

YANDI AG / CONTROLLED WORKING PUBLICATION

YandiOS™ Complete Report

Institutional operating architecture for secure, traceable and scalable medicinal agriculture

REPORT POSITION	A consolidated strategic, technical, compliance and commercial blueprint. YandiOS is presently a proposed architecture and research programme; it is not represented as deployed, certified or regulator-approved.

Owner	Principal author	Edition	Reference date
Yandi AG	Maxwell Moore	Complete Report v1.0	2 September 2026

From the first acre forward.

GOVERNANCE

Document control and reading rule

Field	Record
Document title	YandiOS Complete Report
Owner	Yandi AG
Principal author	Maxwell Moore
Purpose	Define the current YandiOS proposition, system boundaries, reference architecture, controls, commercial logic and staged development pathway.
Status	Controlled working report - design/reference stage
Distribution	Founder, advisers, prospective strategic partners, government and controlled diligence recipients
Review cycle	At every material design gate; otherwise quarterly during development
Supersession	Future approved revisions supersede this edition; prior editions remain in the document register.

TRUTH RULE

Evidence takes precedence over enthusiasm. A concept is not a prototype; a prototype is not an operating system; an internal control is not certification; and regulator engagement is not approval.

Important limitations

- This report is not legal, regulatory, engineering, investment or cybersecurity advice.
- Security details are deliberately architectural. Site-specific positions, thresholds, response timings, vulnerabilities, credentials and network diagrams belong in restricted annexes.
- Economic figures are management scenarios unless independently validated by contracts, audited costs and demonstrated field performance.
- The YandiOS™, CropSecure™, CropFingerprint™, GridSecure™, GeoSpatialEngine™ and Growing Partners™ names are project designations; the ™ symbol does not represent registered status.

Executive summary

YandiOS is the evidence and coordination layer that makes a distributed medicinal-agriculture network governable without requiring Yandi AG to own every acre.

Current position. YandiOS has a coherent doctrine, named subsystem portfolio, field-security reference architecture, data and workflow concepts, an IP register and a 50-acre validation pathway. The available evidence does not yet establish production software, completed integrations, regulator acceptance, certifications, customers or recurring software revenue.

Strategic value. Its strongest proposition is the unification of five control problems that are normally fragmented: partner operations, geospatial security, crop/batch provenance, quality/compliance evidence and commercial handoffs. That makes YandiOS more than farm-management software and more than a perimeter alarm system.

Conclusion	Assessment	Implication
Strategic coherence	Strong	Preserve the Codex-to-system hierarchy and a single evidence chain.
Technical maturity	Early design	Build the smallest auditable identity/event/workflow prototype before broad features.
Regulatory fit	Plausible, unapproved	Use ODC requirements and site-specific specialist advice as design inputs; never claim acceptance early.
Commercial readiness	Unvalidated	Treat software, security and provenance revenue as hypotheses to be tested independently.
Defensibility	Emerging	Control names, schemas, methods, decision records and evidence; pursue registrations and contracts deliberately.

Recommended next move

Commission a 12-16 week Discovery-to-Prototype programme centred on one complete evidence chain: approved crop plan → mapped block/grid → event capture → human response → immutable audit history → harvest/batch custody → compliance export. Run it on a non-regulated test environment first, then progress only through formal gates.

FOUNDATION

1. Purpose, scope and system boundary

YandiOS is proposed as the institutional operating and intelligence layer connecting farms, blocks, genetics, crops, harvests, batches, security events, quality decisions, processing, buyers, payments, research evidence and scale decisions.

YandiOS is	YandiOS is not
A shared identity, workflow and evidence architecture	A licence, permit, certification or substitute for accountable people
A coordination layer for distributed production	A claim that every sensor, farm or workflow must be centrally controlled
A source of audit-ready records and decision context	A guarantee that records will be legally admissible or regulator-accepted
A potential software/managed-service product	A validated recurring-revenue product today
A learning loop across seasons and partners	A reason to collect unlimited farmer, worker or customer data

Operating hierarchy

Layer	Authority
The Yandi Codex	Constitutional principles, truth rules, evidence gates and institutional limits
Yandi AG	Commercial steward, accountable organisation and rights holder
YandiOS	Operating, intelligence, evidence and coordination architecture
Growing Partners™	Independent production network operating under lawful agreements
Subsystems	Specialised security, geospatial, provenance and assurance functions
Human authorities	Legal, quality, security, commercial and governance decisions

STRATEGY

2. Problem and differentiated proposition

Large outdoor medicinal-crop programmes must coordinate physical security, regulated records, crop identity, partner performance, quality release and buyer evidence across places and organisations. Existing tools often solve only one slice.

Control problem	Typical fragmentation	YandiOS proposition
Field operations	Farm tasks and agronomy records sit apart from regulated status.	Bind work, location, crop identity, permissions and evidence.
Security	Alarms, video, access and field maps have separate event histories.	Use geospatially addressed events and one incident ledger.
Provenance	Seed, crop, harvest, test, process and sale identifiers drift.	Maintain genealogy from authorised source to customer lot.
Partner network	Each farm recreates workflows, templates and buyer access.	Shared standards with explicit local responsibility.
Learning	Quality, security and commercial results do not return to field decisions.	Closed-loop evidence across genetics, place, practice and outcome.

The differentiator is not any single sensor, map or QR code. It is the controlled relationship among identity, place, event, authority, custody, evidence and outcome across a regional network.

POSITIONING

The operating system for secure medicinal agriculture: field-scale controls, defensible provenance and coordinated market access - from seed to sale.

SUBSYSTEMS

3. Product portfolio

Component	Mandate	Primary outputs	Maturity
YandiOS™	Core platform, identity, workflow, status, evidence, reporting and integration.	Operational record, dashboards, audit exports, decisions.	Architecture
GeoSpatialEngine™	Canonical spatial model for precinct, farm, block, zone, cell and event location.	Maps, geofences, cell registers, spatial joins, risk overlays.	Named concept
GridSecure™	Addressable physical/geospatial perimeter and protected-zone layer.	Cell health, correlated events, incident location and history.	Reference architecture
CropSecure™	Crop-risk and security assurance workflow.	Alerts, classifications, response tasks, evidence packages, metrics.	Architecture
CropFingerprint™	Persistent crop and provenance identity.	Genealogy, chain of custody, quality/test links, customer evidence.	Architecture
Growing Partners™	Network participation and common operating framework.	Partner status, acreage, readiness, tasks, obligations and performance.	Business concept

Subsystem boundaries

- GeoSpatialEngine answers where. GridSecure describes which physical cell or zone. CropSecure governs what the event means and what happens next. CropFingerprint preserves what biological/material identity was affected. The core YandiOS platform records who had authority, what evidence exists and what state changed.
- A subsystem may remain valuable internally without becoming a standalone commercial product. Commercialisation is a separate evidence gate.

TECHNICAL BLUEPRINT

4. Reference architecture

The recommended architecture is modular, API-first and event-led, with local-first operation for critical field controls. Cloud services may coordinate and analyse, but loss of wide-area connectivity must not disable essential detection or local logging.

Layer	Capabilities	Design principle
Experience	Role-specific web/mobile views; live map; work queues; incident command; audit export.	Show status and responsibility, not raw data overload.
Domain services	Identity, partner, crop, security, custody, quality, document, commercial and reporting services.	Clear boundaries; independent state machines.
Event and workflow	Append-only event store, rules, notifications, approvals, escalation and task orchestration.	Original history preserved; corrections appended.
Data	Operational database, geospatial store, object/evidence storage, analytics warehouse, key management.	Minimum necessary data; lineage and retention.
Edge / field	Gate/access control, sensor gateways, camera references, local buffer, health monitoring, offline procedures.	Fail safe; store and forward; no cloud-only safety dependency.
Integration	Laboratories, ERP/accounting, document systems, weather/remote sensing, logistics, regulators where authorised.	Contracted interfaces; least privilege; validation.

Core event grammar

IDENTITY CHAIN

Precinct → Farm → Block → Zone / Grid Cell → Crop Identity → Event → Response → Evidence → Decision → Learning

Architecture decision records should document every material choice, its alternatives, evidence, owner and reversal cost.

DATA ARCHITECTURE

5. Domain model and state control

Entity	Minimum identity and relationships
Organisation / person	Role, authority, credential status, employer/partner, access scope, training and conflicts.
Precinct / farm / block / zone / cell	Stable geospatial identifier, boundary version, risk class, permitted activity and system health.
Genetic source	Source, right-to-use basis, variety/line, receipt and propagation links.
Crop identity	Farm/block, genetics, season, approved plan, agronomic history and affected events.
Harvest / batch / lot	Quantity, timestamps, custody, segregation, transformations, samples, tests and disposition.
Security incident	Original signals, correlation, classification, location, affected identities, actions, evidence and closure.
Quality record	Specification, deviation, hold/release/reject authority, CAPA and supporting evidence.
Commercial record	Customer/specification, offer/contract status, delivery, acceptance, price basis, payment and farmer settlement.

Controlled states

Domain	Illustrative states
Crop	Draft → submitted → approved → active → harvested → closed / destroyed
Material	Received → quarantined → sampled → released / rejected → processed → dispatched
Incident	Signal → alert → incident → acknowledged → contained → investigated → closed / reopened
Partner	Prospect → assessed → approved → contracted → active → suspended / exited
Evidence	Observed → verified / disputed → superseded; never silently overwritten

OPERATING MODEL

6. Priority user roles and decision rights

Role	Accountable decisions	System access principle
Project / operations lead	Programme activation, resourcing and cross-functional escalation.	Portfolio view; cannot override quality or legal vetoes.
Growing Partner / farm manager	Field execution, staff, inputs, tasks and local incidents.	Own-farm scope; attributable actions.
Security controller	Classification, escalation, preservation and response coordination.	Security views; restricted operational detail.
Quality authority	Hold, release, rejection, deviation and CAPA.	Independence from production pressure.
Compliance / licence lead	Authorised activities, reports, inspections and regulator correspondence.	Controlled regulatory record and reporting.
Agronomy / research lead	Protocols, observations, analysis and recommendations.	Cannot rewrite source records; hypotheses labelled.
Commercial lead	Specifications, offers, contracts, delivery and settlement.	Customer and price access segregated.
System administrator	Configuration, users, integrations and recovery.	No unilateral business/quality authority; privileged activity logged.

HUMAN VETOES

Legal compliance, quality release/rejection, partner exclusion, material security escalation, acreage activation, confidential-data use and public claims remain explicit human decisions.

OPERATING DESIGN

7. End-to-end workflows

The first release should prove a small number of complete workflows rather than a large menu of disconnected screens.

Workflow	Trigger	Controlled outcome
Partner onboarding	Candidate farm or operator identified.	Due diligence, rights, roles, boundaries, training and approval status evidenced.
Crop activation	Approved plan, site, genetics and authority ready.	Unique crop identity and mapped production scope established.
Security incident	One or more signals or observations occur.	Located, classified, acknowledged, escalated and preserved incident record.
Harvest and custody	Authorised harvest begins.	Quantity, containers, handoffs, transport and receiving reconciled.
Quality disposition	Sample/testing and review completed.	Named authority releases, rejects or holds material with reasons.
Buyer fulfilment	Specification and lawful sale route established.	Lot genealogy, documents, delivery, acceptance and payment linked.
Recall / investigation	Quality, diversion or customer concern raised.	Affected genealogy traced; material and evidence located rapidly.

Golden-path demonstration

1. Create a mapped test farm, block and grid-cell register.
2. Create an authorised crop identity linked to a genetics record and approved plan.
3. Generate simulated field/security events offline and online.
4. Require named acknowledgement, escalation and append-only correction.
5. Convert crop identity to harvest and batch identities with custody handoffs.
6. Attach a mock test result and quality decision.
7. Export an audit/incident/traceability pack and verify reconstruction by an independent reviewer.

FIELD SECURITY

8. GridSecure™ reference design

The current 50-acre concept models two independent intruder-resistant perimeter layers with opaque screening, a sterile detection corridor and nominal 10 m geospatial cells. An illustrative square 50-acre site has about 1,799 m of perimeter, approximately 180 cells per layer and approximately 360 two-layer cells. Actual geometry must follow survey and approved design.

Element	Fixed concept	Open decision
Physical layers	Two barriers capable of independent delay; screening is an overlay.	Certified materials, height, separation, foundations, wind/flood design.
Cell addressing	Stable property > system > layer > sector > cell > sensor address.	Surveyed registry, naming governance and lifecycle changes.
Detection	Ground, barrier, corridor, access, video reference, tamper and health signals.	Technology, spacing, thresholds, calibration and false-alarm performance.
Escalation	Weak anomaly through confirmed critical threat.	Site-specific classification, response timing and authority.
Resilience	Local detection/logging and store-and-forward.	Power duration, carriers, satellite role, redundancy and recovery.

NEXT DESIGN GATE Site survey + qualified security engineer/consultant + ODC pre-engagement + 30-50 m non-regulated sensor trial before regulated procurement.

SECURITY AND CROP RISK

9. CropSecure™ operating assurance

CropSecure should join physical security with disciplined operations. Its value comes from converting signals into accountable actions and measurable assurance, not from accumulating alerts.

Stage	Required record	Quality test
Prevent	Approved controls, access, workforce protocol, maintenance and exceptions.	Can current authorised state be demonstrated?
Detect	Original signal, source health, time, location and affected identity.	Can silence be distinguished from system failure?
Correlate	Independent signals, access/work orders and camera references.	Are incidents explainable without hiding uncertainty?
Respond	Severity, owner, acknowledgement, action, notification and safety constraints.	Did the correct person act within the approved procedure?
Preserve	Original evidence, export, checksum where appropriate, custody and retention.	Can an independent reviewer reconstruct the event?
Learn	Root cause, near miss, false alarm, CAPA and design change.	Did the system improve without erasing the original record?

Essential metrics

- Detection-chain availability and sensor health visibility
- Median acknowledgement and escalation times by severity
- False/nuisance alert rate and repeat causes
- Open incidents, overdue actions and repeated bypasses
- Percentage of events with complete identity, time, location and response records
- Exercise results, recovery time and closed corrective actions

TRACEABILITY

10. CropFingerprint™ provenance spine

CropFingerprint is a persistent evidence structure connecting biological source, place, practice, custody, transformation, quality and customer outcome. It should avoid unsupported claims that digital records alone prove authenticity, causation or immutable truth.

Lifecycle	Evidence linked to identity
Source	Genetic source, authorisation/right-to-use, receipt, propagation and parent-child lineage.
Place	Farm, block, boundary version, soil/water baseline and environmental context.
Production	Plan, inputs, tasks, observations, sensors, deviations and security history.
Harvest	Time, crew, quantity, container IDs, field-to-receival custody and reconciliation.
Process	Transformation relationships, yields, losses, samples, tests, holds and release.
Market	Specification, customer, delivery, acceptance, complaint/recall and realised outcome.
Learning	Genetics × place × practice × quality × netback analysis with evidence grade.

PROVENANCE RULE

A record may demonstrate who asserted what, when and against which evidence. It does not automatically prove the biological truth of the assertion; verification methods and uncertainty must remain visible.

PLACE AS A CONTROLLED IDENTITY

11. GeoSpatialEngine™

GeoSpatialEngine is the recommended formal name for the spatial capability implied by GridSecure and the precinct model. It should own canonical geometry and spatial relationships, not every operational record.

Capability	Initial requirement	Later opportunity
Boundary registry	Versioned precinct, farm, block, zone, route and cell geometry.	Multi-farm network topology and regional risk/capacity maps.
Address service	Stable readable identifiers independent of sensor vendor.	Cross-organisation spatial federation.
Event location	Map security, agronomy, maintenance and custody events.	Pattern detection and targeted assurance.
Geofencing	Warn when an activity, device or movement conflicts with permissions.	Automated risk rules with human review.
Remote sensing	Link approved imagery/indices to crop identity and observation date.	Research and anomaly hypotheses after ground-truthing.
Privacy/security	Generalised public views and restricted operational layers.	Fine-grained policy-based spatial disclosure.

Spatial data must carry source, capture time, accuracy, coordinate reference, boundary version, owner, sensitivity and permitted-use metadata.

ASSURANCE

12. Compliance and regulatory alignment

YandiOS should be designed to support a licensed operator’s obligations; it cannot itself grant authority. ODC guidance and licence conditions at the time of application, variation and operation must control the detailed design.

Requirement area	YandiOS support	Boundary
Licence/permit scope	Authorised locations, activities, quantities, conditions and expiry alerts.	Authoritative legal register requires human/legal ownership.
Site/security	Control register, tests, incidents, access and maintenance evidence.	Final system subject to site-specific assessment and acceptance.
Inventory/reconciliation	Crop, harvest, material movements, losses, waste and annual/periodic reconciliation.	Reconcile against physical counts and official reporting format.
Personnel/access	Role, training, approvals, access review and visitor/contractor record.	Employment, police and regulator requirements remain external.
Inspection readiness	Controlled document pack, evidence links, exceptions and corrective actions.	System output must be reviewed; audit-ready is not audit-approved.
Change control	Assess security, site, process and system changes for approval/variation impact.	Do not deploy material regulated change on software authority alone.

Current official sources confirm that medicinal-cannabis cultivation/production uses a licence and relevant permit framework, security forms part of application assessment, and permit holders have periodic reporting and reconciliation obligations. Requirements should be rechecked at every gate.

TRUST ARCHITECTURE

13. Cybersecurity, privacy and evidence integrity

Domain	Baseline design requirement
Identity and access	Unique accounts, MFA, role/attribute-based access, privileged separation, joiner/mover/leaver workflow and access reviews.
Segmentation	Separate field/OT security, corporate IT, guest, analytics and third-party integration zones.
Data protection	Encryption in transit and at rest where appropriate; managed keys; secrets vault; protected backups.
Software security	Secure SDLC, code review, dependency control, vulnerability management, testing and release approval.
Logging/evidence	Synchronised time, append-only audit history, protected exports, transparent corrections and monitored admin actions.
Resilience	Offline procedures, local buffer, redundancy, tested restores, disaster recovery and incident communications.
Privacy	Purpose limitation, data minimisation, notices/consent where required, access/correction, retention and disposal.
Third parties	Due diligence, data-processing terms, support access control, breach duties, portability and exit plans.

Assurance pathway

Use the Australian Essential Eight as a practical baseline, design an information-security management system aligned to ISO/IEC 27001:2022, and maintain a SOC 2 readiness control map if US enterprise buyers require it. SOC 2 is an independent attestation target, not a product feature or self-declared certification.

PRIVACY

The Australian Privacy Principles govern covered entities’ handling of personal information. Collect only what is reasonably necessary, control cross-border disclosure and apply APP 11 security/retention duties where applicable.

ENGINEERING

14. Non-functional requirements

Attribute	Founding target / acceptance concept
Availability	Tiered by function: critical local field controls continue during WAN outage; cloud targets set after threat and cost analysis.
Integrity	All state changes attributable; original events retained; corrections append; evidence objects hashable and access-controlled.
Performance	Critical alerts appear locally within site-engineered limits; ordinary workflows remain usable on rural connectivity.
Scalability	Identifiers and tenancy support 50 → 500 → 5,000 acres without assuming those scales are approved or economic.
Interoperability	Documented APIs, exportable data, standard geospatial formats and vendor-neutral identifiers.
Usability	Role-specific queues, plain language, accessible design, low-bandwidth operation and minimal duplicate entry.
Maintainability	Modular services, automated tests, observability, configuration control and documented runbooks.
Portability/exit	Yandi and partners can export their authorised records; vendor exit and key-person risks are planned.
Auditability	Every material record has source, actor, time, version, state, decision authority and evidence links.

DELIVERY

15. MVP and validation programme

The MVP should prove the evidence spine, not attempt to automate the entire agricultural enterprise.

Release	In scope	Exit evidence
R0 - Discovery	Users, regulatory map, threat model, data rights, domain model, workflow maps, architecture decisions.	Approved product brief, risk register and prototype acceptance criteria.
R1 - Prototype	Mapped site/cells, user roles, crop identity, simulated events, incident workflow, harvest/batch custody, audit export.	Independent walkthrough reconstructs golden path and failures.
R2 - Non-regulated field pilot	Edge gateway, sensor health, offline buffer, map/alerts, response exercise and recovery.	Measured reliability, false alerts, usability and controlled evidence.
R3 - 50-acre integrated readiness	Validated interfaces, SOPs, training, security/quality sign-off and regulator-aligned documentation.	Formal go/no-go gate; no critical uncontrolled dependency.
R4 - Multi-farm replication	Tenant/partner separation, differing connectivity and operating conditions.	Repeatable onboarding, support cost and control performance.

Prototype exclusions

- Automated quality release, autonomous law-enforcement notification or unsupervised regulatory filing
- Claims of immutable biological truth, AI-determined guilt, intent or compliance
- Full enterprise resource planning, laboratory information management or video-management replacement
- Production use of unvalidated satellite/remote-sensing outputs as the sole basis for regulated decisions

EXECUTION

16. 12-16 week delivery roadmap

Weeks	Workstream	Deliverables
1-2	Discovery and control framing	Stakeholder map, use cases, status baseline, threat model, legal/regulatory questions, data-rights principles.
3-4	Architecture and experience design	Domain/state model, interface flows, spatial registry, role matrix, prototype specification, ADRs.
5-8	Prototype build	Identity, map/cell register, event ingestion/simulation, incident workflow, custody chain and audit export.
9-10	Security and privacy hardening	Access controls, audit protection, backup/restore, privacy mapping, vendor/edge review.
11-12	Test and independent walkthrough	Golden paths, failure modes, outage test, evidence reconstruction, usability and defect closure.
13-16	Field-pilot preparation	30-50 m test plan, procurement specification, SOPs, training, ODC pre-engagement pack and gate decision.

Minimum founding team

Capability	Accountability
Product / programme lead	Scope, stakeholders, evidence gates, budget and decisions.
Domain/compliance lead	Licence/permit questions, records, quality/security boundaries and reporting.
Solution architect / lead engineer	Architecture, build quality, integrations, resilience and technical documentation.
UX/geospatial specialist	Rural workflows, map/cell model, accessibility and low-bandwidth usability.
Security engineering	Physical/cyber threat design, controls, testing and incident evidence.
Data/privacy adviser	Data rights, APP mapping, retention, sharing and research governance.

BUSINESS MODEL

17. Commercial model and evidence gates

Potential layer	Commercial form	Proof required before forecast
YandiOS platform	Subscription, acreage/organisation tier, managed service or enterprise licence.	Deployable product, support cost, willingness to pay and retention.
CropSecure / GridSecure	Module, monitoring/assurance service, implementation and maintenance.	Detection performance, integration economics, regulator/customer value.
CropFingerprint	Traceability/provenance service, buyer evidence package or API.	Identity accuracy, interoperability, acceptance and avoided cost/value.
Growing Partners	Participation/service arrangement.	Farmer netback, adoption, rights, contract fairness and repeat seasons.
Infrastructure/markets	Processing/storage/tolling, aggregation or transaction margin.	Throughput, capacity, lawful contracts, acceptance and payment.
Genetics/research	Licence, royalty, propagation or collaboration.	Rights, distinct value, repeatable performance and enforceability.

The pitch-deck 5,000-acre scenario ($325m regional crop value, $60.8m platform revenue, 64% gross margin and $27.8m EBITDA potential) should remain explicitly labelled a management planning scenario. It is not an audited forecast and depends on unvalidated yield, price, adoption, network capture, cost and regulatory assumptions.

COMMERCIAL RULE

Validate each revenue layer separately. Crop value is not Yandi revenue; projected network activity is not contracted demand; and software usage is not willingness to pay.

INTELLECTUAL INFRASTRUCTURE

18. IP, data rights and defensibility

The project register currently designates CropSecure™, CropFingerprint™ and GridSecure™ as linked YandiOS research concepts. GeoSpatialEngine™ should be added through controlled documentation if adopted. Internal designation alone does not grant statutory rights.

Asset	Protection/action
Names and brands	Clearance searches, domain/social control, consistent use and professional advice on trade-mark filings and classes.
Software/source	Authorship and contractor assignment, repository control, licence policy, secrets management and release provenance.
Schemas/methods	Versioned domain/event models, documented know-how, confidentiality and selective publication strategy.
Designs/security methods	Controlled annexes; assess patent/design potential before public disclosure where genuinely novel.
Data	Contracts define source rights, access, permitted uses, research use, derived insights, portability, retention and exit.
Partner contributions	Explicit background/foreground IP, improvements, licences, confidentiality and publication terms.
Evidence corpus	Provenance and governance; avoid asserting ownership over farmer facts or third-party data beyond lawful rights.

Defensibility is expected to come from a compound system: trusted relationships, regulator-informed workflows, field validation, proprietary know-how, interoperable evidence structures, longitudinal results and disciplined execution - not from a single trademark or database.

MARKET POSITION

19. Competitive differentiation

Category	Usually optimises	YandiOS distinction
Farm-management software	Tasks, inputs, agronomy and yield.	Adds regulated identity, security incidents, custody, quality authority and buyer evidence.
Physical-security integrator	Barriers, cameras, alarms and monitoring.	Links cell-addressed events to crops, people, responses, compliance and learning.
Seed-to-sale / track-and-trace	Inventory movements and mandated reporting.	Extends into broadacre geospatial security and Growing Partner operating coordination.
Quality / document system	SOPs, deviations, training and release.	Connects controlled records directly to place, crop genealogy and field events.
Traceability/provenance platform	Product genealogy and claims.	Integrates agricultural execution, diversion control and regional network economics.
Commodity marketplace	Buyers, suppliers and transactions.	Makes market access the end of an evidence chain, not a detached listing.

Strategic moat sequence

1. Prove one complete evidence chain.
2. Earn regulator, partner and buyer confidence without overstating endorsement.
3. Accumulate high-quality, permissioned longitudinal evidence.
4. Improve operating standards and economics using verified results.
5. Make multi-farm replication easier than recreating controls independently.
6. Commercialise only the modules whose external value and support economics are demonstrated.

CONTROL

20. Governance and assurance model

Forum / owner	Mandate	Cadence
Yandi AG board / governing body	Risk appetite, capital, strategy, rights and scale gates.	Monthly/quarterly and gate decisions
YandiOS steering committee	Product priorities, architecture boundaries, budget and dependency risk.	Fortnightly during build
Quality authority	Independent quality states, deviations, CAPA and release rules.	Continuous / formal review
Security authority	Threat model, site controls, incidents, exercises and restricted information.	Weekly operational / quarterly assurance
Data and research governance	Privacy, partner rights, research protocols, access and publication.	Monthly / per project
Change advisory	Regulated/critical changes, testing, approvals, rollback and evidence.	Per release/change
Independent assurance	Penetration testing, control review, field/security design and evidence reconstruction.	Before critical gates and annually

Every critical control should have an owner, purpose, implementation evidence, test method, test frequency, exception process and link to the risks it mitigates.

MATERIAL RISKS

21. Risk register

Risk	Current rating	Priority treatment
Architecture described as deployed capability	High	Publish maturity labels; maintain claims register; require approval for external statements.
Regulatory/security design rejected or materially changed	High	Early ODC engagement; qualified site/security design; modular and reversible procurement.
Founder/key-person dependency	High	Decision records, role delegation, source/document control and succession-ready operating system.
Farmer data/control distrust	High	Contractual data rights, minimisation, transparent uses, portability and governance representation.
Cyber or physical compromise	High	Threat-led layered controls, segmentation, monitoring, response, recovery and independent tests.
MVP scope/cost expansion	High	Golden-path scope, fixed gates, architecture decisions and kill/defer criteria.
Poor field connectivity / power	Medium-High	Local-first operation, buffers, health monitoring, failover and outage exercises.
False alarms and operator fatigue	Medium-High	Sensor trial, correlation rules, tuning, maintenance and human-factors testing.
Unvalidated economics / customer need	High	Buyer discovery, written specifications, pilots, price evidence and separate revenue validation.
IP leakage / ownership ambiguity	Medium-High	Assignments, registers, confidentiality, partner terms and pre-disclosure advice.

EVIDENCE

22. Success measures and scale gates

Dimension	Founding measures
Regulatory/readiness	Requirements mapped; open regulator questions; approved controls; no critical authorisation gap.
Traceability	Time to reconstruct genealogy; reconciliation variance; missing links; recall exercise accuracy.
Security	Control availability; verified detection; nuisance rate; response times; exercise outcomes; overdue faults.
Quality	Right-first-time records; deviations; holds; CAPA closure; release independence and customer acceptance.
Product	Task completion, active use, workflow duration, duplicate entry, support load and user confidence.
Cyber/privacy	MFA/privileged coverage, patch/vulnerability status, restore tests, incidents, access reviews and retention compliance.
Commercial	Qualified users/buyers, written need, pilot commitments, willingness to pay, acquisition/support cost and retention.
Partner/farmer	Onboarding time, training, satisfaction, netback, repeat participation and dispute/exit experience.

Systems validation ladder

Gate	Minimum proof
S0 Architecture	Purpose, users, rights, accountabilities, failure modes and legal boundaries.
S1 Prototype	Core identity/event/workflow demonstrated.
S2 Controlled field trial	Measured real-farm reliability and usability under bounded, lawful conditions.
S3 Integrated 50-acre use	Supports the demonstration without critical uncontrolled dependency.
S4 Multi-farm replication	Works across independent users, connectivity and operating styles.
S5 External value	Third party demonstrates material value from evidence/service.
S6 Commercial product	Repeatable deployment, support, rights, security, pricing and willingness to pay.
S7 Institutional infrastructure	Auditable, resilient, transferable and able to survive founder absence.

RECOMMENDATION

23. Immediate decisions and 30-day action plan

Five decisions will convert YandiOS from a coherent body of work into a controlled development programme.

1. Adopt this report as the YandiOS baseline and nominate an accountable product/programme lead.
2. Approve the system boundary and product maturity language for all external materials.
3. Authorise a Discovery-to-Prototype brief with fixed golden-path scope, budget range and gate criteria.
4. Commission site/security pre-engagement: survey, qualified security review, ODC question register and non-regulated sensor-test design.
5. Commence rights hygiene: consolidated IP register, trade-mark advice, contractor assignments, data-rights principles and controlled disclosure.

Days	Action	Output
0-7	Baseline and ownership	Approved report, decision owners, document register, claims/status register.
8-14	Discovery mobilisation	Stakeholders, user interviews, regulatory questions, threat model, data map and architecture workshop.
15-21	Prototype specification	Domain/state model, UX flows, cell registry, acceptance tests, vendor/build options and cost plan.
22-30	Gate 1 decision	Signed product brief, delivery plan, risk treatment, field-test plan and go/no-go funding decision.

RECOMMENDATION

Build the proof, then build the network. Do not make acreage, security procurement or revenue promises outrun the evidence chain that YandiOS is intended to protect.

CONTROLLED REFERENCE

Appendix A - Requirements traceability starter

ID	Requirement	Verification
REQ-001	Every regulated/material entity has one stable ID and explicit lifecycle state.	State-transition and duplicate-ID tests.
REQ-002	Every critical event records source, actor/system, synchronised time, place and affected identity.	Event-schema validation and audit reconstruction.
REQ-003	Original events cannot be silently overwritten; corrections are attributable.	Tamper/change test and export review.
REQ-004	Critical field detection and logging continue during WAN loss.	Outage and resynchronisation test.
REQ-005	Quality release/rejection requires named authorised human decision.	Permission and workflow tests.
REQ-006	Access is least-privilege, reviewed and privileged actions are monitored.	Access review and admin-log test.
REQ-007	Partner and personal data use is purpose-limited, documented and exportable as agreed.	Data map, notice/contract and export test.
REQ-008	Security-sensitive implementation detail is restricted by role and document classification.	Role test and disclosure review.
REQ-009	System can reconstruct crop-to-lot genealogy and custody within an agreed time.	Trace/recall exercise.
REQ-010	System status claims and external reports identify evidence level and approval state.	Claims-register and publication review.

EVIDENCE BASE

Appendix B - Source register

Internal Yandi sources

- The Yandi Codex - Systems Annex: YandiOS Product & Intellectual Infrastructure Doctrine (July 2026).
- YandiOS GridSecure 50-Acre Reference Architecture v1.0 (26 July 2026).
- YandiOS Research Project IP Register v1.0 (26 July 2026).
- Yandi AG Police Technical Briefing - YandiOS (July 2026).
- YandiOS 15-Card Pitch Deck (August 2026).
- The Yandi Codex - Founding and Book One/Book Two editions (July 2026).

Current external reference points

- Office of Drug Control - medicinal cannabis licence application guidance.
- Office of Drug Control - quarterly reporting obligations (updated 18 March 2026).
- OAIC - Australian Privacy Principles and APP Guidelines (updated 13 May 2026).
- Australian Cyber Security Centre - Essential Eight maturity model.
- ISO/IEC 27001:2022 - Information security management systems.

External pages were checked on 2 September 2026. Detailed legal, regulatory, tax, engineering, insurance, privacy and certification advice should be obtained at the relevant gate.

CLOSING COVENANT	The crop proves the system. The system creates the record. The record creates knowledge. Knowledge improves the next crop. When that cycle can travel without losing truth, responsibility or farmer viability, YandiOS has become infrastructure.

END OF REPORT / YANDIOS COMPLETE REPORT v1.0