	Incident plan, contact tree, exercise and incident records
Recover	Restoration, failover, customer communication and improvement	RPO/RTO, restore tests, DR exercise and post-incident actions

Minimum technical baseline

- **Identity:** Unique accounts, MFA for privileged/remote access, least privilege, role separation, joiner-mover-leaver workflow and periodic reviews.
- **Secrets:** No credentials in source code, tickets or shared documents; use environment secret stores, rotation and scoped service identities.
- **Application security:** Threat modelling, peer review, dependency/SAST/secret scanning, OWASP ASVS-based requirements, secure session/authentication and tested input/output controls.
- **Data security:** Classification, purpose limitation, encryption in transit, protected storage, tenant isolation, export controls, retention and secure deletion.
- **Infrastructure:** Hardened configuration, patching, controlled administration, web application firewall where appropriate, egress awareness and independent status monitoring.
- **Supply chain:** Approved dependencies/vendors, lockfiles, provenance, licence review, vulnerability monitoring, SBOM capability and integrity checks for releases.
- **Resilience:** Tested backups, immutable/offline copy where feasible, deployment rollback, documented restoration and independent contact/status capability.
- **Vulnerability handling:** Public security contact, responsible disclosure process, severity/ownership, remediation targets and customer advisories when required.

Data-protection programme

Table 21. Privacy-by-design operating controls

Control	Required practice
Records of processing	Identify controller/processor roles, purposes, data categories, subjects, recipients, locations, vendors, retention and security.
Lawful and fair processing	Document the applicable lawful basis and provide clear notices; obtain valid consent only where consent is the correct basis.
Data minimisation	Collect only what is needed, make optional fields clear, avoid open-ended collection and review old fields/data.
Rights handling	Authenticated request intake, search/export/correction/deletion workflow, decision record and statutory timeline tracking.
DPIA	Assess high-risk processing before launch, especially biometrics, CCTV/computer vision, monitoring, children/learners, profiling and consequential AI.
Processors	Due diligence, data-processing terms, confidentiality, security, subprocessors, location, assistance, breach and deletion/return obligations.
International transfers	Map transfers and use lawful transfer mechanisms and risk assessment appropriate to the destination and contract.
Breach response	Detect, contain, assess risk, preserve evidence, involve privacy/legal leadership and notify affected parties/regulators when required.

Security assurance roadmap

Begin with an internal control baseline mapped to NIST CSF 2.0 and OWASP ASVS, then build an information security management system aligned to ISO/IEC 27001:2022. Add privacy management alignment to ISO/IEC 27701:2025, AI management alignment to ISO/IEC 42001:2023 and business-continuity alignment to ISO 22301:2019 as scope and customer demand justify. Do not claim certification until an accredited body issues a valid certificate for a defined scope.

SENTINEL PLACEMENT RULE: the portal, licensing, governance, incidents, evidence and safe public checks may begin on compatible shared hosting; local, continuous or high-volume security workloads require customer-controlled collectors, VPS workers or approved managed providers.

SECTION 12 | Hosting, Infrastructure, and Migration Strategy

Current hosting decision: The public Rihuum Digital Ecosystem uses OpenAI Sites for application delivery and D1 for controlled application data. Namecheap remains the registrar, authoritative DNS and domain-email provider. Sentinel AI's PHP/MySQL package is a separate engineering-alpha staging candidate. Namecheap shared hosting may support bounded low-risk components, but not heavy AI, long-running agents, streaming, safety-critical workloads or regulated high-availability services.

Media and domain rule: Optimised silent cinematic loops may be served by the current Sites/CDN delivery path with poster images, metadata-only preload, pause controls and reduced-motion fallbacks. Namecheap DNS changes must preserve valid mail records. Bare and www hostnames must follow the approved canonical/redirect register; no redirect or certificate state is assumed complete without live verification.

Phase 1 hosting pattern

- Separate each domain, staging site and production application with distinct document roots, databases, credentials and deployment records.
- Keep application configuration and secrets outside the repository; block direct web access to private storage, logs, backups and configuration.
- Build and test release artefacts in CI; deploy a known artefact rather than editing production files through the hosting control panel.
- Use a hosted CDN/DNS/WAF service where appropriate, external uptime monitoring, licensed payment providers, external transactional email and a separately reachable status page.
- Use cron for bounded jobs and a database queue; enforce idempotency, timeouts, retries and a dead-letter/failed-job review.
- Encrypt backups before copying them to a separate provider/account; perform and record restoration tests.

Workload placement

Table 22. Shared-hosting suitability

Workload	Shared hosting position	Required alternative/trigger
Public corporate/product sites	Suitable when hardened, cached and monitored	Move for availability, traffic, security or deployment-control needs
Early Rihuum OS pilot	Conditionally suitable for low-risk tenants and bounded load	Move before enterprise/high-risk data or sustained background processing
Client portals	Only after isolation, secure sessions, monitoring, backup and contractual fit are verified	Dedicated VPS/cloud for stronger isolation or SLA
AI model inference	Use external approved AI services through RIA; do not host heavy models	GPU/cloud/private inference when economics, privacy and scale justify
Autonomous/long-running agents	Not suitable	Controlled worker infrastructure with queue, sandbox, observability and kill switch

Workload	Shared hosting position	Required alternative/trigger
Video/CCTV storage and analytics	Not suitable for operational scale	Edge/NVR plus secure object storage or specialist platform
Telemetry ingestion	Only small pilots	VPS/cloud message ingestion, time-series storage and device security

Migration triggers

Table 23. Evidence that triggers infrastructure migration

Trigger class	Example signal	Response
Reliability	Resource throttling, recurring latency, queue backlog, missed jobs or inability to meet recovery/availability objectives	Move affected application to managed VPS/container/cloud
Security/privacy	Enterprise isolation, log retention, encryption, network control, residency or vendor-assurance requirement	Dedicated environment and stronger control plane
Scale	Sustained users, storage, telemetry, AI inference or integration volume beyond plan constraints	Capacity design, load test and staged cutover
Operations	Need for workers, containers, Redis, private networks, blue/green deployment or full observability	Platform migration with automated infrastructure
Commercial	Client SLA, procurement, on-premise/private cloud, contractual audit or regional deployment	Approved enterprise deployment pattern
Economics	Managed migration lowers unit cost or risk at forecast demand	Business case with total cost and exit plan

Migration method

1. Inventory code, data, files, domains, certificates, jobs, integrations, secrets, logs, backups and operational dependencies.
2. Build the target environment from documented configuration; rehearse deployment, migration, monitoring, security and restore.
3. Run compatible data migrations and synchronisation; validate counts, checksums, permissions and critical business journeys.
4. Lower DNS TTL in advance, take a final protected backup, freeze writes if needed and execute the approved cutover runbook.
5. Smoke-test, monitor and communicate; keep the rollback window and old environment protected until acceptance criteria are met.
6. Remove obsolete access and data safely, update diagrams/runbooks/contracts and complete a lessons review.

SECTION 13 | Development, Testing, Staging, and Production Processes

Environment rule: Code moves forward through controlled environments; production data does not move backward into development. Each environment has a distinct purpose, identity, data rule and access boundary.

Table 24. Environment model

Environment	Purpose	Data and access	Deployment
Local/developer	Fast coding, unit tests and isolated experiments	Synthetic fixtures; developer-only secrets; no production credentials	Developer tooling and reproducible setup
Integration	Combined modules, APIs and automated workflows	Synthetic or approved anonymised test data; team/service access	Automatic from accepted changes
Test/QA	Functional, regression, security, accessibility and performance testing	Controlled test identities/data; QA and authorised testers	Versioned release candidate
Staging/UAT	Production-like rehearsal and customer acceptance	Representative minimised data; no uncontrolled production copy	Same artefact and migration path as production
Production	Live contracted service	Real data; least privilege; privileged access monitored and reviewed	Approved, logged release with backup, smoke test and rollback
Sandbox/demo	Sales demos, training and integration trials	Clearly non-production; synthetic tenants; resets and expiry	Approved demo build; isolated from live clients

Promotion controls

1. A change is linked to an approved requirement, reviewed code and test evidence.
2. CI produces a uniquely identified artefact and records dependency/security checks.
3. The same artefact is deployed to staging, where migrations, configuration, smoke tests and rollback are rehearsed.
4. Release approval confirms residual risk, communications, support coverage, monitoring, backup and recovery readiness.
5. Production deployment is logged; health and critical business journeys are verified before the release is closed.

Secrets, external assets and manual configuration

- RME 0.3 Configuration Centre is the controlled intake for public identifiers, provider references, environment settings, feature state and activation evidence.
- Secrets, private keys and provider credentials remain encrypted or server-side; they never appear in browser payloads, public documents, source control or ordinary logs.
- Every entry records environment, owner, source, classification, verification state, test evidence, effective date and rollback/deactivation method.

- Missing values display “Not configured” or “Pending verification”; fabricated identifiers, sample production keys and silent defaults are prohibited.
- Feature flags remain disabled until the corresponding asset, provider contract, consent/privacy review, sandbox/UAT, monitoring and approval gates pass.

Production access

Direct production modification is prohibited except through a documented emergency procedure. Privileged access requires named accounts, MFA where supported, approval proportionate to risk, session/action logging, time-bounded elevation and post-use review. Database changes use versioned migrations; manual repair scripts are reviewed, backed up, logged and retained as controlled artefacts.

SECTION 14 | Version Control and Release Management

Source-of-truth rule: If code, infrastructure configuration, schema, prompt, policy-as-code or deployment procedure affects production, its controlled version belongs in an approved repository or document system with an owner and change history.

Repository standard

- One accountable owner, product/service classification, README, setup, architecture link, support status and licence notice.
- Protected main branch, required peer review, successful checks, traceable work item and no committed secrets.
- Short-lived branches or trunk-based development; long-lived release branches only where a maintained version requires them.
- CODEOWNERS or equivalent for security-critical, platform, infrastructure, billing and data migration areas.
- Dependency lockfiles, automated update workflow, release tags, changelog and retained build/release evidence.
- Access review at least quarterly and immediately after role change, departure, compromise or vendor change.

Release classes

Table 25. Release classes and approval

Class	Typical change	Minimum approval
Standard	Planned backward-compatible feature, fix or configuration	Product/engineering owner after automated gates and staging acceptance
Major	Breaking API, material workflow, architecture, data or contract change	Product, technology, service, security/privacy and commercial approval
Security	Vulnerability remediation or hardening	Security and technical owner; disclosure/communications as required
Emergency	Critical incident restoration or actively exploited risk	Designated incident/change authority with minimum safe test and rollback
Infrastructure	Hosting, network, runtime, database or provider change	Technology/service owner; migration, capacity and recovery evidence

Release record

- Product/service, version, date/time, environment, artefact identifier and commit/tag.
- Scope, work items, user impact, known limitations, data migration and compatibility.
- Test/security evidence, approvers, backup reference, deployment and rollback steps.
- Monitoring window, smoke-test result, incidents/rollback and final release status.

- Customer/support communications, documentation and post-release review date.

Release cadence

Use a predictable release train for customer-facing products, supported by continuous delivery to non-production. High-value low-risk changes may be released more frequently when automation and observability are mature. Security patches follow risk-based urgency. Cadence must never override the evidence required to deploy safely.

SECTION 15 | Feature-Development Framework

Feature rule: A feature is an investment hypothesis: a specific change for a defined user is expected to improve a measurable outcome. Shipping is not proof; observed use and benefit are proof.

Feature flow

1. **Capture:** Record the problem, affected users, evidence, urgency, requester and strategic link.
2. **Discover:** Observe workflows, alternatives and constraints; establish baseline and outcome metric.
3. **Decide:** Prioritise against value, reach, risk reduction, effort, dependency, strategic reuse and opportunity cost.
4. **Specify:** Define scope/non-goals, journeys, acceptance, analytics, security/privacy, support and migration.
5. **Design and validate:** Prototype the riskiest assumption with users and technical/control reviewers.
6. **Build and verify:** Deliver a thin vertical slice, test, document and instrument it.
7. **Release and learn:** Roll out progressively, measure outcome and decide to expand, change or remove.

Feature brief

Table 26. Minimum feature brief fields

Field	Required question
Problem and user	Who experiences what problem, and what evidence supports it?
Outcome	Which behaviour/business measure should change, from what baseline?
Scope	What is included, explicitly excluded and deferred?
Acceptance	How will users, QA and operations know the feature works?
Data/AI	What data, model, prompt, knowledge, tool, retention and evaluation changes occur?
Trust	What threat, privacy, legal, accessibility, safety or fraud impacts must be controlled?
Operations	How is it monitored, supported, recovered, rolled back and eventually retired?
Commercial	Does packaging, price, entitlement, contract, training or support change?

Prioritisation guardrails

- Protect mandatory security, privacy, legal, resilience and severe-defect work from feature crowding.
- Prefer shared platform capabilities when two or more validated products need the same function.
- Do not build a bespoke client request into the core product until reuse, configuration and lifecycle ownership are understood.
- Include total lifecycle cost: design, implementation, infrastructure, support, documentation, compliance, migration and retirement.

- Limit work in progress; finishing, measuring and learning has priority over starting more initiatives.

SECTION 16 | Feature Updates and Upgrades

Upgrade principle: Every supported product has a maintained path from its current version to a supported future version, including data, configuration, integrations, users, documentation and rollback.

Upgrade programme

- **Inventory:** Maintain runtimes, frameworks, packages, models, prompts, APIs, operating systems, devices and vendor end-of-support dates.
- **Classify:** Separate routine patching, backward-compatible upgrade, breaking change, security emergency and platform migration.
- **Test:** Use compatibility matrices, automated regression, representative data, load, integration, migration and recovery tests.
- **Communicate:** Publish impact, action, timing, support window, deprecation and rollback information appropriate to clients and staff.
- **Roll out:** Use pilot tenants, feature flags, canary/percentage rollout or maintenance windows according to risk and platform capability.
- **Review:** Measure adoption, errors, support demand, performance, cost and intended benefit; remove obsolete paths.

Dependency and provider changes

Table 27. Change impact checks

Change	Required checks
Library/framework	Security advisories, licence, API compatibility, build/test, performance and rollback
Runtime/database	Vendor support, migration tools, extensions, character/timezone behaviour, query plans and backups
AI model/provider	Quality/safety regression, data terms, location, retention/training, latency, cost, rate limits and fallback
Payment/communications	Webhook/API contracts, reconciliation, fraud, delivery, consent, failover and customer messaging
Hardware/firmware	Compatibility, secure update, warranty, device identity, rollback, safety and field-support plan

Deprecation policy

Deprecation is announced through a supported release before removal whenever feasible. Notices state the affected capability, reason, replacement, migration steps, support dates and contact. Removal occurs only after telemetry and client records show an acceptable migration state or an authorised exception is recorded. Security risk may justify an accelerated timeline with executive and customer communication.

SECTION 17 | New Feature Releases

Release readiness: A new feature is ready for general availability only when it is valuable, usable, secure, supportable, documented, measurable and commercially clear - not merely when code is complete.

Table 28. Feature release stages

Stage	Audience and purpose	Minimum controls
Internal alpha	Rihuum staff validate concept and operational fit	Synthetic/minimised data, explicit limitations, rapid feedback
Private beta	Selected customers validate outcome and integration	Pilot terms, tenant isolation, support owner, monitoring and rollback
Public beta	Broader learning where risk is controlled	Clear beta label, no unsupported commitments, capacity and incident plan
General availability	Supported production offer	Pricing/entitlement, documentation, SLA/support, security, recovery and commercial approval
Limited availability	Regulated, high-complexity or partner-dependent feature	Qualification criteria, solution review and controlled deployment

Go-to-market readiness

- One-sentence value proposition, ideal customer profile, supported use cases and explicit non-use cases.
- Packaging, entitlement, price logic, contract/SLA impact, implementation effort and margin estimate.
- Demo environment, sales enablement, onboarding, product documentation, knowledge-base articles and training.
- Support escalation, telemetry dashboard, status communications, rollback and incident contacts.
- Launch metrics for awareness, activation, adoption, outcome, support, reliability, security and commercial conversion.

Post-release review

Review at 24-72 hours for technical health, then at a period suited to the user cycle for adoption and outcome. Compare actual performance with the baseline and release hypothesis. Close the launch only after defects and documentation gaps have owners; schedule a later benefit review to decide whether to expand, redesign or retire the capability.

SECTION 18 | Software Versioning

Versioning standard: Rihuum products and public APIs use Semantic Versioning 2.0.0 where a clear public interface exists: MAJOR for incompatible change, MINOR for backward-compatible functionality and PATCH for backward-compatible fixes.

Table 29. Version identifiers across the ecosystem

Asset	Version method	Example and rule
Product/application	MAJOR.MINOR.PATCH	2.4.1; immutable release; tag may be v2.4.1
RME Core	MAJOR.MINOR.PATCH plus compatibility matrix	RME 1.4.0 declares supported Rihuum OS/module/API/schema ranges; no product deploys against an unverified core version
Pre-release	SemVer suffix	2.5.0-beta.2; not represented as production-stable
Build	SemVer build metadata/artefact id	2.4.1+build.20260722.3; traceable to commit
API	Major version in contract/route or negotiated header	/api/v1; compatible additions do not force a new major
Database schema	Monotonic migration identifiers	202607221430_add_audit_index; applied state recorded
AI prompt/policy	Independent immutable version	support-triage-prompt 1.3.0; linked to model, tools and evaluation
Model/evaluation set	Provider/model id plus Rihuum registry version	Approved model snapshot and evaluation suite version retained
Documents/policies	Major/minor with approval date	Blueprint 2.1; policy 1.2; controlled supersession
Hardware/firmware	Vendor and Rihuum compatibility record	Device model, hardware revision, firmware and support state

Compatibility commitments

- Declare and document the public interface before promising semantic compatibility.
- Never change an already released artefact in place; issue a new version.
- Publish breaking changes, migration guides and support timelines before major upgrades.
- Pin critical dependencies and record a support matrix for client deployments and integrations.
- Version AI behaviour components together in an evaluation record even when the user-facing product version does not change.

Semantic Versioning reference: <https://semver.org/>. See Appendix E.

SECTION 19 | Database and System Migrations

Migration rule: Every production data or system change is versioned, reviewable, rehearsed, observable and recoverable. A database backup alone is not a migration plan.

Expand-migrate-contract pattern

1. **Expand:** Add backward-compatible schema, fields, tables or APIs while old code continues to work.
2. **Migrate:** Backfill or transform data in bounded, restartable batches with validation, monitoring and exception handling.
3. **Switch:** Deploy code that reads/writes the new structure; use flags or compatibility layers for controlled transition.
4. **Observe:** Confirm counts, integrity, latency, errors, business journeys and downstream integrations through a defined stability window.
5. **Contract:** Remove obsolete fields, paths or compatibility code only after consumers and rollback windows are cleared.

Migration plan

Table 30. Required migration controls

Control	Evidence
Scope and owner	Systems, tenants, data, integrations, downtime, owner, approver and support contacts
Data mapping	Source-to-target fields, types, transformations, defaults, identifiers, retention and rejected records
Risk	Threat/privacy assessment, integrity risks, performance, vendor limits and business impact
Rehearsal	Representative dataset, elapsed time, capacity, migration logs, validation and recovery result
Protection	Verified backup/snapshot, encryption, access, retention and independent copy
Execution	Idempotent scripts, checkpoints, rate control, lock/timeout handling and change window
Validation	Counts, checksums, constraints, samples, permissions, reports and business acceptance
Rollback/forward fix	Decision threshold, time window, scripts, responsible authority and communication

Data migration principles

- Preserve original evidence until the target is accepted and retention/deletion is authorised.
- Use stable immutable identifiers; do not treat names, email addresses or mutable external references as primary identity without mapping.
- Handle dates, time zones, currency, decimal precision, character encoding and null/default semantics explicitly.
- Record rejected, duplicated or transformed data and assign business owners to resolve exceptions.
- Test tenant boundaries and authorisation after migration, not only data counts.

- Keep migration logs free of unnecessary personal or secret data and protect them as controlled records.

System and vendor migration

A vendor migration includes identities, contracts, licences, integrations, network paths, data exports, retention/deletion confirmation, support procedures, monitoring, billing reconciliation and user change. Exit capability must be assessed at procurement and tested before a vendor becomes operationally critical.

SECTION 20 | Backup, Rollback, Recovery, and Disaster-Management Procedures

Recovery principle: A backup is useful only when Rihuum can locate it, decrypt it, restore it, validate it and resume the priority service within an approved business time objective.

Service recovery tiers

Table 31. Proposed recovery objectives for board approval

Tier	Examples	Proposed RTO	Proposed RPO	Minimum pattern
Tier 1 - Critical	Identity, production client operations, billing entitlement, core support	4 hours	1 hour	Frequent protected backup/replication, tested runbook, priority response
Tier 2 - Important	CRM, Academy delivery, client projects, operational reporting	12 hours	4 hours	Automated backups, separate copy, documented restore
Tier 3 - Standard	Public websites, knowledge content and non-critical internal tools	24 hours	24 hours	Daily backup, redeployable artefact and DNS/content recovery
Tier 4 - Archive	Closed projects, historical records and long-term evidence	As agreed	As archived	Encrypted archive, retention index and periodic readability check

RTO is the target time to restore service; RPO is the maximum target data-loss window. These are planning recommendations, not contractual promises, until approved, funded and tested.

Backup standard

- Apply a 3-2-1 style resilience pattern where proportionate: multiple copies, different media/services and at least one separately controlled/offline or immutable copy.
- Back up databases, uploaded files, critical configuration, keys/escrow where appropriate, repositories, deployment records and documentation; do not assume hosting backups cover all assets.
- Encrypt transfers and stored backup; restrict deletion and restoration rights; record access and rotation.
- Define retention by legal, contractual, business and privacy need; automated expiry must not destroy litigation, audit or incident holds.
- Monitor backup jobs and storage capacity; failed jobs create owned alerts, not silent dashboard warnings.
- Run sample restores monthly for critical data and full service recovery exercises at least annually or after material change, with frequency increased for higher risk.

Rollback strategies

Table 32. Rollback mechanism by change type

Change	Preferred recovery
Application release	Redeploy the last known-good immutable artefact and compatible configuration
Feature	Disable with a governed feature flag or configuration while preserving evidence
Database migration	Backward-compatible code plus forward repair; restore only when the loss/consistency decision is authorised
Infrastructure	Recreate previous configuration or route traffic to prior environment
AI model/prompt/tool	Pin and reselect last approved bundle; suspend tool authority; re-run evaluations
Content/policy	Restore prior approved version with an audit trail and correct downstream copies

Disaster response

1. Declare the incident/disaster level, incident commander and communications lead; protect life and safety first.
2. Contain further loss, preserve evidence and confirm which services, tenants, data, vendors and obligations are affected.
3. Invoke the relevant continuity and recovery runbooks; communicate verified facts through approved channels and status services.
4. Restore in business-priority order, validate security and integrity, and obtain service-owner acceptance.
5. Complete legal/privacy/contractual notifications as required; maintain a decision and communications log.
6. Conduct a blameless lessons review, track corrective actions and re-test changed controls.

SECTION 21 | Maintenance and Technical-Support Framework

Service model: Support is part of the product. No offer reaches general availability without ownership, hours, channels, severity definitions, escalation, knowledge, maintenance and end-of-support terms.

Support operating model

- **Level 0:** Self-service status, documentation, knowledge base, guided diagnostics and safe in-product help.
- **Level 1:** Intake, identity/entitlement verification, categorisation, known fixes, communication and routing.
- **Level 2:** Product/implementation specialists reproduce, configure, repair data/workflows and coordinate vendors.
- **Level 3:** Engineering, security or infrastructure investigates defects, vulnerabilities, systemic reliability and permanent correction.
- **Problem management:** Recurring incidents are grouped, root causes and workarounds published, and corrective changes prioritised.

Proposed severity model

Table 33. Illustrative incident response targets

Severity	Definition	Initial response target	Update target
S1 Critical	Widespread outage, confirmed major breach/safety issue, or critical business process unavailable with no workaround	15-30 minutes for contracted 24x7 service	At least hourly while active
S2 High	Major degradation or important function unavailable for multiple users; limited workaround	1 business hour	Every 4 business hours
S3 Medium	Limited defect with workaround and no material data/security impact	1 business day	Agreed milestone updates
S4 Low/Request	Question, minor issue, enhancement or planned service request	2 business days	On material change

Targets must be reconciled to staffing, monitoring and each signed service agreement before being offered contractually.

Maintenance classes

- Preventive: patching, dependency/runtime updates, capacity, backup tests, access reviews, data cleanup and certificate renewal.
- Corrective: defect, vulnerability, configuration and data repair with root-cause follow-up.
- Adaptive: browser/device/API/regulatory/vendor compatibility and infrastructure migration.
- Perfective: performance, usability, accessibility, supportability and operating-cost improvement.
- Lifecycle: end-of-sale, deprecation, migration, end-of-support and secure retirement.

Support data and customer experience

All support contacts should enter one service system linked to the client, product, entitlement, environment, release and asset. Record symptom, impact, diagnosis, actions, communications, resolution, cause and knowledge article. Sensitive data belongs in approved protected fields or attachments, never in unnecessary free text. Customer satisfaction and reopen/recurrence rates are reviewed with response and resolution metrics.

SECTION 22 | Quality Assurance and Software-Testing Procedures

Quality objective: Testing provides evidence about risk; it does not prove perfection. Quality is designed into requirements, architecture, code, data, operations and support, then verified continuously.

Test portfolio

Table 34. Required test layers

Test type	Purpose	Automation expectation
Unit/component	Business rules, validation and isolated module behaviour	High for stable logic; fast and deterministic
Integration/contract	Database, modules, APIs, providers and asynchronous workflows	Automate critical contracts and failure cases
End-to-end	Priority user journeys across the deployed system	Small reliable suite plus exploratory testing
Security	Threat controls, SAST/dependency/secrets, authentication, authorisation, input/output and penetration	Automated baseline; independent manual testing by risk
Privacy/data	Purpose, consent/notice, rights, minimisation, isolation, retention, export and deletion	Automate repeatable tenant/data controls
Accessibility	Keyboard, semantics, contrast, labels, zoom, screen-reader paths and content	Automated scan plus manual assistive review
Performance/resilience	Load, latency, capacity, timeout, retry, failover, queue and recovery	Scenario-based before scale/material change
Migration/recovery	Schema/data transformation, rollback/forward fix and restore	Every migration in CI/staging; periodic full exercises
AI evaluation	Task success, grounding, safety, bias, privacy, security, cost and regression	Versioned suites on every material model/prompt/knowledge/tool change
UAT	Business fitness, usability, control and operational readiness	Human acceptance with recorded scenarios/results

Release quality gates

- No unresolved critical defect or vulnerability; high-risk exceptions require named authorised acceptance, compensating controls and expiry.
- Critical business journeys, tenant boundaries and permission tests pass in the release candidate.
- Performance and capacity are appropriate to forecast demand and hosting limits.
- Migrations, backup, restore or rollback are verified proportionate to change risk.
- Monitoring, support knowledge, runbooks, documentation and communications are complete.
- AI changes meet approved evaluation thresholds; high-impact outputs/actions retain required human control.

Defect management

Defects are classified by customer impact, security/privacy, data integrity, frequency, detectability and workaround. Each has an owner, affected versions, root-cause category, target release and verification evidence. Escaped defects and recurring causes feed design standards, automated tests and training. Quality metrics must discourage hiding defects or inflating test counts.

Independent assurance

Use independent penetration testing and specialist reviews before high-risk production use, after material architecture/security change and at a frequency based on exposure and contract. Hardware, CCTV, telematics and physical-access installations require site acceptance, safety, failover, tamper and evidence-retention tests in addition to software testing.

SECTION 23 | Documentation and Change-Management Processes

Documentation rule: A system is not maintainable when essential knowledge lives only in a person's memory, a chat thread or an unversioned file.

Documentation architecture

Table 35. Controlled documentation set

Audience	Required documents
Board/executive	Strategy, portfolio, budget, risk, KPI, policies, investment decisions and business continuity
Product/commercial	Product brief, roadmap, pricing, licence, SLA, implementation, release and lifecycle
Architecture/engineering	ADRs, diagrams, module/API/data contracts, setup, code standards, migrations and dependency records
Security/privacy	Policies, risk/threat/DPIA, controls, access, processing records, vendors, incidents and assurance evidence
Operations/support	Deployment, monitoring, backup/restore, incident, escalation, troubleshooting, assets and maintenance
Users/clients	Onboarding, configuration, role guides, release notes, knowledge base, status and support channels
Academy	Curriculum, outcomes, content ownership, assessment, moderation, credentials, learner policy and instructor guides

Change request and approval

1. Describe the current state, proposed change, reason, benefits, urgency, scope, owner and affected stakeholders.
2. Assess product, architecture, security, privacy, legal, financial, people, customer, vendor, migration and continuity impacts.
3. Classify standard, normal/major or emergency change and route to the appropriate authority.
4. Plan build/test, communication, training, deployment, monitoring, rollback and post-change review.
5. Execute through controlled environments; record actual outcome, deviations, incidents and evidence.
6. Update the authoritative documents, configuration, knowledge and training; close only after acceptance.

People-side adoption

- Identify who must understand, decide, perform or support a new way of working.
- Explain purpose and impact early; include affected staff and clients in design and pilot feedback.
- Provide role-specific training, practice environments, job aids and manager reinforcement.
- Measure adoption and workarounds, not only attendance; resolve process, incentive and usability barriers.

- Retire old processes and access deliberately after the new process is stable.

Retention and review

Each controlled document has an owner, classification, version, approval, effective date, review date and superseded status. Retain documents according to legal, contractual, operational and evidential need while avoiding indefinite storage of unnecessary personal data. Public content has accuracy and freshness reviews; expired claims, prices, team profiles and security statements are corrected or removed promptly.

SECTION 24 | Emerging Technologies and Market Opportunities

Innovation position: Rihuum will evaluate emerging technology as a business option, not a marketing identity. Adoption requires a real problem, comparative advantage, safe operating model and acceptable lifecycle economics.

Table 36. Technology opportunity and near-term posture

Technology	Rihuum opportunity	2026 posture
Agentic AI	Knowledge work, service orchestration, operations and domain copilots	Build governed Levels 0-3 first; restricted tools, approvals and evaluation
Computer vision	Security events, asset/quality observation and hospitality operations	Pilot only with DPIA, lawful signage/use, accuracy and human verification
IoT and edge	Facilities, agriculture, fleet, energy, cold-chain and asset telemetry	Partner-led pilots with device identity, secure update and offline resilience
Digital twins	Operational models of sites, assets and processes	Start with data/asset model and dashboards before high-cost simulation
Predictive analytics	Maintenance, demand, churn, risk and resource planning	Use where reliable labelled history and actionable interventions exist
Robotics/automation	Inspection, hospitality/service and repetitive physical tasks	Research/partnership; safety and maintenance economics govern adoption
Blockchain	Multi-party provenance or settlement where no trusted operator is acceptable	Use only after a conventional signed database fails the trust requirement
Spatial/immersive	Technical training, remote assistance and property/event experiences	Selective prototypes tied to learning or service outcomes
Privacy-enhancing technology	Secure analytics, data collaboration and minimisation	Evaluate tokenisation, differential privacy or federated methods by use case
Quantum readiness	Long-lived sensitive data and cryptographic inventory	Maintain crypto inventory; follow standards transition rather than speculative products

Opportunity evaluation scorecard

- Problem severity, reachable buyer, willingness to pay and existing alternatives.
- Rihuum right-to-win: relationships, data, workflow knowledge, platform reuse, delivery channel and defensible IP.
- Technical feasibility, data readiness, infrastructure, skills, vendor dependence and time-to-evidence.
- Security, privacy, safety, legal, ethical, accessibility and social impacts.
- Total lifecycle cost, gross-margin path, support/maintenance and exit capability.

- Experiment design with a stop condition; successful demonstration alone does not equal commercial readiness.

Priority market plays

- SME operating systems: modular CRM, workflow, billing, inventory, people and service management.
- Public-service and institutional workflow modernisation with local implementation and data-governance capability.
- Hospitality/property technology combining guest/service workflows, events, access, security, facilities and analytics.
- Fleet, logistics and field-service intelligence combining telematics, asset, maintenance, proof and billing workflows.
- AI and cybersecurity readiness for organisations that need practical governance, training, evaluation and implementation.
- Digital workforce programmes linked to live projects, apprenticeships and employer-measured outcomes.

Africa-specific opportunity extensions

- Cross-border trade, export readiness and AfCFTA-aligned workflow coordination through licensed and country-validated partners.
- Maritime, ports, blue-economy, climate, circular-economy and distributed energy operations where field evidence and asset visibility create measurable value.
- Cooperative, association, faith/community, artisan, gig-work and diaspora service models that require affordable membership, commerce, communication and accountable workflows.
- Pharmaceutical and medical-supply coordination that complements validated clinical and regulatory systems without unsupported clinical claims.
- Low-data, offline-tolerant, accessible and progressively multilingual experiences designed for device, power, connectivity and digital-skills realities.

SECTION 25 | Technology Research and Innovation Roadmap

Research model: Rihuum's innovation laboratory must turn uncertainty into evidence and reusable knowledge. It is not an unrestricted prototype factory.

Innovation funnel

Table 37. Research and commercialisation stages

Stage	Activity	Decision evidence
Scan	Market, customer, regulatory, research, vendor and competitor signals	Opportunity thesis and strategic relevance
Frame	Problem, user, current alternatives, value, risk and learning question	Testable hypothesis and owner
Experiment	Smallest safe prototype, data study or service trial	Recorded method, result, limitations and next decision
Validate	Customer desirability, technical feasibility, trust and commercial evidence	Pilot design and investment case
Incubate	Controlled product/service with operating, IP and support model	Paid pilot and gate metrics
Commercialise	Packaging, channel, delivery, governance and scale	Repeatability, unit economics and portfolio approval
Transfer/stop	Move to product team, license/partner, publish learning or close	IP/knowledge record and resources released

Research themes by horizon

- **0-12 months:** RME shared core and contracts; RME-powered Rihuum OS thin slices; RIA governance; Nigerian SME workflows; Academy outcomes; shared-hosting portability; security and data baselines.
- **12-36 months:** Sector modules; multilingual/local knowledge; edge/IoT operations; private AI; advanced analytics; partner APIs and marketplace controls.
- **3-5 years:** Digital twins, regional data collaboration, robotics partnerships, smart-city components and African domain datasets/models where lawful and sustainable.
- **5-10+ years:** New human-computer interaction, resilient distributed infrastructure, frontier AI governance and post-quantum transition according to mature standards and market need.

Research governance

- Maintain an experiment register with hypothesis, owner, budget, data, risk, method, result, artefacts, IP and decision.
- Use synthetic or governed data; experiments never bypass privacy, security or client commitments.
- Review third-party licences before code, models or data enter a commercial product.
- Fund explicit, revisable innovation capacity without weakening reliability or client commitments; publish selected work only after legal, security, confidentiality and claims review.

SECTION 26 | Market Expansion and Commercialisation Strategy

Expansion principle: Expand a repeatable offer, not organisational complexity. A new market requires customer evidence, delivery capacity, legal/tax/data readiness, partner due diligence and a funded support model.

Phased market path

Table 38. Market expansion sequence

Phase	Market focus	Entry method	Readiness gate
1 - Nigeria reference base	Priority sectors and cities with reachable buyers	Direct sales, founder/executive networks, partnerships and paid lighthouse pilots	Repeatable implementation, reference clients and controlled service quality
2 - West African corridor	Selected English/French markets after research	Local delivery/reseller partners and regional enterprise relationships	Localisation, legal/tax/data assessment, partner enablement and support
3 - Pan-African sectors	Countries where a proven vertical solves a common problem	Strategic alliances, cloud marketplaces, donor/development programmes and enterprise channels	Regional platform, currency/tax, data location, multilingual and assurance maturity
4 - Selected international	Diaspora-linked SMEs, specialist African operations and software exports	Digital acquisition, OEM/technology alliances and enterprise procurement	International contracts, privacy transfers, IP, support zones and competitive differentiation

Commercialisation playbook

1. Define the ideal customer, economic buyer, urgent problem, outcome and why Rihuum can win.
2. Package a narrow offer with scope, implementation, subscription/licence, support and evidence-based promise.
3. Recruit lighthouse customers under clear pilot terms and obtain permission for measured references only after success.
4. Standardise discovery, configuration, migration, training, go-live, support and renewal to reduce implementation variance.
5. Build partner channels with qualification, territory/lead rules, training, demo, margins, quality, security and termination terms.
6. Localise content, language, currency, tax, payments, data, accessibility, support and contracts before broad promotion.

Partnership strategy

Table 39. Partner categories and safeguards

Partner	Value	Safeguard
Technology/cloud	Infrastructure, AI, productivity, security and marketplace capability	Exit plan, data terms, service levels, security, costs and competence
Hardware/OEM	CCTV, networking, access, IoT and telematics supply/warranty	Authorisation, genuine supply, warranty, spares, firmware and support
Delivery/reseller	Local sales, implementation and support	Certification, client ownership, brand, quality, data access, audit and termination
Academia/training	Curriculum, instructors, research, credentials and talent	Learning outcomes, IP/content, assessment integrity and learner protection
Government/development	Policy alignment, skills, infrastructure and market programmes	Procurement integrity, measurable outcomes, sustainability and public accountability
Investor/venture	Capital, governance, network and commercial expertise	Strategic fit, rights, dilution, use of funds, reporting and conflicts

Country readiness checklist

- Demand, competitors, willingness to pay, routes to market and reference relevance.
- Entity/registration, tax, employment, foreign exchange, import, telecom/device and sector licensing.
- Privacy, cybersecurity, cross-border data, government/cloud procurement and localisation obligations.
- Payment collection, currency, invoicing, collections, repatriation and fraud controls.
- Language, culture, accessibility, time zone, support, installation and spare-parts capacity.
- Partner diligence, anti-bribery, sanctions, beneficial ownership, reputation and contractual enforcement.

CYBERSECURITY LICENSING: Sentinel Core and every security capability use independent server-side entitlements. A licence never replaces written authority, verified ownership, exact scope, approval, data-protection or commissioning requirements.

SECTION 27 | Pricing, Licensing, Subscription, and Revenue Models

Pricing principle: Price the value and operating commitment, then verify that the resulting revenue covers delivery, infrastructure, support, risk, channel and continued product investment. Do not copy a competitor price without comparable scope and economics.

Table 40. Revenue architecture

Model	Best use	Core price drivers
SaaS subscription	RME, Rihuum OS, AI, portals, LMS and analytics	Tenant, users, modules, sites/assets, usage, support and billing term
Usage-based	AI tokens/actions, messages, storage, telemetry or transactions	Metered unit, included allowance, overage, cap and cost volatility
Implementation	Discovery, configuration, data migration, integration and training	Complexity, data, systems, locations, risk and acceptance
Managed service	Hosting, operations, cybersecurity, networks, devices and support	Coverage hours, assets, sites, volume, SLA and tooling
Term/perpetual licence	On-premise/private deployments with client control	Environment, modules, users, term, maintenance, upgrade and audit rights
Hardware/project	CCTV, access, networking, IoT, telematics and events	Bill of materials, logistics, installation, warranty, margin and maintenance
Training	Public courses, cohorts, enterprise skills and certification support	Learners, duration, instructor, lab, content, assessment and credential
Advisory/research	Strategy, architecture, security, analytics and innovation	Scope, expertise, evidence, duration and deliverables
Partner/IP	OEM, reseller, white-label, marketplace, royalty and venture	Territory, rights, volume, support, IP, exclusivity and governance

RME and Rihuum OS packaging hypothesis

- **RME Foundation:** Core tenant, identity, policy, master records, audit, commercial entitlements, support and lifecycle controls included beneath every supported Rihuum product.
- **Starter:** RME Foundation plus a Rihuum OS CRM/workflow thin slice, standard reports, self-service knowledge and business-hours support for smaller organisations.
- **Growth:** More modules, integrations, automation, analytics, environments and customer-success support.
- **Enterprise:** Advanced identity, isolation, audit, SSO, private deployment options, contractual assurance, extended support and solution architecture.
- **Sector editions:** Configured workflows and integrations for Academy, hospitality, smart operations, fleet or other validated verticals.
- **AI add-ons:** Authorised knowledge, assistants and agents priced by capability/usage with guardrails, evaluation and audit included as baseline trust features.

Licensing principles

- Use central entitlements and signed licence/activation records; define tenant, environment, module, user/device/asset, term and support rights.
- Permit reasonable offline operation for approved on-premise clients through time-bounded signed licences and auditable renewal, not brittle constant phone-home dependence.
- Do not collect unnecessary device or personal data for licence enforcement; provide an appeal/support path for false lockouts.
- Separate Rihuum-owned code, third-party/open-source components, client data/configuration and jointly developed IP in contracts and repositories.
- Security patches necessary to safely operate a supported product are not withheld as a premium feature.
- Define suspension, termination, export, deletion, renewal, support and end-of-life rights clearly.

Pricing governance and unit economics

Before approval, each price has a cost model covering infrastructure/vendor consumption, implementation labour, support, sales/channel cost, payment fees, warranty/returns, compliance and ongoing product investment. Track gross margin, contribution margin, acquisition cost, payback, retention, expansion and support cost by offer and segment. Discounting requires authority, reason, expiry and visibility; avoid one-off prices that create permanent support obligations without recurring funding.

This blueprint intentionally avoids invented naira or dollar prices. The commercial team should complete market interviews, competitor scope analysis and cost baselines, then submit a board-approved price book.

SECTION 28 | Client Onboarding and Deployment Procedures

Client outcome: Onboarding is complete when the client can use, govern and obtain value from the solution safely - not when software is merely installed.

End-to-end onboarding

Table 41. Client onboarding and deployment stages

Stage	Rihuum activity	Client acceptance evidence
Qualify	Confirm buyer, problem, budget, timing, authority, risk, fit and conflicts	Mutual decision to discover or decline
Discover	Map goals, users, process, data, systems, sites, controls, support and baseline	Validated discovery record and priority outcomes
Contract	Proposal/SOW, responsibilities, milestones, fees, licence, SLA, data/security and change control	Signed agreement and authorised contacts
Prepare	Project plan, tenant/environment, identities, data plan, integrations, risk/DPIA, training and go-live	Readiness checklist and approved design
Configure/build	Configure modules, implement integrations, migrate/test data, document and demonstrate	Iteration acceptance and issue log
Validate	UAT, security, privacy, performance, migration, recovery, operations and support rehearsal	Signed UAT/readiness decision and residual risk
Go live	Final backup/cutover, smoke tests, monitoring, communications and hypercare	Production acceptance and stable operation
Adopt	Training, usage review, outcome tracking, support and optimisation	Adoption/outcome review and improvement plan
Renew/expand/exit	Value review, commercial renewal, new modules or controlled export/termination	Renewal/expansion order or completed exit evidence

Client responsibility matrix

- Rihuum owns product quality, approved configuration, documented delivery, secure operation within its scope, support and transparent risk communication.
- The client owns timely decisions, accurate requirements, authorised data, user governance, internal change, agreed infrastructure/access and lawful business use.
- Shared responsibilities - security incident coordination, data migration validation, integration testing, business continuity, user adoption and third-party dependencies - are explicit in the SOW/RACI.
- Rihuum does not accept credentials through ordinary email/chat; use approved secure exchange and remove temporary access promptly.

Deployment patterns

Table 42. Client deployment options

Pattern	Use	Key control
Shared multi-tenant SaaS	Standardised offer and fastest update path	Tenant isolation, entitlements, usage, privacy and shared-service reliability
Dedicated hosted	Higher isolation, performance or client configuration	Automated dedicated environment, cost allocation and lifecycle parity
Client cloud/private cloud	Enterprise governance, residency or integration	Shared-responsibility model, access, deployment, telemetry and support connectivity
On-premise/edge	Sites, devices, intermittent links or regulated infrastructure	Signed releases, offline licence, secure update, backup, monitoring and field support
Hybrid	Cloud control/data services plus edge/site operations	Clear trust boundaries, synchronisation, failure behaviour and data movement

Offboarding

Confirm termination authority, charges, support/end date, legal hold, client data export format, transfer method, deletion/return, identity/access removal, devices/assets, DNS/integrations, licences, vendor accounts and final reconciliation. Produce an offboarding certificate/record describing what was exported, retained under authority and deleted, subject to technical and legal limits.

SECTION 29 | Staff Recruitment, Training, and Performance Management

People strategy: Recruit for accountability, learning and ethical judgement as well as technical skill. Use the Academy as a talent pipeline, but do not place inexperienced staff alone in high-risk production, security, financial or client decisions.

Workforce planning

- Derive roles from the approved portfolio, client commitments, control requirements and capacity forecast.
- Define each role's outcomes, decision rights, skills, security/data access, reporting line, backup and development path before recruiting.
- Use employees for enduring core capability and accountable ownership; use contractors/partners for time-bounded or specialist needs with IP, confidentiality, access and exit controls.
- Maintain succession and key-person plans for company administration, product, infrastructure, security, finance, client relationships and vendor accounts.

Recruitment and onboarding

1. Approve the role, cost, employment/contract basis, outcomes and assessment rubric.
2. Use structured screening and practical, job-relevant assessment; do not request unnecessary personal data.
3. Verify identity, qualifications/references and conflicts proportionate to the role and law; document fair selection.
4. Execute employment/contract, confidentiality, IP assignment, acceptable-use, data-protection and conflict obligations.
5. Provision least-privilege access, approved devices/tools, security training, role induction, mentor and first 30/60/90-day outcomes.
6. Confirm performance and fit at defined checkpoints; close access and recover assets immediately on role change or exit.

Rihuum Technology and Digital Hub

The Academy is both a commercial education unit and Rihuum's workforce-development engine. Programmes should be designed from job/task outcomes, not tool popularity. Each programme requires curriculum ownership, prerequisites, learning outcomes, instructor standard, practical labs, assessment/moderation, learner support, accessibility, academic-integrity controls, credential verification and outcome measurement. The Academy's separate CAC registration number must be verified and displayed wherever legally required before public document release.

Table 43. Academy programme architecture

Track	Examples	Outcome evidence
Digital foundations	Productivity, internet safety, data literacy, communication and employability	Practical tasks and digital portfolio

Track	Examples	Outcome evidence
Software and product	Web/mobile, APIs, databases, QA, UX, product and DevSecOps	Reviewed projects, tests, repository and demo
AI and data	AI literacy, prompt/workflow design, analytics, ML, RIA and responsible AI	Evaluation report, governed prototype and use-case defence
Cybersecurity/ infrastructure	Security fundamentals, networking, cloud, support and incident skills	Configured lab, troubleshooting and scenario assessment
Smart systems	CCTV, access, IoT, telematics, field safety and maintenance	Site/lab installation, documentation and acceptance test
Leadership and transformation	Strategy, process, product ownership, data governance and change	Organisation-specific transformation plan

Performance management

- Quarterly objectives connect enterprise priorities to measurable team and individual outcomes.
- Performance includes delivery, quality, customer value, security/privacy, documentation, teamwork, learning and conduct - not volume of activity alone.
- Managers provide frequent feedback; formal reviews use evidence, recognise constraints and define support or corrective plans.
- Promotion requires sustained next-level scope and behaviour; technical and management career paths are both available.
- Training is tracked by applied competence and business result, not certificates alone.

SECTION 30 | Risk Management and Business Continuity

Risk governance: Rihuum accepts risk consciously through named owners and approved appetite; it does not accept risk because nobody recorded it.

Enterprise risk process

1. Identify risk from strategy, products, clients, legal duties, technology, people, vendors, assets and external change.
2. Describe cause, uncertain event and consequence; identify affected objectives and existing controls.
3. Assess likelihood and impact across financial, client, service, legal, security/privacy, safety and reputation dimensions.
4. Choose treatment: avoid, reduce, transfer/share or accept; name owner, action, budget, due date and residual risk.
5. Monitor indicators and control evidence; escalate appetite breaches and overdue high-risk treatments.
6. Review monthly for management, quarterly for board priority risks and immediately after material events.

Priority risk register

Table 44. Initial enterprise risks and treatments

Risk	Principal treatment	Owner
Portfolio overextension	Stage gates, capacity limits, product owner and stop/pause decisions	CEO / Portfolio Committee
Cash-flow and collections	Rolling forecast, deposits/milestones, receivables control, margin review and contingency	Finance / CEO
Unverified legal records or licences	Corporate/legal register, counsel review and pre-launch licensing checklist	Company Secretary
Cyberattack or data breach	Security baseline, monitoring, incident response, vendor controls, backup and exercises	Security / CTO
Shared-hosting constraint/failure	Suitability rules, independent backups/status, portability and migration triggers	CTO / Service Ops
AI harmful or unauthorised action	RIA, authority levels, approved tools, human approval, evaluation, monitoring and kill switch	AI Council / Product
Client concentration	Segment/channel diversity, account plans, recurring offers and concentration limits	Commercial / Finance
Key-person dependency	Documentation, deputies, credential custody, succession and cross-training	CEO / People
Vendor/supply-chain failure	Due diligence, contracts, inventory, alternatives, exit/data export and vendor monitoring	Procurement / CTO
Poor delivery/service quality	Scope control, QA gates, implementation playbook, service metrics and root-cause action	Product / Service Ops

Risk	Principal treatment	Owner
Hardware safety/warranty	Approved OEMs, site safety, acceptance, spares, warranty and maintenance records	Smart Solutions lead
Reputation/unsupported claims	Evidence review, approval workflow, correction process and spokesperson protocol	Corporate Communications / Legal

Business continuity

- Complete a business-impact analysis for customer support, identity, delivery, billing/collections, communications, Academy sessions and field operations.
- Define minimum people, technology, site, supplier, information and cash requirements for each priority activity.
- Maintain remote-work and alternate-location capability, contact trees, delegated authority and offline copies of essential runbooks/contacts.
- Map single points of failure: domain/DNS, hosting, power/connectivity, payment, email, credentials, vendors, instructors and client contacts.
- Exercise plausible scenarios - ransomware, hosting outage, lost device, key-person unavailability, field safety event, vendor failure and payment disruption - and track actions.

SECTION 31 | Legal, Regulatory, and Compliance Requirements

Compliance position: Rihuum will maintain one obligations register that maps each entity, product, service, country, client sector, dataset, vendor and contract to a named owner, evidence and review date. This section is a control checklist and must be validated by qualified advisers.

Nigeria corporate and general obligations

Table 45. Core legal and regulatory workstreams

Area	Action required
Corporate/CAC	Reconcile incorporation documents, beneficial ownership/share records, directors, registered office, annual returns, business names and display of legal name/registration number.
Tax and finance	Obtain current professional advice on federal/state taxes, VAT, withholding, payroll, transfer pricing where relevant, invoicing, record retention and incentives.
Data protection	Implement the Nigeria Data Protection Act 2023 and current NDPC guidance: governance, processing records, lawful basis, rights, security, processors, DPIAs, breaches and transfers.
Consumer/competition	Use fair terms, transparent pricing/renewal, accurate claims, complaint/redress, safe products and fair market conduct under applicable FCCPC requirements.
Cybercrime/evidence	Maintain lawful access, logging, incident handling, evidence preservation and cooperation processes; prohibit unauthorised access/testing.
Employment	Comply with contracts, payroll/statutory duties, workplace policies, equality/fairness, health/safety and worker data protection.
IP	Register/maintain trademarks and domains; execute employee/contractor IP assignments; manage copyright, patents where suitable, trade secrets and open-source licences.
Contracts	Standard MSA/SOW, licence/SaaS, SLA, DPA, support, reseller/vendor, Academy, hardware/warranty and acceptable-use terms with controlled deviations.

Licensing and sector trigger matrix

Table 46. Pre-launch regulatory triggers

Offering	Questions before sale or deployment
Telecom/network services	Is Rihuum merely installing/maintaining client networks or providing a regulated communications/value-added service requiring NCC analysis/licence?
Payments/financial services	Is Rihuum integrating a licensed PSP or performing regulated payment, credit, wallet, switching, remittance or financial-advice activity requiring CBN/other approval?
CCTV/biometrics/access	What lawful purpose, notice, DPIA, retention, access/evidence, accuracy, worker/public monitoring and security obligations apply?
Telematics/IoT/radio	Do equipment approval, spectrum/SIM/communications, import, location tracking, safety or sector rules apply?
Training/credentials	Is a course a Rihuum certificate of completion or represented as an accredited qualification requiring a regulator/awarding-body partnership?
Hospitality/events	What local premises, tourism, fire/safety, food, alcohol, music, event, tax and employment permits apply to the actual service?

Offering	Questions before sale or deployment
Health/education/children	Are sector approvals, safeguarding, special-category data, parental/guardian controls or professional restrictions triggered?
Government/critical infrastructure	What procurement, local-content, hosting/data, security clearance, records, audit and sovereign/critical-system requirements apply?

Startup and innovation status

Rihuum should assess eligibility and commercial value under the Nigeria Startup Act 2022 through the official Startup Support and Engagement Portal. Eligibility, labelling and incentives must be confirmed by the responsible authorities and professional advisers; the company must not advertise itself as a labelled startup unless the label has actually been issued and remains valid.

International readiness

- Perform country-specific entity, tax, employment, consumer, product, cybersecurity, data-transfer and sector analysis before entry.
- Use international data-processing and transfer terms appropriate to each jurisdiction and client role.
- Screen partners and transactions for sanctions, export controls, anti-bribery, beneficial ownership and conflicts as applicable.
- Protect trademarks, domains, software, data rights and confidential know-how in target markets before major promotion or licensing.
- Do not assume Nigerian contracts, licences, privacy notices or professional credentials automatically work abroad.

SECTION 32 | Financial and Investment Planning

Financial rule: The board should fund validated capability and preserve runway. Revenue, bookings and cash are different; profitability, cash collection, renewal obligations and product investment must be reconciled in one management model.

Financial operating system

- Monthly reconciled profit/loss, balance sheet, cash flow, receivables/payables, tax and management commentary.
- Rolling 13-week cash forecast plus annual budget and multi-year scenario model.
- Project/product/client cost and margin records, including time, infrastructure, vendor, support, hardware, warranty and channel cost.
- Delegated spending, procurement and contract authority; finance@rihuum.com issues authorised finance records, payment@rihuum.com records payments and account@rihuum.com performs separate approval. Dual control applies to payments and changes to beneficiary or bank details.
- Revenue recognition and deferred revenue reviewed by qualified accounting advisers for subscriptions, licences, services, training and hardware bundles.
- Asset, inventory, licence and vendor commitment registers; no uncontrolled recurring subscriptions.

Planning allocation bands

Table 47. Illustrative operating allocation bands

Investment area	Indicative band	Board decision test
Product, engineering and QA	25-40%	Does spend create reusable, supportable product and reduce delivery risk?
Sales, marketing and partnerships	12-22%	Is there a defined segment, conversion path, margin and payback hypothesis?
Customer success and service	10-18%	Can contracted clients onboard, adopt, renew and receive promised support?
Infrastructure, security and compliance	8-15%	Does capacity/control match current risk and near-term commitments?
Academy, people and capability	8-15%	Does training close skill gaps and produce measured workforce/client outcomes?
Corporate operations/legal/finance	8-15%	Are statutory, cash, governance and contracting controls reliable?
Research/innovation and contingency	5-12%	Are experiments bounded and is contingency sufficient for plausible shocks?

Bands are planning envelopes, not a budget and not intended to sum at their upper limits. The annual plan must select allocations that sum to 100% and reflect actual cash, stage and commitments.

Scenario and funding strategy

Table 48. Funding scenarios

Scenario	Priority	Capital approach
Bootstrap/control	Corporate compliance, domains, core team, paid services, RME core, Rihuum OS thin slice and one pilot	Founder/retained earnings, deposits, milestone billing, grants where suitable
Base growth	Repeatable product, customer-success capacity, Academy cohorts and managed services	Operating cash, strategic partners, non-dilutive programmes and selective debt only against predictable cash
Accelerated scale	Regional sales, platform/cloud, assurance, sector modules and acquisitions/partnerships	Equity/strategic investment after governance, metrics, IP and unit economics are investor-ready

Investor readiness

- Clean corporate/statutory records, cap table, beneficial ownership, board minutes and material contracts.
- Assigned IP, domain/trademark records, open-source/data/model rights and employee/contractor agreements.
- Reconciled historical financials, forecasts, tax status, use of funds and scenario assumptions.
- Product architecture, security/privacy, client metrics, pipeline, unit economics, references and risk register.
- Data room index with controlled access, confidentiality, version ownership and disclosure log.

SECTION 33 | Marketing, Branding, and Customer-Acquisition Strategy

Market message: Rihuum should be known for solving operational problems with secure, intelligent and maintainable technology - not for listing every technology it can use.

Positioning pillars

- African context and international engineering discipline.
- One partner across software, AI, security, skills, infrastructure and selected smart/industry solutions.
- Rihuum Master Enterprises as the trusted shared core, with Rihuum OS as the modular digital operating experience connecting people, process, data and service.
- Responsible Agentic AI with clear authority, evidence, security and human accountability.
- Commercial outcomes, lifecycle support and migration readiness rather than one-off technology installation.

Acquisition engine

Table 49. Customer journey and primary channels

Stage	Customer question	Rihuum channels/content
Awareness	Do they understand my industry problem?	Search-led articles, sector guides, social insight, events, Academy and partner presence
Consideration	Can they solve it safely and practically?	Use cases, architecture/security explainers, workshops, demos and references
Decision	Is value, cost, risk and implementation clear?	Discovery, business case, proposal, pilot, due-diligence pack and roadmap
Onboarding	Will we achieve value without disruption?	Kickoff, implementation portal, training, readiness, status and hypercare
Adoption	Are users succeeding and outcomes improving?	In-product guidance, knowledge, reviews, community and customer success
Expansion/advocacy	Should we renew, expand or recommend?	Value report, roadmap, new modules, partner offers, case study and referrals

Blog and index strategy

Each domain should publish original, expert-reviewed articles that answer real buyer and practitioner questions. The initial editorial pillars are RME, Rihuum OS and business systems; responsible AI and Agentic AI; cybersecurity and data protection; digital skills and careers; cloud/infrastructure; smart security/IoT/telematics; hospitality technology; analytics and innovation. Each article requires a defined audience, search intent, author/reviewer, evidence links, practical examples, update date, accessible structure, original value and conversion path. Do not mass-publish generic AI text or copy third-party work; quality, expertise and freshness are the indexing strategy.

CRM and marketing operations

- One account/contact model, lead source taxonomy, consent/lawful-basis record, lifecycle stage and owner across all domains.
- Qualification criteria and response targets; no unowned leads or personal contact spreadsheets outside approved systems.
- Campaign naming, cost, target, content, channel, conversion and revenue attribution with privacy-respecting analytics.
- Email/SMS preference centre, suppression, opt-out and frequency controls; purchased or scraped lists require legal and ethical rejection/review.
- Monthly funnel review from qualified demand to collected revenue, implementation success, retention and expansion.

Brand controls

- Official logo master files, brand guide, approved templates and asset repository with usage rights.
- Legal name, RC, email, phones, domain and 'Built and Developed by Rihuum Intercontinental Limited' attribution on controlled artifacts as applicable.
- Technical, legal, client-confidentiality and evidence review for product, security, AI, performance, certification and customer-result claims.
- Social account register, named owners, MFA, recovery contacts, approval and incident/takedown process.

SECTION 34 | Key Performance Indicators and Reporting Framework

Measurement rule: A KPI has one definition, source, owner, cadence and decision. Establish baselines in the first 90 days, then approve targets; do not reward teams for metrics they can improve while harming customer value or risk.

Table 50. Enterprise KPI framework

Perspective	Core measures	Primary decisions
Financial	Collected revenue, recurring revenue, gross/contribution margin, operating cash, runway, receivables age and forecast variance	Capital, price, collections, capacity and portfolio
Commercial	Qualified pipeline, win rate, sales cycle, acquisition cost, average contract, channel contribution and concentration	Segment, channel, offer and sales capacity
Customer	Activation/time-to-value, adoption, retention/renewal, expansion, satisfaction, complaint and support effort	Onboarding, product gaps, success and renewal
Product	Active tenants/users, workflow completion, feature adoption, outcome metric, reliability and unit cost	Roadmap, usability, packaging and retirement
Engineering	Lead time, deployment frequency, change failure, restore time, escaped defects and automation reliability	Process, architecture, quality and staffing
Security/privacy	MFA/access coverage, vulnerability age, control tests, incidents, recovery tests, rights requests and vendor risk	Risk treatment, assurance and investment
Service operations	Availability, incident response/resolution, backlog age, first-contact resolution, recurrence and SLA attainment	Support capacity, reliability and knowledge
People/Academy	Critical-role coverage, time-to-productivity, performance, retention, skills application, completion and employment/client outcomes	Recruitment, learning, succession and programme design
Innovation	Experiments completed, time-to-evidence, validation rate, IP/reuse, pilot conversion and research spend	Continue, transfer, partner or stop

Metric definition standard

- Name and decision purpose; exact numerator, denominator, inclusion/exclusion and time basis.
- Authoritative system/source, data owner, refresh, reconciliation and quality checks.
- Segment dimensions such as product, plan, sector, country, cohort, channel and client - subject to privacy and minimum group size.
- Baseline, target, threshold/guardrail, direction, owner and action when outside range.
- Change log so historical comparisons remain interpretable after a definition or source change.

Reporting cadence

- Daily/real-time: service health, security alerts, critical queues, payment failures and field safety as needed.
- Weekly: cash/collections, pipeline movement, delivery, incidents, client risk and blockers.
- Monthly: executive scorecard with trends, forecast, drivers, decisions and action ownership.

- Quarterly: board strategy, portfolio, risk, financial, customer, people, technology and market review.
- Annual: audited/reconciled performance, strategy and budget, control maturity, business continuity and public impact where appropriate.

Data quality

Every board KPI should be traceable to reconciled source data. Automated dashboards do not remove ownership: review completeness, accuracy, timeliness, uniqueness, validity and consistency; disclose material gaps and estimates. Finance is reconciled to accounting/bank records; CRM to signed contracts and collections; product telemetry to known identities/events; support to ticket records.

SECTION 35 | Implementation Phases, Timelines, and Milestones

Execution discipline: The roadmap starts immediately, but commitments beyond the next gate remain conditional on evidence, resources and board approval. Each milestone closes with documented acceptance, not optimistic status language.

Table 51. Integrated implementation roadmap

Period	Enterprise milestones	Exit evidence
0-30 days	Appoint owners; verify corporate/domain facts; inventory portfolio/assets; establish registers; approve architecture and top risks	Signed ownership, verified-facts list, portfolio map, risk/actions and 90-day budget
31-90 days	Three-domain foundation; CRM/service/finance basics; repositories/CI/environments; backups; RME core prototype and Rihuum OS shell; first market discovery	Working digital ecosystem, restore test, release evidence, RME/OS demo and pilot decision
Months 4-6	Paid lighthouse pilot; RME identity/workflow/licensing/support through a Rihuum OS thin slice; Academy LMS pilot; security/privacy baseline and onboarding playbook	Pilot acceptance, adoption/quality data, compatibility evidence, support runbook, processing records and unit-cost view
Months 7-12	General-availability narrow offer; subscription/billing; customer success; partner pilots; migrate workload if triggers met	Repeatable deployment, renewal intent, margin evidence, release cadence and board scale decision
Months 13-24	Additional validated modules; VPS/cloud platform; advanced RIA; regional partner entry; independent assurance	Multi-client/sector reference base, scalable operations, assurance findings closed and country gate
Months 25-36	Extension/marketplace controls; private/enterprise deployments; selected West African scale; venture commercialisation	Stable platform contracts, partner economics, regional service model and funded growth plan
Years 3-5	Pan-African sector plays, mature product lines, certifications where justified, data/research assets and selective acquisitions	Sustainable recurring economics, governance maturity and recognised market position
Years 5-10+	International software exports, strategic infrastructure/AI capability, venture portfolio and enduring talent ecosystem	Diversified resilient enterprise with measurable economic and societal impact

Workstream milestones

Table 52. First-year workstreams

Workstream	90-day milestone	12-month milestone
Corporate/legal	Verified records, obligations and contract templates	Current filings, IP register, vendor/client controls and legal review cadence
Brand/domains	Three-domain architecture and shared design/content governance	Measurable acquisition, original blog library and controlled client operations
RME and Rihuum OS	RME contracts, core architecture and OS demonstrator	Supported RME-powered commercial thin slice with paid clients and roadmap evidence

Workstream	90-day milestone	12-month milestone
AI/data	RIA policy, model gateway design and bounded assistant	Evaluated production AI and approved Level 3 agent workflow
Security/privacy	Inventory, MFA/access, baseline, incident and backup/restore	Control testing, vendor/DPIA programme and independent review by risk
Commercial/service	ICP, offer, CRM pipeline, onboarding and support model	Repeatable sales-to-renewal flow and unit economics
Academy/people	Programme architecture and workforce plan	Delivered cohorts, applied skills/outcomes and internal talent pathway
Infrastructure	Separated environments, CI release and migration plan	VPS/cloud decision from measured triggers; tested DR

Milestone acceptance

- Accountable owner confirms scope and evidence; independent reviewer confirms high-risk controls.
- Actual cost, time, outcome, defects, incidents, residual risk and operational load are recorded.
- Documentation, training, support, monitoring, backup/recovery and ownership are complete.
- Portfolio committee decides next funding, constraints, corrective action, pause or closure.

SECTION 36 | Short-, Medium-, and Long-Term Growth Plans

Long-term direction: Rihuum's path to leadership is cumulative: first become controlled and trustworthy, then repeatable and commercially proven, then scalable, regional and platform-led. Reputation follows sustained evidence.

Short term - foundation and proof (0-12 months)

- Complete corporate, legal, financial, domain, brand, portfolio and technology control foundations.
- Launch the three-domain ecosystem with strong original content and unified CRM/service journeys.
- Build RME Core and one commercially narrow Rihuum OS module; use them internally, then deliver paid lighthouse pilots.
- Deploy RIA and low-risk AI assistants; establish agent authority, evaluation, security and audit controls.
- Operationalise the Academy, implementation, support, backup/DR, QA and release systems.
- Establish baseline KPIs and approve evidence-based budget, prices and targets.

Medium term - repeatability and regional scale (1-3 years)

- Grow recurring subscriptions, licences and managed services while protecting implementation and support quality.
- Add validated Rihuum OS sector modules and advanced analytics/Agentic workflows behind stable RME and RIA contracts.
- Move appropriate workloads to VPS/cloud/hybrid infrastructure with stronger automation, isolation and observability.
- Build certified partner paths for delivery, hardware, training and market access; enter selected West African markets.
- Develop independent assurance and appropriate ISO-aligned management systems; seek certification only where justified.
- Create a strong internal leadership bench and Academy-to-employment/apprenticeship pipeline.

Long term - African platform and innovation enterprise (3-10+ years)

- Operate mature product lines and a governed module/partner ecosystem powered by RME and experienced through Rihuum OS.
- Serve enterprise and public-sector clients through SaaS, private cloud, hybrid and on-premise patterns across selected regions.
- Commercialise defensible African workflow, knowledge and analytics assets with lawful rights and responsible AI governance.
- Expand the Technology and Digital Hub into a recognised workforce-development and applied research network.

- Develop or partner on smart-city, edge, digital-twin, robotics and future infrastructure solutions only where measurable value and safety justify them.
- Use the venture builder to incubate, license, partner, spin out or acquire products under disciplined governance and capital allocation.

Non-negotiable growth guardrails

Table 53. Guardrails that protect the Rihuum future

Guardrail	Meaning
One trusted identity	Protect the official logo, legal identity, RC, domains and evidence-based claims across every unit.
One platform direction	Reuse RME and RIA; no isolated product stack without an approved exception, compatibility contract and lifecycle plan.
Security and privacy baseline	Growth never depends on silent acceptance of uncontrolled customer, data, AI or infrastructure risk.
Customer outcome before feature volume	Invest when use, value, retention and viable economics are visible.
Portable and recoverable systems	Every product remains versioned, documented, migration-ready, backup-enabled and rollback/recovery capable.
Legal before market promise	Verify licences, contracts, IP, tax, data and sector obligations before launch or country entry.
People and service capacity	Do not sell availability, support, installation or transformation capacity Rihuum cannot sustain.
Continuous learning	Measure, review, publish lessons internally and update this blueprint as facts change.

Board closing statement

This blueprint gives Rihuum a coherent foundation for decades of development without pretending that every future product, technology or market can be predicted. Its enduring value lies in the operating discipline: verified identity, clear ownership, modular architecture, responsible intelligence, secure delivery, commercial evidence, controlled change, recovery, documented learning and deliberate expansion. If these disciplines are maintained, Rihuum can evolve continuously without rebuilding the company or its core platforms each time technology and markets change.

SECTION 37 | RAHIS Hospitality Platform and Digital Ecosystem Expansion

Board direction for the Sandralia pilot and the reusable hospitality product family

Rihuum will develop the Rihuum AI Hospitality Intelligence Suite (RAHIS) as a multi-tenant product family within the Rihuum Intelligent Software Ecosystem. Sandralia Hotel by White Stones is the controlled pilot property. RAHIS v8.3.0 is the consolidated integration candidate comprising the v8.1 operating core, v8.2 Paystack test/sandbox adapter and v8.2 Sentinel security overlay. Sentinel remains non-authoritative for reservations, rates, folios, payments, payroll, biometrics, doors, CCTV and all hotel systems of record.

TRUTHFUL PRODUCT BOUNDARY A menu item or attractive dashboard is not a live integration. OTA, payment, translation, advertising, Google and messaging publication remain adapter-pending until contracts, credentials, consent, security review, reconciliation and acceptance evidence are complete.

37.1 Strategic product decision

Decision	Controlled direction	Required evidence
One hotel operating system	PMS, CRS, distribution, booking, guest journey, F&B, finance, workforce, maintenance and collaboration share one governed kernel.	Cross-module workflow tests, ownership map and reconciled records.
Sandralia-first, product-ready	Pilot the platform at Sandralia while keeping identity, currency, tax, policies, modules and integrations tenant-configurable.	Tenant isolation, theme pack and repeatable onboarding runbook.
Deterministic operations	Availability, money, tax, commissions, inventory, approvals and status transitions remain server-calculated and auditable.	Database constraints, immutable events and reconciliation evidence.
Governed intelligence	AI explains, drafts, forecasts and recommends; consequential external actions require scoped permission and human approval.	Evaluation set, source references, content hash and decision log.
Portable delivery	Begin with a modular shared-hosting-compatible release, then migrate through VPS, hybrid and managed-cloud tiers without product rewrite.	Adapters, migrations, backup/restore and tested cutover plan.

37.2 RAHIS product capability map

Capability plane	Product modules	Authoritative outcomes
Stay and inventory	PMS, central calendar, reservations, room assignment, stay, folio, housekeeping, maintenance and self-service arrival/departure.	One guest/stay record and dated inventory without silent overbooking.
Distribution and revenue	Channel manager, room/rate mapping, CRS, booking engine, rate shopper, forecasting, restrictions, dynamic-pricing recommendations.	Synchronized inventory/rates with approval, acknowledgement and parity

Capability plane	Product modules	Authoritative outcomes
		evidence.
Guest engagement	Unified OTA/direct inbox, translation state, templates, journey automation, CRM, loyalty, reviews and reputation cases.	Faster response with consent, source language and reservation context.
Commerce and fulfilment	Restaurant/bar catalogue, room service, pickup, external delivery, cart, checkout, POS, kitchen routing, payment and vehicle dispatch.	Server-priced orders, station-specific work and proof of fulfilment.
Business control	Finance, cash, reconciliation, procurement, stores, HR, payroll, security, fleet, utilities, ICT, cyber and executive reporting.	Append-only evidence, segregation of duties and source-backed metrics.
Growth and collaboration	AI-assisted ads/social, leads, retargeting governance, branded web, blog, WorkSuite mail/calendar/docs/sheets/slides/files/chat/tasks/meetings.	Draft-first external activity and property-scoped collaboration.

37.3 Departmental digital operating model

The objective is not merely paper reduction. Each department receives a role-scoped work queue, approved runbooks, shift execution records, evidence capture, exception routing, service-level clocks, handoffs and management reports. Paper may remain only where law, safety or outage continuity requires it; controlled forms must be digitised and reconciled afterwards.

Department	Digitised daily work	Control/report outcome
Executive Office	Strategy, approvals, daily brief, risk and performance review	Executive scorecard; decision register
Front Office & Reservations	Bookings, arrivals, stays, keys, folios, departures	Arrival control; room and deposit exceptions
Housekeeping & Laundry	Room status, cleaning, linen, minibar, lost property	Room turnaround; discrepancy and linen variance
Food & Beverage Service	Table, bar, room-service and delivery fulfilment	Order SLA; void, discount and tray collection
Kitchen, Bakery & Stewarding	Production stations, recipes, wastage, hygiene, wash-up	Prep/dispatch times; waste and safety evidence
Banquets & Events	Enquiry, quotation, BEO, space, setup, consumption and billing	Event profitability; change and handover log
Sales & CRM	Accounts, leads, pipeline, contracts and activities	Conversion, production and account profitability
Marketing & E-commerce	Content, campaigns, consent, ads, social and web demand	Approved spend, attribution and direct-booking funnel
Guest Relations & Concierge	Requests, preferences, recovery, transport and VIP journeys	Response time; recovery and satisfaction
Revenue & Distribution	Rates, restrictions, inventory, channels, pace and forecast	ADR, RevPAR, pickup, parity and sync health
Finance & Night Audit	Posting, settlement, cash, journals, receivables and close	Balanced journals; cash and interface reconciliation
Procurement & Stores	Requisition, quotes, purchase, receipt, issue and stock count	Three-way match; stock and supplier variance
Engineering & Maintenance	Assets, preventive work, defects, utilities and projects	Uptime; response, energy and recurring faults
Security, Safety & Loss Prevention	Patrols, incidents, access, keys and emergency readiness	Incident chain; patrol and corrective-action evidence
ICT & Cybersecurity	Service desk, devices, identities, backups, vulnerabilities and	Availability, restore proof

Department	Digitised daily work	Control/report outcome
	changes	and risk closure
Human Resources	People records, attendance, shifts, leave, training and performance	Roster, payroll input and competency evidence
Transport & Fleet	Airport transfers, dispatch, cars, bikes, fuel and maintenance	Trip proof; utilisation, fuel and safety exceptions
Recreation, Pool, Gym & Spa	Bookings, capacity, hygiene, waivers and guest service	Utilisation, safety checks and revenue
Legal, Privacy & Compliance	Contracts, data rights, retention, incidents and obligations	Approval, breach and compliance register
Quality & Sustainability	Audits, standards, complaints, energy, water and waste	CAPA closure and verified sustainability metrics

37.4 Distribution, booking and revenue controls

7. Maintain one canonical room type, rate plan, restriction and dated inventory record for each property and record mode.
8. Map every external room/rate identifier explicitly; unmapped or ambiguous records enter a human exception queue.
9. Create holds and confirmed reservations against dated inventory using atomic capacity checks; release or conversion creates immutable allocation events.
10. Publish rates or availability only in operational mode after a separate decision maker approves the exact source hash.
11. Persist provider acknowledgement, retry state, reconciliation outcome and the last known trustworthy source timestamp.
12. Calculate occupancy as sold room nights divided by available room nights, ADR as recognised room revenue divided by sold room nights, and RevPAR as recognised room revenue divided by available room nights; disclose zero denominators and reconciliation state.

NO ABSOLUTE GUARANTEE The architecture is designed to prevent avoidable overbooking. It must not promise that overbooking can never occur: provider latency, manual channel changes, outages and contract limitations require monitoring, safety stock and documented recovery procedures.

37.5 Public hotel experience and direct commerce

- A responsive, accessible hotel website with accommodation, dining, events, location, about, contact, policies and an editorial departmental blog.
- A branded direct-booking journey with live-source labels, date and party validation, room terms, taxes/fees, cancellation rules, booking hold and controlled payment handoff.
- A restaurant and bar catalogue with server-owned prices, modifiers, cart, checkout, room service, pickup, external delivery, order tracking and car/bike dispatch.
- Search metadata, structured data, sitemap and robots controls; indexing remains disabled until the public domain, content and legal notices pass launch review.
- GA4 measurement ID G-CLFV1L0KVJ is confirmed for rihuum.tech only. GA4 for rihuum.com and rihuum.net, GTM, Search Console values, AdSense publisher/seller data and Maps API/Place ID remain manual activation inputs. Tags or ads load only after valid identifiers, consent/privacy review and production tests.
- Sandralia public claims use the property's official source. The current official site describes a four-star property; RAHIS may promise five-star digital experience quality but must not alter the hotel's formal rating.

37.6 Unified communications and reputation

Workflow	AI assistance	Human and system control
Unified inbox	Summarise threads, detect intent and draft replies	Reservation context, property scope, source language and immutable messages
Translation	Show proposed translation and response	Original retained; quality state and provider terms disclosed

Workflow	AI assistance	Human and system control
Journey messaging	Personalise approved templates and upsell suggestions	Consent, trigger, quiet hours, variable allow-list and opt-out
Guest recovery	Classify severity and recommend service recovery	Delegated limits; manager approval for compensation
Review response	Draft empathetic, evidence-aware reply	No publication without separate hash-bound approval

37.7 Agentic AI operating boundary

Level	Permitted behaviour	Examples	Required control
A0 — Observe	Read approved, scoped records	Search, explain, summarise	Role and property filter; no mutation
A1 — Recommend	Produce ranked, sourced options	Rate, staffing, recovery or maintenance suggestion	Evidence, uncertainty and human choice
A2 — Draft	Create a non-executing work item	Reply, campaign, journal or task draft	Schema validation and immutable provenance
A3 — Execute with approval	Run an approved, bounded action	Publish rate/content; release configured message	Separate approval, source hash, budget and rollback
A4 — Bounded automation	Repeat low-risk configured actions	Internal reminders, SLA routing, anomaly alert	Policy, monitoring, kill switch and periodic review

Prohibited autonomous actions

- No unapproved rate, inventory, ad, social, review, payment, refund, journal, employment, access or safety-critical publication.
- No storage of full card data, raw biometric templates, passwords, provider secrets or unrestricted identity documents.
- No invented facts, fabricated source states, hidden price changes, discriminatory targeting or use of guest data without a lawful and disclosed basis.
- No direct database mutation that bypasses tenant, record-mode, approval, idempotency, audit or reconciliation controls.

37.8 RAHIS WorkSuite

RAHIS WorkSuite is an original collaboration environment, not a copy of Google Workspace. It provides hotel-scoped mail and inbox governance, calendar and shifts, documents, spreadsheets, presentations, shared files, chat, tasks, approvals, enterprise search and RAHIS Connect meetings. Optional Gmail, Google Calendar and Drive interoperability uses approved OAuth adapters and never implies ownership of Google products or automatic external delivery.

37.9 Hosting evolution and resilience

Tier	Purpose	Placement and controls	Exit trigger
Shared hosting	Controlled pilot and public experience	PHP/MySQL-compatible modular monolith or supported hosted runtime; 5-minute scheduler; external managed adapters	Sustained jobs, websocket needs, latency, security or scaling exceed limits

Tier	Purpose	Placement and controls	Exit trigger
VPS	Dedicated application and worker control	Reverse proxy, containers/process manager, managed secrets, queue workers, replicas and monitoring	Multi-region, regulated workload or elasticity requirements
Hybrid	Property continuity and cloud intelligence	Local bridges/cache for doors, attendance, POS or outage continuity; encrypted central control plane	Fleet-wide scale and proven recovery patterns
Managed cloud	Regional multi-property SaaS	Tenant isolation, autoscaling, managed database/queue/storage, WAF, observability and tested disaster recovery	Continuous optimisation rather than product rewrite

37.10 Multi-property commercialisation

- Central reservation groups and memberships define which properties can participate in CRS inventory and performance reporting.
- Each customer receives a tenant, property identity, theme, module entitlements, policies, currency/tax rules, data-retention schedule and connector catalogue.
- Property data remains isolated; group users receive explicitly delegated cross-property access and every query is scoped.
- A client launch pack includes discovery, configuration workbook, data mapping, migration rehearsal, training, go-live checklist, support plan and exit/export procedure.
- Commercial claims use measured outcomes. Statements such as increased revenue or reduced cost must carry baseline, period, method and exclusions.

37.11 Sandralia pilot acceptance programme

Gate	Minimum acceptance evidence	No-go examples
Identity and access	MFA, least privilege, active property role, departmental scope and break-glass test	Owner shortcut grants operational powers
Inventory and booking	Dated capacity, hold/confirmation allocation, cancellation release and concurrency test	Confirmation succeeds without inventory
Money and POS	Server pricing, tax/fee rules, shift control, settlement and balanced reconciliation	Client controls price or raw card data is stored
Publication	Separate decision, source hash, consent/budget, provider acknowledgement and rollback	Status flag alone enables external publish
Department operations	Approved runbook, shift assignment, step evidence, exception and manager review	Paper-only daily process without outage rationale
Data and reports	Metric definition, source, freshness, reconciliation, filter and export permission	Decorative or invented KPI presented as live
Public launch	Responsive/accessibility check, legal notices, domain, SEO consent and contact/room fact approval	Unverified star rating or activated tags without consent
Recovery and release	Forward migration, backup/restore, rollback, monitoring and signed checkpoint	Unrehearsed migration or untraceable deployed source

37.12 Programme metrics

Outcome	Metric	Definition discipline
Distribution reliability	Acknowledged sync success, latency, stale inventory and reconciliation exceptions	Measure by provider, direction, property and time window
Direct demand	Search-to-room, room-to-checkout and checkout-to-confirmed conversion	Exclude controlled demo and failed/expired holds

Outcome	Metric	Definition discipline
Hotel performance	Occupancy, ADR, RevPAR, net channel revenue and contribution	Use recognised amounts and disclose commissions/refunds
Guest service	First response, resolution, SLA miss, recovery and satisfaction	Segment by channel/language without exposing direct identifiers
F&B operations	Acceptance, preparation, dispatch, delivery, cancellation, void and waste	Server timestamps and station ownership
Paper-to-digital adoption	Eligible workflows executed digitally and reconciled exceptions	Do not count legal/outage continuity forms as failure
AI quality	Acceptance, correction, groundedness, policy breach and rollback	Version by model, prompt, tool and evaluation set

37.13 Controlled dependencies and open decisions

- Confirm Sandralia room inventory, active rates, taxes, fees, cancellation and payment policies before enabling public checkout.
- Execute OTA/channel-manager agreements and obtain sandbox/production credentials, webhook rules and certification requirements.
- Select PCI-compliant payment providers and local methods; complete settlement, refund, dispute and reconciliation design.
- Approve Google property IDs, canonical production domain, consent categories, privacy notice and advertising eligibility before indexing or tag activation.
- Approve departmental owners, runbooks, delegation thresholds, retention classes, escalation paths and outage continuity forms.
- Confirm service-level, recovery, data-residency and commercial terms for translation, AI, messaging, ads and reputation providers.

37.14 RAHIS v8.3 Controlled Consolidated Release Candidate

Programme record: RAHIS has advanced through a v8.1 controlled operating core and two v8.2 components. Version 8.3 consolidates their product and activation governance; it does not claim that live payment, OTA, hardware, hotel-network or Sentinel production connections are commissioned.

Release fact	Controlled value	Decision significance
Release	RAHIS v8.3.0 controlled consolidated integration candidate	Consolidates the v8.1 operating core, v8.2 Paystack test adapter and v8.2 Sentinel overlay without changing their maturity labels.
Deployment	OpenAI Sites application delivery and D1 controlled data; repository commit 1abda50b1c07706ba79b10a63e92ce66344eaab8	The source baseline is traceable; the production deployment identifier and post-deployment checks must be recorded separately.
Access	Protected administration and explicitly authorised tenant/property roles	Protected access does not by itself establish hotel workforce IAM or public production.
Property truth	Sandralia Hotel by White Stones; Jabi, Abuja; verified 4-star and 102 rooms	Five-star remains the design/service-quality ambition, not a changed hotel rating.
Acceptance	Controlled code, configuration and sandbox/test evidence	Supports the release candidate; provider onboarding, hotel UAT and production sign-off remain separate.
Open exception	Live OTA, production payments, hardware, third-party APIs, Sentinel collectors and exact provider credentials remain uncommissioned.	Configure manually through RME 0.3 and activate only after contract, security/privacy, test, reconciliation and rollback gates.

Implemented and packaged release components

- v8.1 Sites/D1 operating core with controlled hotel workflows, tenant/property scope, audit and release boundaries.
- v8.2 Paystack adapter in test/sandbox mode with manual credential, callback, settlement and production-approval gates.
- v8.2 Sentinel overlay packaged as a disabled-by-default, signed, property-scoped and non-authoritative security bridge.
- ERP, SaaS and CRS configuration foundations use explicit systems of record, entitlements, approvals, reconciliation and migration controls.
- OTA, payment, messaging, maps, identity, locks, CCTV, biometrics, POS and other providers are registered manually and remain inactive until commissioned.
- Current controlled repository baseline: commit 1abda50b1c07706ba79b10a63e92ce66344eaab8; deployment identifiers and acceptance evidence belong in the release register.

P0 gates before live or commercial activation

Gate	Required next evidence	No-go boundary
One operational ledger	Confirm the authoritative Sites/D1 ledger and signed integration boundaries; document any future PHP/MySQL migration.	Do not operate competing D1 and PHP/MySQL inventory, folio, finance or payment ledgers.
Hotel workforce IAM	MFA, lifecycle, least privilege, role review, recovery and break-glass test.	Sites owner ingress is not a hotel staff identity system.
Full PMS/F&B	Complete PMS, F&B, ERP, SaaS and CRS UAT, including inventory, night audit, folio/payment, KDS/stock and reconciled finance.	Do not market a module as production-complete where the relevant operating, reconciliation or recovery gate remains open.
External providers	Register each provider manually; complete contracts, credentials, mappings, privacy/security review, sandbox/UAT, retry, reconciliation and rollback.	OTA, live Paystack/other payments, Google, ads, messaging, translation and hardware remain inactive until commissioned.
Commercial multi-tenancy	Composite tenant/property keys, isolation tests, lifecycle and per-tenant backup/restore.	Do not onboard a second customer into the pilot data model.
Public production	Browser/accessibility and content UAT; abuse controls; monitoring/recovery; domain/indexing; hotel sign-off.	Keep owner-only until these gates pass.

Cross-industry portfolio expansion outside the controlled RAHIS property boundary

Version 3.1 retains separate RME-powered industry directions. Each requires sector discovery, licensing, delivery ownership, configuration records and independent acceptance evidence before commercial activation.

Vertical pack	Approved product direction	Control boundary
Financial Services	Accounting, tax work, insurance/referral, consulting and periodic financial reporting/planning.	Regulated advice or services require licensed professionals/partners and approvals.
Professional Services	Consulting, coaching, training, projects, research/analysis and delivery control.	Credentials, confidentiality, expert sign-off and acceptance remain mandatory.
Manufacturing	ERP, MES, QMS, SCM and governed CAD/document interoperability.	Plant safety, engineering authority and approved quality systems remain controlling.
Distribution	Inventory, orders, warehouse, freight, delivery and analytics.	Stock, tax, carrier and proof-of-delivery transactions must reconcile.
Construction	Schedule, resources, cost, contracts/permits/drawings, field reports and safety.	Professional sign-off, permits, safety and contracts remain human-controlled.

The RAHIS completion and external-activation register is the required companion record for provider assets, department runbooks, paperless exceptions, release acceptance, rollback and live commissioning.

CONTROLLED CONCLUSION Version 3.1 authorises the RAHIS v8.3 controlled candidate and separate cross-industry RME product directions as governed programmes. It does not authorise uncontrolled provider publication, live payment/OTA claims, regulated professional activity without authority, or replacement of required human, legal, safety, finance and audit judgement.

SECTION 38 | Rihuum Sentinel AI Cybersecurity Suite and Integrated Defence Platform

38.1 Executive product decision

Rihuum Intercontinental Limited formally establishes the Rihuum Sentinel AI Cybersecurity Suite as the company-wide defensive cybersecurity product family. Sentinel AI is the central control plane. Each capability is separately licensable, tenant-scoped, authorised-use-only and evidence-driven through RME, RIA, Rihuum OS and Digital Ecosystem contracts.

This controlled update is executive-authorised for engineering, staging, commercial planning and Board ratification. It does not claim that all provider, device or managed-service capabilities are commissioned or generally available.

38.2 Platform hierarchy

Layer	Controlled role
Rihuum Intercontinental Limited	Owner, developer, operator, licensor and accountable governance authority.
Rihuum Digital Ecosystem	Corporate trust, product discovery, academy, customer workspaces, security status and support across the three domains.
RME	Shared organisations, identity, MFA, permissions, licensing, audit, RME 0.3 configuration, notifications, updates, backups, integrations and support.
RIA	Governed AI models, agents, knowledge, tools, evaluation, provenance, cost controls, human approvals and kill switches.
Rihuum Sentinel AI	Central cybersecurity command, authorisation, evidence, detection, response, posture and commercial module platform.
Collectors and adapters	Customer-controlled local observations and approved provider/device integrations; outbound and least privilege.
RAHIS v8.3 candidate	Hospitality system of record and consolidated release candidate; v8.2 Sentinel bridge remains signed, property-scoped, disabled by default and non-authoritative.

38.3 Sentinel AI operating principles

- Deny by default: no operation without authenticated identity, active tenant, permission, entitlement, verified asset, approved written authority, exact scope, valid window and matching execution tier.
- Defensive use only: no credential theft, malware, destructive payload, covert interception, arbitrary shell, unauthorised persistence or indiscriminate scanning.

- Human authority: AI is advisory by default; reversible consequential actions require recorded approval, idempotency, rollback and verification; irreversible autonomous action is prohibited.
- Evidence over confidence: source records, hashes, timestamps, provenance, correlation and chain of custody remain authoritative; AI confidence is explicitly labelled.
- Separation of systems of record: Sentinel does not become the operational ledger for payments, payroll, reservations, inventory, access control or biometrics.
- Portable delivery: shared-hosting control plane first, then isolated workers, hybrid bridges and cloud services as measured triggers require.
- Commercial truth: registered, implemented, configured, connected, tested, accepted and generally available are distinct product states.

38.4 Forty separately licensable defensive modules

Security family	Licensable modules
AI Security	RCSAISEC - AI, Agentic AI and Model Security
Application Security	RCSWEB - WebShield Website Security; RCSAPI - API and Mobile Application Security
Asset Protection	RCSSECURETRACK - SecureTrack AI Device and Asset Recovery
Automation	RCSAUTOMATION - SOAR and Governed Security Automation
Cloud Native Security	RCSCONTAINER - Container and Kubernetes Security
Cloud Security	RCSCLOUD - Cloud Security Posture and Workload Protection
Cryptographic Security	RCSCRYPTO - Cryptographic Agility, PKI and Post-Quantum Readiness
Data Security	RCSVAULT - Data Protection, DSPM and Secure File Vault
Detection Engineering	RCSDECEPTION - Deception and Honeypot Manager; RCSHUNT - Threat Hunting and Detection Engineering
Endpoint Security	RCSENDPOINT - Endpoint Guardian
Executive Assurance	RCSPOSTURE - Security Posture, Board Scorecard and Assurance Reporting
Exposure Management	RCSVASM - Vulnerability and Attack-Surface Manager; RCSATTACKPATH - Security Digital Twin and Attack-Path Intelligence
External Risk	RCSDIGITALRISK - Digital Risk and Brand Impersonation Protection
Fraud Defence	RCSFRAUD - Fraud and Transaction Security Intelligence

Security family	Licensable modules
Governance	RCSGRC - Compliance, Privacy and Risk Manager; RCSTPRM - Third-Party and Supply-Chain Risk Manager
Human Risk	RCSPHISH - PhishGuard Awareness and Simulation
Human and Identity Security	RCSINSIDER - Insider Risk and User Behaviour Analytics
Identity Security	RCSIDENTITY - Identity Threat Defence and Zero Trust Manager; RCSSECRETS - Secrets, API Key and Machine Identity Security
Incident Response	RCSINCIDENT - Incident Response and Digital Evidence Manager
Industry Security	RCSHOSPITALITY - Hospitality Cyber Defence
Managed Security	RCSMDR - Managed Detection and Response Operations
Messaging Security	RCSEMAIL - Email and Domain Security Manager
Mobile Security	RCSMOBILE - Mobile Device and Application Security
Network Security	RCSNETWORK - Network, Wi-Fi and IoT Security Auditor
Operational Technology	RCSSMARTSEC - Smart Security, OT and ICS Integration
Platform	RCSCORE - Rihuum Sentinel AI Core
Privacy	RCSPRIVACY - Privacy Operations and Data-Protection Automation
Product Security	RCSDEVSECOPS - DevSecOps and Software Supply-Chain Security
Resilience	RCSRANSOM - Ransomware Resilience and Backup Monitor; RCSBCM - Business Continuity and Cyber Resilience Manager
SaaS Security	RCSSAAS - SaaS Security Posture Manager
Security Operations	RCSSOC - Sentinel AI SOC and XDR
Threat Intelligence	RCSTHREAT - Threat Intelligence Manager
Training	RCSCYBERRANGE - Cyber Range and Ethical Hacking Laboratory
Workforce Security	RCSREMOTE - Remote Workforce and Collaboration Security

Maturity at v0.2.0-alpha: 23 module foundations, 14 adapter-required modules and 3 planned modules. Registration or navigation does not prove live operational depth. The Product Charter and release evidence record govern capability claims.

38.5 Scope Guardian and authorised assessment model

13. Verify customer identity, legal owner and asset ownership evidence.

14. Record written authorisation, permitted modules, actions, modes, dates, maintenance windows, data handling and emergency contacts.
15. Canonicalise and hash every target; reject credentials, query strings, malformed ranges and central access to private networks.
16. Validate the server-side module entitlement and exact assessment scope.
17. Match the operation to shared-control-plane, collector, hybrid, external-provider or lab-only execution tier.
18. Require separate approval for controlled intrusive validation or reversible response action.
19. Apply emergency stop, rate, concurrency, body/response, data-minimisation and retention controls.
20. Record actor, reason, target, policy decision, correlation reference, result, evidence and rollback status.

38.6 AI security and autonomous defence boundary

Capability	Allowed role	Mandatory boundary
Security copilot	Search, explain, summarise, draft, correlate and recommend	Role-filtered sources, citations/provenance, redaction and uncertainty.
Detection engineering	Generate or validate bounded read-only rule DSL	No shell or SQL execution; testing and approval lifecycle.
Evidence fusion	Combine confidence and corroboration from independent sources	Never replace source evidence or hide contradictory signals.
Security digital twin	Rank bounded attack paths from registered assets and relationships	No contact with assets unless a separately authorised assessment exists.
SOAR	Prepare or execute reversible approved actions	Dual control, exact connector, idempotency, rollback and post-check.
AI/agent security	Assess prompts, tools, memory, models, retrieval and automation	AISVS/ATLAS-aligned tests, kill switch and no secret exposure.

38.7 Data, evidence and privacy architecture

- Tenant and property context is server-derived; client-supplied tenant identifiers are never trusted for authorisation.
- Secrets are encrypted or represented by aliases/hashes; private keys, passwords, access tokens, full card data and raw biometrics are prohibited in ordinary events, evidence and AI prompts.
- Evidence includes hash, source, actor, timestamp, correlation, classification, retention, access history and legal-hold status.
- Incident, finding, risk and remediation records have explicit status transitions and accountable owners.
- Cryptographic inventory records algorithm, key length, expiry, dependency, deprecation and post-quantum transition status without collecting secret key material.

- Behaviour analytics uses minimised subject hashes and requires privacy review, proportionality, explainability and human investigation.

38.8 RAHIS Hospitality Cyber Defence integration

Integration element	Controlled behaviour
Direction	RAHIS sends minimised security events outbound through a durable outbox.
Authentication	Canonical JSON, HMAC-SHA-256, key ID, event ID, timestamp, replay and duplicate controls.
Scope	Tenant and property mapping; exact event allow-list.
Prohibited data	Passwords, tokens, private keys, card data, raw biometrics, session cookies, OTPs and recovery codes.
Authority	Sentinel responses are non-authoritative for hotel operations.
Local devices	ZKTeco, CCTV, smart locks and private network devices remain behind a hotel-local outbound bridge.
Commissioning	Backup/restore, migration, privacy/security review, signature/replay/idempotency, monitoring, rollback and signed hotel UAT.

38.9 Digital Ecosystem and domain integration

Domain/surface	Sentinel AI role
rihuum.com	Corporate trust, governance, partnerships, investor and general sales narrative.
rihuum.tech	Cybersecurity product catalogue, demos, Academy, secure onboarding and client workspace entry.
rihuum.net	Security status, infrastructure, managed operations, collector/edge documentation and service continuity.
platform.rihuum.tech	Authenticated RME 0.3 product and configuration control plane after explicit activation approval.
sentinel.rihuum.tech	Recommended dedicated Sentinel workspace when staging and operations are commissioned.
academy.rihuum.tech	Rihuum Technology and Digital Hub courses, cyber range and certification preparation.

38.10 Hosting and scale path

Stage	Placement	Exit or migration evidence
Shared hosting	Portal, licensing, scope, safe public checks, findings, incidents, GRC, reports, signed endpoints.	Clean install, backup/restore, security/performance tests and low-concurrency pilot.
VPS	Workers, queues, cache, managed database, object storage, central observability and blue/green release.	Queue/concurrency/integration volume or service-control trigger.
Hybrid	Cloud control plane plus customer-local collectors and hotel bridges.	Private-device integration, resilience, offline queue and data-local need.
Cloud/SaaS	Regional multi-tenant services, autoscaling, formal SRE, HA/DR and data-residency controls.	Portfolio scale, multi-country operation and defined SLOs.

38.11 Commercial editions and revenue model

Edition	Indicative composition
Foundation	Sentinel Core, posture, safe web/domain checks, incident/evidence, GRC and reporting.
Professional	Foundation plus exposure, email/domain, DevSecOps, phishing awareness, threat intelligence and automation foundations.
Enterprise	Professional plus commissioned endpoint/network/cloud/SaaS/identity/data modules, collectors and digital twin.
Hospitality	Enterprise profile plus Hospitality Cyber Defence and commissioned RAHIS/property bridge.
MDR	Licensed modules plus Rihuum analysts, SLA, escalation, response authority and managed operations.
Academy/Cyber Range	Isolated training tenancy, courses, labs, scoring and certificates; no real-world target authority.

38.12 Standards and assurance baseline

The Suite maps evidence and programme outcomes to NIST CSF 2.0, NIST SP 800-61 Rev. 3, NIST zero trust and SSDF guidance, NIST AI RMF/GenAI Profile, NIST post-quantum standards, OWASP ASVS 5.0.0, OWASP AISVS 1.0, MITRE ATT&CK 19.1, MITRE ATLAS, CISA KEV/Secure by Design, CIS Controls 8.1, PCI DSS 4.0.1, ISO/IEC 27001:2022 and the Nigeria Data Protection Act 2023/GAID 2025. Mapping supports implementation and evidence; it does not create certification or legal conclusions.

38.13 Release and no-go gates

- No Critical or High security defect remains open.
- Clean database install and controlled upgrade complete with reconciliation.
- Tenant, permission, entitlement, scope, approval and emergency-stop negative tests pass.

- Encrypted backup restoration succeeds within approved objectives.
- Collector and RAHIS signature, replay, revocation, offline and degraded-provider tests pass.
- No prohibited sensitive content appears in browser, logs, evidence, AI prompts or backups.
- SAST, DAST, dependency, secret, SBOM and independent penetration tests are accepted.
- Performance, accessibility, responsive and representative Nigerian connectivity tests pass.
- Operator runbooks, training, support, incident response, legal/privacy review and customer UAT are signed.

38.14 Current controlled status

The v0.2.0-alpha source is an engineering alpha and controlled staging candidate. Automated evidence covers 144 PHP files, 112 PHP tests, seven collector tests, four RAHIS bridge tests, 61 routes and 16 migrations. Live MySQL/MariaDB migration, Namecheap staging, restore, penetration, performance, provider and customer acceptance remain open. No public statement may describe the suite as a commissioned live service until those gates pass.

38.15 100-day execution mandate

21. Ratify this v3.0 controlled update and assign product, security, privacy, commercial and release owners.
22. Create the Sentinel staging subdomain/database, run clean install and restore evidence.
23. Commission the first Foundation edition and owned public-web posture workflow.
24. Pilot the RAHIS v8.3 candidate and its v8.2 Sentinel overlay with Sandralia in disabled-by-default staging mode.
25. Package and install the restricted collector on one authorised Rihuum test environment.
26. Complete independent application security review and remediate all Critical/High findings.
27. Publish accurate product pages, authorised-use terms, privacy notices, service descriptions and Academy curriculum.
28. Run a controlled SME/hospitality pilot and measure detection, remediation, usability, support cost and renewal evidence.

APPENDIX A | First 90-Day Action Register

Use: The CEO should convert this register into the approved work-management system, assign named individuals and budgets, and review completion evidence weekly.

Table 54. First 90-day actions

ID	Action	Accountable role	Due	Completion evidence
A0 1	Verify CAC profile, incorporation documents, directors/shareholding, beneficial ownership, registered office and annual-return status	Company Secretary / CEO	Day 15	Signed corporate-facts register and corrective filing plan
A0 2	Verify the separate CAC name/number and records for Rihuum Technology and Digital Hub	Company Secretary	Day 15	Verified certificate/profile and approved display value
A0 3	Secure domain registrar, DNS, hosting, email and social accounts with named owners, MFA and recovery custody	CTO / Security	Day 10	Asset/access register and recovery test
A0 4	Inventory every website, repository, application, client deployment, database, vendor, device, licence and dataset	CTO / PMO	Day 20	Complete classified asset/portfolio inventory
A0 5	Approve reserved decisions, executive roles, portfolio committee and Technology/Data/AI Council	Board / CEO	Day 20	Terms of reference, RACI and meeting calendar
A0 6	Approve top risks, risk appetite, incident authority and 90-day funding envelope	Board / CEO / Finance	Day 30	Board decision and funded action register
A0 7	Establish accounting close, cash forecast, receivables, procurement/payment control and product/project cost capture	Finance lead	Day 30	Reconciled opening dashboard and 13-week forecast
A0 8	Approve official brand asset repository, logo usage, legal/footer data and interim digital design tokens	Corporate Communications / Legal	Day 30	Versioned brand guide and templates
A0 9	Approve three-domain sitemap, canonical/redirect plan, content ownership, privacy/terms and analytics/consent design	Product / Marketing / Privacy	Day 30	Signed information architecture and content register
A1 0	Launch/refresh corporate, technology/Academy and operations foundations on rihuum.com, rihuum.tech and rihuum.net	Product / Engineering	Day 75	Production release, accessibility/security checks and analytics
A1 1	Set up approved repositories, branch protection, CI checks, environments, artefact releases, issue and documentation standards	Engineering lead	Day 30	Working pipeline and first controlled release
A1 2	Implement separate staging/production databases, protected secrets, monitoring, backups and a recorded restore test	Engineering / Service Ops	Day 45	Restore report and recovery runbook
A1 3	Approve RME and Rihuum OS product charters, platform hierarchy, modular architecture, tenant/data model, contracts, ADRs and first thin-slice workflow	Product / CTO	Day 35	Product briefs, diagrams, contracts, ADRs and accepted backlog

ID	Action	Accountable role	Due	Completion evidence
A1 4	Deliver and govern RME 0.3 Configuration Centre and the Rihuum OS thin slice: identity, tenant, roles, policy, audit, manual provider assets and support.	Engineering	Day 80	RME/OS controlled release, configuration schema, access review, test evidence, security review and operator documentation.
A1 5	Approve RIA policy, AI use-case register, model gateway design, agent authority levels and evaluation template	AI/Data lead / Security	Day 45	Approved AI governance pack
A1 6	Deliver one bounded, source-grounded internal knowledge assistant without autonomous system changes	AI/Product	Day 75	Evaluation, access, audit and pilot feedback
A1 7	Implement CRM pipeline, proposal/SOW controls, onboarding, service desk and customer-success ownership	Commercial / Service Ops	Day 60	One traceable prospect-to-support workflow
A1 8	Select one ideal customer segment and recruit paid lighthouse pilot(s) using qualification and risk gates	Commercial / Product	Day 75	Signed pilot, baseline, success metrics and delivery plan
A1 9	Approve Academy programme architecture, learner policies, instructor/assessment standards and first cohort business case	Academy director	Day 60	Programme pack, verified legal identity and launch decision
A2 0	Baseline enterprise KPIs and submit 12-month operating plan, budget, prices and migration decision to the board	CEO / Finance / PMO	Day 90	Reconciled scorecard and board-approved annual plan

APPENDIX B | Governance and RACI Matrix

R = Responsible (does the work); A = Accountable (one final owner); C = Consulted; I = Informed. Role names may be held by one person during the lean stage, but accountability must remain explicit.

Table 55. Enterprise decision RACI

Decision/activity	Board	CEO	Product	CTO/Eng	Security/Privacy	Finance	Commercial	Service Ops
Strategy and risk appetite	A	R	C	C	C	C	C	I
Annual portfolio and budget	A	R	C	C	C	R	C	I
Product discovery/roadmap	I	A	R	C	C	C	C	C
Architecture/technology standard	I	C	C	A/R	C	I	I	C
Security/privacy risk	I	C	C	R	A/R	I	I	C
AI/Agentic authority	I/A*	A	R	R	R	C	I	C
Price and packaging	I	A	R	C	C	R	R	C
Client contract/deviation	I	A	C	C	C	C/R	R	C
Production release	I	I	A	R	C	I	I	C
Major incident	I	A	I	R	R	C	C	R
Country/regulated market entry	A	R	C	C	C	C	R	C
Product sunset	I/A*	A	R	C	C	C	C	R

*Board accountability applies when the decision exceeds delegated authority, risk appetite, material capital or major client/market commitment.

Reserved board matters - proposed

- Strategy, annual budget and capital/funding transactions outside delegated limits.
- New country, regulated business, acquisition/disposal, major joint venture or material IP transfer.
- Risk appetite, major unresolved breach/incident, material litigation and public regulatory commitment.
- Appointment/removal and remuneration of senior executives, significant borrowing/security and related-party transactions.
- Material product/platform discontinuation or change that threatens contractual continuity or reputation.

APPENDIX C | Architecture Principles and Decision Standards

Table 56. Architecture principles

Principle	Decision test
Business outcome first	Which user/business outcome and metric justify this component or complexity?
Modular monolith first	Can a clean module boundary solve the problem before a distributed service?
Secure/private default	Is the safest reasonable configuration enabled without expert client action?
Least privilege and explicit trust	Which identity needs which action, data and duration, and how is it verified/audited?
Tenant isolation	Can any code, query, file, cache, job, log or AI context cross an organisation boundary?
Portable interfaces	Can storage, provider, host or model change through an adapter/configuration rather than product rewrite?
Backward-compatible evolution	Can the system expand, migrate, switch and contract without unsafe big-bang change?
Observable and operable	Can operators detect, diagnose, support, restore and explain the component?
Accessible/responsive	Does the primary journey work across relevant screens, keyboard and assistive technologies?
Data minimisation and lifecycle	Why is each field/event retained, who owns it and how is it corrected/exported/deleted?
Governed intelligence	Are model, knowledge, memory, tool, authority, evaluation and human accountability explicit?
Buy/build/partner discipline	Is this capability differentiating, and are total lifecycle cost and exit options understood?

Architecture Decision Record template

- Title, identifier, status, date, owner and reviewers.
- Context, decision drivers, constraints and measurable quality attributes.
- Options considered, including do nothing/buy/partner, with security, privacy, cost and operations.
- Decision and rationale; consequences, trade-offs and risks.
- Implementation/migration/rollback; monitoring and review trigger.
- Linked threat model, DPIA, product requirement, release and superseding ADR.

APPENDIX D | Policy, Process, and Documentation Register

Table 57. Minimum controlled-document roadmap

Document/control	Owner	Priority	Review
Corporate facts and statutory obligations register	Company Secretary	Immediate	Monthly/trigger
Delegation of authority and reserved matters	Board/CEO	Immediate	Annual
Enterprise risk and exception policy	CEO/Risk	Immediate	Quarterly
Information security policy and control baseline	Security/CTO	Immediate	Annual/trigger
Data protection/privacy governance and processing register	Privacy/Legal	Immediate	Quarterly/trigger
Incident response and breach procedure	Security/Privacy	Immediate	After exercise/incident
Business continuity and disaster recovery plan	Service Ops	Immediate	Annual/trigger
Backup, restoration and retention standard	CTO/Service Ops	Immediate	Six-monthly
Product governance and lifecycle policy	Head of Product	90 days	Annual
Secure SDLC, repository and release standard	Engineering/Security	Immediate	Six-monthly
Architecture principles and ADR process	CTO	Immediate	Annual
AI/Agentic AI governance and acceptable-use policy	AI Council	Immediate	Quarterly/trigger
AI/model/prompt/tool/evaluation register	AI/Data lead	90 days	Continuous
Vendor, open-source and supply-chain policy	Procurement/CTO	90 days	Annual
Access control and joiner-mover-leaver process	People/Security	Immediate	Quarterly
Asset, device and software licence policy	IT/Finance	90 days	Quarterly
Client onboarding, deployment and offboarding playbook	Service Ops	90 days	Six-monthly
Support, severity, SLA and maintenance policy	Service Ops	90 days	Six-monthly
Pricing, discount and commercial approval policy	Finance/Commercial	90 days	Quarterly
Contract templates and deviation matrix	Legal/Commercial	Immediate	Annual/trigger
Marketing claims, content and social governance	Marketing/Legal	90 days	Six-monthly
People handbook, conduct, performance and learning	People	90 days	Annual
Academy curriculum, assessment and credential policy	Academy	90 days	Each programme
Financial close, procurement and payment controls	Finance	Immediate	Annual
KPI dictionary and data-quality standard	PMO/Data	90 days	Quarterly

APPENDIX E | Source and Evidence Register

Source policy: The sources below support the external legal, governance and engineering references used in this blueprint. They do not certify Rihuum's compliance. Laws, regulator guidance and standards change; authorised owners must verify the current official text before relying on it for a transaction or launch.

- S1. Corporate Affairs Commission - official Nigerian corporate registry and CAMA 2020 context.** [Open official source](#)
- S2. Nigeria Data Protection Commission - Nigeria Data Protection Act 2023.** [Open official source](#)
- S3. Nigeria Data Protection Commission - NDP Act objectives and official FAQs.** [Open official source](#)
- S4. Nigeria Data Protection Commission - official resources and current guidance register.** [Open official source](#)
- S5. Startup Nigeria - official Startup Support and Engagement Portal and Nigeria Startup Act overview.** [Open official source](#)
- S6. Startup Nigeria - current portal terms and labelled-startup obligations.** [Open official source](#)
- S7. Federal Competition and Consumer Protection Commission - official mandate.** [Open official source](#)
- S8. NIST Cybersecurity Framework 2.0.** [Open official source](#)
- S9. NIST AI Risk Management Framework - Generative AI Profile (NIST AI 600-1).** [Open official source](#)
- S10. CISA - Secure by Design principles and manufacturer responsibility.** [Open official source](#)
- S11. OWASP Application Security Verification Standard (ASVS).** [Open official source](#)
- S12. OWASP Agentic AI - Threats and Mitigations.** [Open official source](#)
- S13. OWASP Top 10 for Agentic Applications.** [Open official source](#)
- S14. OWASP IoT Security Verification Standard.** [Open official source](#)
- S15. Semantic Versioning 2.0.0.** [Open official source](#)
- S16. ISO/IEC 27001:2022 - Information security management systems.** [Open official source](#)
- S17. ISO/IEC 27701:2025 - Privacy information management systems.** [Open official source](#)
- S18. ISO 22301:2019 - Business continuity management systems.** [Open official source](#)
- S19. ISO/IEC 42001:2023 - Artificial intelligence management system.** [Open official source](#)
- S20. ISO 9001:2015 - Quality management systems (monitor the announced revision).** [Open official source](#)

All online sources were checked on 22 July 2026. Rihuum-specific corporate facts are company-supplied and board-approved; reconcile them to official records during Action A01/A02.

APPENDIX F | Glossary

Table 58. Key terms

Term	Meaning in this blueprint
ADR	Architecture Decision Record: a controlled explanation of a consequential technical decision and its trade-offs.
Agentic AI	AI software that plans and performs multi-step work using knowledge, memory and tools within an authority model.
API	Application Programming Interface: a documented software contract for exchanging data or actions.
BIA	Business Impact Analysis: identification of priority activities, disruption impacts and recovery needs.
CI/CD	Automated continuous integration and controlled delivery/deployment of tested, traceable release artefacts.
CRM	Customer Relationship Management: account, contact, opportunity, activity, service and lifecycle records.
DPIA	Data Protection Impact Assessment for processing likely to create high privacy risk.
ERP	Enterprise Resource Planning: integrated operational and financial processes such as procurement, inventory and projects.
Feature flag	A governed switch that enables controlled rollout or shutdown of a capability without changing the release artefact.
GA	General Availability: a product/feature that is priced, documented, supported and approved for production use.
HRIS	Human Resources Information System for workforce records, processes and reporting.
IAM	Identity and Access Management for accounts, authentication, roles, permissions and lifecycle.
Idempotent	Safe to retry without causing unintended duplicate effects.
LMS	Learning Management System for programmes, content, cohorts, assessment and learner administration.
Modular monolith	One deployable application whose internal business modules have explicit boundaries and contracts.
Multi-tenancy	One platform serving multiple organisations while enforcing tenant-specific data, access and configuration.
PWA	Progressive Web Application: a responsive web experience that can support app-like capabilities where appropriate.
RIA	Rihuum Intelligence Architecture: the governed AI/model, knowledge, agent, tool, approval, evaluation and audit layer.
RME	Rihuum Master Enterprises: Rihuum's shared multi-tenant enterprise core and product control plane for identity, tenancy, master records, workflow, commercial controls, integrations, audit, support and product lifecycle operations.
Rihuum OS	Rihuum's unified enterprise and industry operating experience and product family powered by RME; initially a business platform, not a desktop OS.
RPO	Recovery Point Objective: target maximum period of data loss after disruption.

Term	Meaning in this blueprint
RTO	Recovery Time Objective: target time to restore an activity or service after disruption.
SBOM	Software Bill of Materials: inventory of software components in a release.
SemVer	Semantic Versioning using MAJOR.MINOR.PATCH rules for a declared public interface.
SLA	Service Level Agreement: contractual service commitments and remedies within a defined scope.
Tenant	An organisation/customer boundary within a shared platform.
Thin slice	The smallest end-to-end capability that can be used and evaluated across interface, logic, data and operations.
UAT	User Acceptance Testing: recorded validation that the solution meets agreed business needs.

APPENDIX G | Open Decisions and Verification Register

Control: The blueprint is complete without guessing unknown facts. The items below must be resolved through authorised company records, budgets, advisers or measured baselines and then inserted through controlled document change.

Table 59. Open items

ID	Item	Required source/decision	Owner	Target
V01	Rihuum Technology and Digital Hub exact CAC registration number/legal form	CAC certificate/profile and company-secretary verification	Company Secretary	Day 15
V02	Exact registered street address, public correspondence address and Google Maps Place ID	Abuja, Nigeria is confirmed only as the registered locality; verify the precise address and Place ID from CAC/board-approved and Google records.	Company Secretary	Day 15
V03	Current directors, shareholders, beneficial owners and statutory filing status	Corporate registers and CAC reconciliation	Company Secretary	Day 15
V04	Tax identifiers, filing status and applicable tax treatment	Qualified tax adviser and authority records	Finance	Day 30
V05	Trademark/IP registrations and chain of title for logo, software, content and domains	IP audit, assignments and official searches	Legal / CTO	Day 45
V06	Exact Namecheap plan, runtime, storage, database, cron, backup, SSH and security limits	Hosting account evidence and test	CTO	Day 10
V07	Current products, repositories, client deployments, commitments and support status	Portfolio/asset inventory	PMO / CTO	Day 20
V08	Approved first RME-powered Rihuum OS ideal customer and lighthouse workflow	Discovery, commercial and portfolio decision	Product / CEO	Day 45
V09	Annual budget, funding envelope, cash/runway and investment priorities	Reconciled finance and board approval	Finance / Board	Day 90
V10	Price book, discounts, support packages and contractual SLAs	Cost/market research and board-delegated approval	Finance / Commercial	Day 90
V11	KPI baselines and numeric targets	90-day reconciled measurement and annual plan	PMO / Finance	Day 90
V12	Named DPO/privacy, security, AI-risk and incident authorities	Executive appointment and legal/risk assessment	CEO	Day 20
V13	Official social accounts and authorised administrators	Account verification and access register	Marketing / Security	Day 15
V14	Formal brand palette/type system and logo master/vector files	Board-approved brand guide derived from official emblem	Marketing / Board	Day 60
V15	Markets/products requiring specific licences or accreditation	Offering-by-offering counsel/regulator review	Legal / Business unit	Before launch

ID	Item	Required source/decision	Owner	Target
V16	Activate and test proposed role-based email inboxes	Namecheap mailbox/forwarder creation, SPF/DKIM/DMARC alignment, delivery tests and ownership register	IT / Security / Corp. Comms.	Before public use
V17	Confirm the authorised public name, title and biography for the supplied leadership portraits	Board/HR-approved leadership profile and publication approval	CEO / Corp. Comms.	Before named publication
V18	Prioritise the expanded sector and product portfolio	Nigeria/Africa discovery evidence, capacity plan, regulatory screen, budget and portfolio decision	Portfolio Committee	Quarterly gate
V19	Digital discovery and advertising identifiers	GA4 G-CLFV1L0KVJ is confirmed for rihuum.tech; obtain and verify .com/.net GA4, GTM, Search Console, AdSense and seller values.	Marketing / Privacy / CTO	Before activation
V20	External provider and API assets	Register contract, environment, public identifiers, protected secrets, mappings, webhooks, tests, monitoring, rollback and production approval in RME 0.3.	Product / Security / Service Ops	Per provider

Controlled completion

When an item is verified, attach the authoritative evidence, record the approver and effective date, update affected websites/templates/contracts/systems, increment this document version as appropriate and retain the superseded copy. No employee or vendor may fill an unknown field with an assumed number, address, certification or licence.



Figure 4. Official Rihuum Intercontinental Limited logo

Rihuum Intercontinental Limited | RC 1476119
rihuumconsult@gmail.com | 09162102777 | 08082407830 | 07031321663
 Built and Developed by Rihuum Intercontinental Limited - www.rihuum.tech

APPENDIX H | Nigeria and Africa Market and Portfolio Expansion

Control: This appendix expands the approved portfolio map using current official and industry evidence. It does not authorise simultaneous development of every named direction. Each product or sector must pass customer, capability, legal, security, commercial and lifecycle gates before investment or sale.

Purpose and strategic interpretation

Nigeria is the reference market for Rihuum's first repeatable products and services; selected West African and wider African corridors follow only after delivery evidence. The opportunity is not simply that more organisations will come online. It is that businesses, institutions and communities need secure operating systems adapted to mobile access, affordability, fragmented workflows, local payment rails, field work, language diversity, trust and regional trade.

Evidence-led market signals

\$240 billion mobile contribution

Evidence: GSMA reports that mobile technologies and services contributed \$240 billion, or 7.8% of African GDP, in 2025.

Rihuum response: Design mobile access, service APIs, identity and payments as platform capabilities.

63% mobile-internet usage gap

Evidence: GSMA estimates that 63% of Africans live within mobile-broadband coverage but are not using mobile internet.

Rihuum response: Treat low-data, affordability, skills, accessibility and relevant content as adoption requirements.

Nigeria Payments System Vision 2028

Evidence: The CBN's current vision is organised around interoperability, security, inclusion, innovation, trust and collaboration.

Rihuum response: Integrate licensed payment providers through replaceable adapters, reconciliation and audit; do not imply an unlicensed payment role.

300,000 initial 3MTT learners

Evidence: Nigeria's 3MTT programme states that its first two phases cover 300,000 learners across technical disciplines.

Rihuum response: Connect Rihuum Technology and Digital Hub programmes to practical projects, portfolio evidence and employer outcomes.

AfCFTA digital-trade direction

Evidence: The African Union adopted the AfCFTA Protocol on Digital Trade in February 2024 to support secure, trustworthy and interoperable digital trade.

Rihuum response: Build configurable country, currency, language, document and integration layers, with corridor-specific legal validation.

Nigeria National AI Strategy 2025

Evidence: NCAIR/NITDA presents responsible AI, local-language capability, skills, research and commercialisation priorities.

Rihuum response: Evaluate local context, languages, bias, cost, connectivity, security and human authority before AI release.

NDP Act and GAID 2025

Evidence: Nigeria's data-protection regime requires operational attention to purpose, risk, controller/processor duties and privacy-impact assessment.

Rihuum response: Make privacy and data governance part of discovery, architecture, supplier management, release and support.

Portfolio expansion scale

Table 60. Controlled v2.2 portfolio scale

Portfolio layer	v2.2 controlled direction
Shared platform	RME enterprise core; Rihuum OS operating experience; RIA governed intelligence
Shared application suites	8: operations; people/learning; finance; customer/commerce; projects/service; assets; data; governance/trust
Industry directions	31 named sector suites plus one custom-sector discovery route
Products/platforms	16 controlled foundation, service, discovery and planned directions
Services	14 commercial service lines spanning engineering, AI, trust, infrastructure, industry delivery, research, commerce and venture building

Expanded industry suite register

Table 61. Named sector families and controlled coverage

Sector family	Named suite directions
Enterprise and markets	Enterprise/SME; retail/commerce/distribution; consumer goods/FMCG; cooperatives/associations; artisans/gig/field-service networks
Government and society	Government/public service; public finance/revenue administration; education/workforce; nonprofit/development; faith/community institutions
Health and wellbeing	Health/life sciences; pharmaceutical/medical supply chain; sports/fitness/wellness
Finance and professional services	Banking/finance/insurance; professional/legal services; diaspora/global-community services
Production and resources	Agriculture/food; manufacturing/industrial; energy/utilities; extractives/natural resources; climate/environment/circular economy
Movement and trade	Logistics/transport/mobility; travel/tourism/aviation; automotive/service networks; maritime/ports/blue economy; cross-border trade/export/AfCFTA
Places, services and infrastructure	Hospitality/property/events; construction/real estate/facilities; telecommunications/service providers; security/safety/emergency
Culture and specialist work	Media/creative/entertainment; custom sector solutions

New product directions added in v2.2

- Rihuum MarketFlow — mobile-first MSME, merchant, cooperative and distributor operations.
- Rihuum TradeBridge Africa — trade counterparties, product/document records, logistics milestones and export readiness.
- Rihuum CivicFlow — authorised public-service requests, cases, permits, programmes, assets and accountable reporting.
- Rihuum FieldOps — offline-tolerant assignments, forms, inspections, evidence and supervisor command.
- Rihuum TrustGraph — consent, obligations, controls, approved identity-provider integrations, evidence and incidents.
- Rihuum African Language and Knowledge Layer — evaluated language, speech, translation and local-knowledge adapters; no universal coverage claim.
- Rihuum Resilience and Sustainability Platform — energy, water, waste, environmental risk, interventions and impact evidence.

Africa-by-design product requirements

- Mobile-first, responsive, accessible and low-data by default.
- Offline-tolerant field workflows with conflict-safe synchronisation and supervisor review.
- Replaceable SMS, email, messaging, USSD and voice adapters only where the use case and provider terms justify them.
- English-first current delivery with evaluated Nigerian and African language pathways; no unsupported language claims.
- Multi-currency, multi-country and licensed-payment-provider integration with reconciliation and audit.
- Tenant isolation, least privilege, purpose limitation, retention, consent where applicable and auditable human authority.
- Data-location and cross-border transfer decisions made per client, country, contract and risk.
- Power, device sharing, intermittent networks and field-support constraints included in testing and recovery design.
- API-first integration with government, financial, telecom, logistics and industry partners; adapters remain replaceable.
- Progressive hosting from the current application platform to managed cloud, VPS, hybrid or client infrastructure only when triggers justify it.
- No autonomous high-impact decision without authority boundaries, evaluation, monitoring and human review.
- Commercialisation begins with one costly workflow and measurable proof—not a simultaneous build across every sector.

Immediate 90-day expansion sequence

29. Confirm three priority Nigerian customer segments and one lighthouse workflow per selected segment.
30. Score all expanded suite directions for urgency, reachable buyer, Rihuum right-to-win, regulation, data, delivery capacity, recurring revenue and platform reuse.
31. Choose one RME-powered Rihuum OS thin slice and one revenue-ready service package; pause the rest at discovery status.
32. Interview customers and delivery partners across at least three relevant Nigerian regions and one West African corridor before regional claims.
33. Prototype low-data and offline journeys on representative Android devices and constrained networks.
34. Validate Nigerian privacy, sector, payment, telecom/device, tax and contracting requirements with qualified specialists.
35. Measure adoption, support load, unit cost, reliability, security and willingness to pay before expanding modules.
36. Quarterly, stop, partner, defer or fund each direction using recorded evidence and portfolio capacity.

Evidence sources added in v2.2

- S21.** GSMA, The Mobile Economy Africa 2026. [Open official source](#)
- S22.** Nigerian Communications Commission, industry statistics. [Open official source](#)
- S23.** Central Bank of Nigeria, Payments System Vision 2028. [Open official source](#)
- S24.** Federal Ministry of Communications, Innovation & Digital Economy, 3MTT. [Open official source](#)
- S25.** African Union, AfCFTA Protocol on Digital Trade. [Open official source](#)
- S26.** NCAIR / NITDA, National AI Strategy and programmes. [Open official source](#)
- S27.** Nigeria Data Protection Commission, NDP Act implementation and DPIA guidance. [Open official source](#)
- S28.** African Union, Digital Transformation Strategy for Africa 2020–2030. [Open official source](#)

APPENDIX I | Corporate Communications, Email and Visual Media Register

Control: The active addresses below are company-confirmed. Proposed addresses are not presented as operational until Namecheap creation, delivery testing, ownership and security controls are complete. The user expressly reaffirmed on 23 July 2026 that the six supplied portraits may be used independently and that the recognisable likeness may appear as one individual in Rihuum's approved static and cinematic ecosystem media, subject to the safeguards in this appendix.

Confirmed active email addresses

Table 62. Active domain email register

Domain / channel	Public address	Administrative address	Primary use
rihuum.com	info@rihuum.com	admin@rihuum.com	Corporate, commercial and general enquiries
rihuum.tech	info@rihuum.tech	admin@rihuum.tech	Products, AI, Academy and technical enquiries
rihuum.net	info@rihuum.net	admin@rihuum.net	Client operations, infrastructure and service enquiries
Continuity	rihuumconsult@gmail.com	—	Fallback and transition continuity; not the preferred branded identity
Finance issuance	finance@rihuum.com	Authorised finance issuer	Controlled invoices and authorised finance records
Payment recording	payment@rihuum.com	Authorised payment recorder	Payment evidence, allocation and reconciliation
Finance approval	account@rihuum.com	Separate finance approver	Independent approval and finance-control segregation

Proposed role-based inboxes

Table 63. Create and test before public use

Proposed address	Purpose
sales@rihuum.com	Qualified commercial and proposal enquiries
partnerships@rihuum.com	Vendors, alliances, investors and institutional partnerships
careers@rihuum.com	Recruitment and talent enquiries
legal@rihuum.com	Contracts, notices and intellectual-property correspondence
privacy@rihuum.com	Data-subject requests and privacy governance
academy@rihuum.tech	Rihuum Technology and Digital Hub programmes
products@rihuum.tech	Product discovery, licensing and technical partnerships

Proposed address	Purpose
support@rihuum.net	Client service requests and managed support
security@rihuum.net	Responsible security reports and security operations
billing@rihuum.net	Invoices, subscriptions and account administration

Email operating rules

- Publish info@ addresses for general use; keep admin@ addresses limited to authorised administration and recovery.
- Assign an accountable owner and backup owner to every mailbox or forwarder; prohibit shared passwords and require multi-factor authentication where supported.
- Preserve and validate MX, SPF, DKIM and DMARC records when connecting Namecheap domains to the application host; website DNS changes must not silently break email.
- Route support, privacy, security, billing and legal correspondence into controlled queues with acknowledgement, retention, escalation and access rules.
- Use group aliases/forwarders when several people need a role address; remove access promptly when responsibilities change.
- Test inbound, outbound, reply, forwarding, spam placement and recovery before publishing any proposed address.

Authorised leadership portraits and likeness use

- Approved source set: six company-supplied photographs received 22 July 2026; independent use and approved identity-preserving derivatives were expressly reaffirmed on 23 July 2026. Preserve each photograph as an independent source asset in the controlled media library.
- Approved derivative use: the user's recognisable face may be placed on a naturally proportioned body as one individual within Rihuum corporate, Academy, infrastructure, industry and cinematic team scenes.
- Do not fabricate credentials, named client participation, awards, event attendance, regulated professional status or endorsements that are not supported by company records.
- Do not create synthetic voice, political messaging, financial instructions, legal authorisation or high-impact impersonation from the likeness without a separate explicit approval and security review.
- Keep source, prompt/edit brief, output, approval, publication location and retirement status in the digital asset register; remove obsolete or unauthorised derivatives.
- Use accurate alternative text, strip unnecessary device/location metadata and keep the person as part of Rihuum's human-centred story rather than as an unsupported performance claim.

Cinematic media and hosting placement

Table 64. Current media placement and limits

Component	Current decision	Migration / control rule
Web applications	OpenAI Sites application delivery with D1 controlled application data	Keep source and migrations portable; record release/rollback evidence and move only when measured reliability, isolation, data, job or scale triggers justify it.
Domains and DNS	Namecheap registrar and authoritative DNS	Use approved canonical/redirect records and preserve MX, SPF, DKIM, DMARC and mailbox continuity.
Email	Namecheap domain email plus Gmail continuity	Validate MX/SPF/DKIM/DMARC and ownership after every DNS change
Cinematic videos	Optimised muted MP4 loops on the application host/CDN	Poster images, preload metadata, pause control, reduced-motion fallback and strict asset budget
Sentinel AI staging candidate	PHP/MySQL v0.2.0-alpha package; bounded Namecheap-compatible staging candidate	Not the current public Sites/D1 runtime; no live-service claim until install, restore, security, performance, provider and customer acceptance pass.
Operational media	External/object/specialist storage when required	Lifecycle, access, encryption, retention, monitoring and recovery must match risk

S29. Namecheap, shared-hosting audio/video policy. [Open official source](#)

S30. Namecheap, shared-hosting resource restrictions. [Open official source](#)

S31. Namecheap, shared-hosting plans comparison. [Open official source](#)

S32. Namecheap, connecting a domain to third-party hosting. [Open official source](#)

v3.1 controlled conclusion

Rihuum's future-facing ambition is expressed through a governed opportunity map, not uncontrolled simultaneous delivery. The operating priority is a verified corporate foundation, reusable RME and Rihuum OS contracts, governed RIA intelligence, controlled manual configuration, revenue-ready services, accepted lighthouse workflows and evidence-based decisions to activate, migrate, pause or retire capabilities.

CONTROLLED CLOSING RECORD | Version 3.1

Controlled conclusion: Version 3.1 consolidates the verified corporate foundation, current Digital Ecosystem runtime, RME 0.3 configuration governance, RAHIS release components and Sentinel staging boundary. It is a controlled execution authority, not evidence that unregistered assets, third-party services or production integrations are active.

Authoritative platform and release baseline

- Rihuum Master Enterprises (RME) is the only current name for the shared enterprise control plane. RETP is retained solely as a superseded historical alias and must not appear in current product naming.
- The public Digital Ecosystem currently uses OpenAI Sites for application delivery and D1 for controlled application data. Namecheap remains the registrar, authoritative DNS and domain-email provider.
- RME 0.3 Configuration Centre is the governed manual-input surface for public identifiers, provider references, environment settings and activation evidence. Secret values require protected server-side storage.
- RAHIS v8.3.0 is the controlled consolidated integration candidate comprising the v8.1 operating core, v8.2 Paystack test/sandbox adapter and v8.2 Sentinel security overlay. Component maturity remains explicit.
- Sentinel AI v0.2.0-alpha remains a Namecheap-compatible engineering alpha and staging candidate. Its PHP/MySQL package is not represented as the current public Sites/D1 production runtime.

Manual configuration and activation governance

1. Register the asset, provider account, contract, owner, environment and permitted purpose.
2. Classify each value as public identifier, sensitive configuration or secret credential.
3. Enter public values through RME 0.3; store secrets only in protected server-side configuration or an approved vault.
4. Keep the feature disabled until validation, privacy/security review, sandbox testing and rollback evidence are complete.
5. Record activation time, approver, test result, monitoring owner, rotation date and decommissioning method.
6. Display “Not configured” or “Pending verification” when a value is absent; never insert fabricated placeholders.

Verified company data and reserved facts

- Verified entity: Rihuum Intercontinental Limited, RC 1476119, incorporated 6 March 2018.
- Registered-office locality supplied by the company: Abuja, Nigeria.
- Authorised finance workflow addresses: finance@rihuum.com for issuance, payment@rihuum.com for recording and account@rihuum.com for separate approval.
- The exact registered street address, public correspondence address, Google Maps Place ID and map pin remain unverified and must not be inferred from the Abuja locality.
- Rihuum Technology and Digital Hub is company-confirmed as CAC-registered, but its exact CAC number and legal form remain reserved pending certificate/profile verification.

Digital discovery and publishing status

- Confirmed GA4 measurement ID: G-CLFV1L0KVJ for rihuum.tech only.
- GA4 identifiers for rihuum.com and rihuum.net, the GTM container, Search Console verification values, approved AdSense publisher/seller values and Maps API/Place ID remain manual activation inputs.
- Search, advertising and maps integrations may be enabled only after account ownership, consent, privacy, content, domain, security and production tests are recorded.

Completion truth and open gates

Current completion boundary: the architecture, configuration surfaces and controlled release candidates are established. Live OTA/channel connections, production payment processing, hotel hardware, third-party APIs, Sentinel collectors, customer UAT, penetration testing, recovery rehearsals, exact legal identifiers and formal production sign-off remain provider- or evidence-dependent gates. No document or website may convert a configured, packaged or test-mode capability into a live-operation claim.

Forward roadmap

- Near term: complete asset registration, RME 0.3 configuration records, provider sandboxes, release evidence and first controlled customer acceptance.
- Scale trigger: move workers, queues, high-volume integrations or stronger isolation to VPS/managed services when measured reliability, security or capacity thresholds require it.
- Hybrid stage: keep customer-local collectors and hotel bridges outbound-only while central governance remains tenant-scoped and auditable.
- Long term: adopt regional cloud/SaaS, HA/DR, data-residency and formal SRE controls only when commercial scale and service objectives justify them.

Version 3.1 controlled conclusion

Rihuum can evolve without rebuilding its foundation when every product reuses RME contracts, separates systems of record, keeps intelligence within explicit authority, records manual configuration as controlled data, and treats commissioning evidence—not ambition—as the boundary of every public claim.