

OwnerRadar

AI Manager for Businesses

Know when one conversation changes the whole business.

Document	Product Requirements Document
Version	0.1
Status	Hackathon build specification
Date	August 6, 2026
Primary demo	Ten-location pizza group; 300-pizza order and risk escalation

Product thesis

Business owners do not need more raw data. They need an intelligence layer that notices material events, understands who made each decision and under which role, escalates only what matters, and helps coordinate a response before an opportunity is lost or a problem becomes expensive.

1. Executive Summary

OwnerRadar is an AI manager for owners and operators. It continuously ingests authorized business communications and operating events, converts them into a live model of people, roles, locations, commitments, decisions, risks, and opportunities, and proactively alerts the correct decision-maker when intervention is justified.

Hackathon objective

Demonstrate a complete live loop: a major order enters through a real phone call, scattered operational signals reveal that the location cannot fulfill it, the AI proactively alerts the owner, proposes a cross-location recovery plan, receives approval by SMS, coordinates the response, and preserves the critical decision lineage on a tamper-evident blockchain record.

Why it matters

- A ten-location owner cannot listen to every call, read every message, monitor every refund, or sit inside every manager conversation.
- Traditional systems record transactions but rarely recognize when one conversation materially changes the entire operation.
- Small businesses are operationally messy: the same person wears several hats, authority is informal, and important commitments live inside calls and texts instead of structured systems.
- OwnerRadar turns those fragmented signals into selective, explainable, actionable intelligence.

Core promise

UNSEEN -> DETECTED -> UNDERSTOOD -> ESCALATED -> COORDINATED -> VERIFIED

Primary product behavior

Capability	What OwnerRadar does	Visible proof in demo
Continuous monitoring	Consumes calls, texts, emails, POS-like events, staffing updates, inventory signals, and manager actions.	Live event stream across ten locations.
Material-event detection	Separates routine noise from events with high business impact, urgency, or owner-level authority requirements.	Owner receives an unsolicited alert only after the major order becomes material.
Role-aware reasoning	Understands which location, company, and role a person was acting under when a promise or decision was made.	Cashier accepts an order above the role escalation threshold.
Cross-location coordination	Finds spare capacity, inventory, people, or vehicles elsewhere in the group.	Production split across three stores and a van reassigned.
Decision lineage	Records evidence, analysis, recommendation, approval, actions, and outcome.	Verified decision path with tamper demonstration.

2. Problem Definition

Problem statement

Owners of multi-location small and midsize businesses often learn about major opportunities, customer commitments, safety incidents, staffing failures, or policy violations only after the event has become costly. The

required information already exists, but it is fragmented across conversations, systems, and people acting in several roles.

The operational reality

- One employee may be cashier, catering coordinator, shift lead, and delivery driver depending on the day.
- A customer promise may exist in a phone call while capacity data exists in a spreadsheet and vehicle status exists in a manager text.
- Escalation rules are often informal: “Tell me if an order is big” rather than a machine-readable threshold.
- The owner is overloaded by routine data, so sending more alerts creates noise rather than control.
- After an incident, participants may disagree about what was said, which rules were active, and why a decision was made.

Problem to solve for the hackathon

Scenario

A cashier at one of ten pizza locations accepts an order for 300 pizzas for the hackathon. The owner is happy about the sale but does not know it happened. The accepting location cannot fulfill the promise alone. Additional messages reveal an ingredient shortage, no delivery vehicle, and an unauthorized discount. OwnerRadar must recognize that the event changes the business, alert the owner without being asked, find a feasible group-wide plan, and coordinate it after approval.

Non-problem

This is not a generic call summarizer, employee surveillance product, replacement POS, legal-advice system, or autonomous manager with unrestricted authority. The product is an intelligence and escalation layer that uses existing operational evidence and preserves human accountability.

3. Users and Buyers

Persona	Need	Hackathon behavior
Multi-location owner / principal	Know only what materially deserves executive attention and approve high-impact interventions quickly.	Receives proactive SMS; replies APPROVE, REVIEW, or CALL MANAGER.
Regional / area manager	Coordinate multiple locations and resolve issues that exceed one store's capacity.	Reviews proposed production split and manager confirmations.
Location manager	Receive precise actions, not broad alerts, and report local constraints.	Accepts or declines production allocation by text.
Frontline employee	Handle customers naturally without learning another complex dashboard.	Completes a normal call; the system extracts the commitment.
Consultant / fractional COO	Understand how the business actually operates and where control gaps exist.	Uses the decision graph and post-event findings.
Auditor / insurer / partner	Verify that critical evidence and decision records were not rewritten.	Uses the blockchain verification view.

Initial target segments

- Multi-location restaurants and catering groups
- Franchise operators and multi-unit retailers
- Home-service companies operating several branches
- Dental, medical, and professional-service groups

- Property-management and facility-service organizations

4. Product Goals and Principles

MVP goals

1. Detect one high-impact opportunity and its operational risks from mixed real-time signals.
2. Proactively alert the owner without requiring the owner to query the system.
3. Explain the alert with traceable evidence, active roles, and business rules.
4. Generate a feasible cross-location recovery plan.
5. Require human approval before consequential external actions.
6. Coordinate the approved plan through real Twilio messages.
7. Create a tamper-evident decision record anchored through QuickNode to Solana.

Design principles

Principle	Requirement
Signal over noise	Routine activity remains quiet. Escalate only events that cross materiality thresholds.
Explain before acting	Every alert must identify evidence, reasoning factors, confidence, and recommended action.
Human authority remains explicit	AI may recommend and coordinate only within configured permissions; owner approval is required for consequential actions.
One person, many hats	The data model separates human identity from business role, location, authority, and time context.
Private by default	Raw calls, messages, customer data, and employee data remain off-chain and access-controlled.
Outcome-oriented	The product should connect detected events to revenue protected, risk reduced, or responsibility clarified.

5. Canonical Hackathon Demo

Fictional company setup

Miami Slice Group operates ten fictional locations. Each location has ordinary order volume, production capacity, ingredients, drivers, and staffing. Several employees work across locations or perform multiple roles.

Miami Slice Group

- Brickell capacity: 120 pizzas before 7:00 PM
- Coral Gables spare capacity: 100 pizzas
- Downtown spare capacity: 80 pizzas
- Doral catering van available
- 6 additional locations with normal activity

Live story

Stage	Event	System response
1. Normal operations	A simulator emits routine orders, shifts, supplier messages, refunds, and customer calls across ten locations.	OwnerRadar quietly builds context; no owner interruption.
2. Material event	A judge calls the Brickell Twilio number and orders 300 pizzas for 7:00 PM. Retell agent or employee accepts.	Call is transcribed; customer commitment and order size are extracted.

Stage	Event	System response
3. Hidden constraints	Simulated texts report limited dough/cheese, delivery van unavailability, and an unauthorized discount.	AI links signals to the same order and calculates fulfillment risk.
4. Proactive escalation	Owner has not opened the app or texted the AI.	Owner receives an unsolicited SMS describing opportunity, risk, evidence, and available plan.
5. Human approval	Owner replies APPROVE.	System distributes production, assigns vehicle, and prepares customer update.
6. Coordination	Location managers reply ACCEPT or DECLINE.	Plan updates live; dashboard moves from red to green.
7. Business development	AI recognizes potential recurring-event customer.	Creates catering-account opportunity and follow-up task.
8. Verification	Critical decision record is hashed and anchored on-chain.	Verification view proves the evidence and approval chain have not changed.

Proactive owner alert

OWNER RADAR - HIGH IMPACT EVENT

Brickell accepted a 300-pizza order due at 7:00 PM. Estimated value: \$4,650.

The location can produce approximately 120 pizzas by the deadline. No delivery vehicle is assigned, and a 12% discount exceeds the cashier's 5% authority.

I found capacity at Coral Gables and Downtown plus an available Doral van.
Reply REVIEW, APPROVE, or CALL MANAGER.

Proposed recovery plan

Brickell: 120 pizzas
Coral Gables: 100 pizzas
Downtown: 80 pizzas
Doral van: delivery
Projected ready: 6:42 PM
Projected arrival: 6:55 PM
Customer follow-up: confirm logistics and create recurring catering lead

6. Scope

Hackathon MVP - required

Area	In scope	Acceptance signal
Locations	Ten seeded fictional locations with capacity, inventory, staffing, and role data.	Dashboard shows all locations and event counts.
Event simulator	Scripted calls/messages/POS-like events emitted every few seconds.	Normal activity visibly streams without triggering owner alert.
Live voice	One Twilio/Retell inbound call with post-call transcript webhook.	Call transcript appears and creates/updates the major order.
AI extraction	Structured extraction of commitments, decisions, roles, risks, opportunities, deadlines, and dependencies.	Decision timeline and graph update from transcript and events.
Materiality engine	Score impact, urgency, confidence, and authority requirement.	300-pizza event triggers immediate escalation; routine events do not.

Area	In scope	Acceptance signal
Owner SMS	Proactive Twilio alert with reply commands.	Owner receives alert without querying system.
Approval orchestration	APPROVE triggers manager tasks and customer update.	Real or simulated recipients receive messages and dashboard changes.
Decision graph	Visual map of event -> commitment -> constraints -> recommendation -> approval -> actions -> outcome.	Clickable nodes show evidence and active persona.
Blockchain anchor	Hash the canonical decision record and store it using Solana through QuickNode.	Verification status and tamper failure are demonstrated.

Out of scope for the hackathon

- Production-grade POS, payroll, accounting, scheduling, Gmail, Slack, or inventory integrations
- Full autonomous purchasing or movement of money
- Employee discipline, termination recommendations, or covert monitoring
- Legal determinations or claims that liability has been established
- Custom blockchain program with complex token economics
- Multi-tenant enterprise administration, billing, or complete role provisioning
- Reliable forecasting trained on historical real-company data

7. Functional Requirements

7.1 Event ingestion and normalization

ID	Requirement	Priority
FR-001	System shall accept a Retell post-call webhook containing call ID, called number, timestamps, transcript, participants, and optional analysis.	Must
FR-002	System shall accept simulated events for SMS, manager chat, POS orders, inventory, staffing, refunds, vehicle status, and supplier communications.	Must
FR-003	Every event shall include source, location, organization, actor, timestamp, event type, body/payload, and correlation identifiers when available.	Must
FR-004	System shall correlate events into an operational case such as ORDER-300-HACKATHON.	Must
FR-005	System should support replaying the complete simulation deterministically.	Should

7.2 Identity, role, and authority model

ID	Requirement	Priority
FR-010	A person shall have one canonical identity and one or more time-bound personas.	Must
FR-011	A persona shall specify organization, location, role, authority, escalation threshold, and allowed actions.	Must
FR-012	An event shall record the inferred or explicit persona under which the actor was operating.	Must
FR-013	When the persona is ambiguous, the system shall flag authority uncertainty rather than invent certainty.	Must
FR-014	The UI shall show when one person functions across multiple locations or responsibilities.	Should

7.3 AI event understanding

ID	Requirement	Priority
FR-020	AI shall extract entities, locations, quantities, deadlines, commitments, decisions, constraints, risks, opportunities, and requested actions.	Must
FR-021	AI shall compare extracted commitments and decisions with the active location policy and actor authority.	Must
FR-022	AI shall distinguish reported facts, inferred facts, and unresolved ambiguity.	Must
FR-023	AI shall cite supporting transcript excerpts or event IDs for each material finding.	Must
FR-024	AI shall produce structured JSON before any natural-language summary.	Must
FR-025	AI shall identify cross-location resources capable of resolving an operational gap.	Must

7.4 Materiality and escalation

OwnerRadar must suppress routine noise and score only events that may warrant intervention.

```
materiality_score = f(impact, urgency, confidence, owner_authority_needed, blast_radius)
```

Dimension	Examples	Range
Impact	Revenue size, safety exposure, customer importance, financial loss, brand effect	0-25
Urgency	Minutes until commitment, ongoing safety issue, customer waiting	0-25
Confidence	Strength and consistency of evidence	0-20
Owner authority	Whether available managers can resolve within policy	0-20
Blast radius	Number of locations, customers, employees, or systems affected	0-10

Initial hackathon threshold: immediate owner alert at 70+, manager-only alert at 45-69, digest below 45. Values are configurable and illustrative, not production-calibrated.

7.5 Proactive notification

ID	Requirement	Priority
FR-030	System shall send an unsolicited Twilio SMS when an event crosses the owner escalation threshold.	Must
FR-031	Alert shall summarize what happened, why it matters, evidence, confidence, and recommended next action.	Must
FR-032	Alert shall provide concise commands: REVIEW, APPROVE, DECLINE, CALL MANAGER.	Must
FR-033	System shall avoid repeated alerts for the same unresolved event unless state materially changes.	Should
FR-034	System shall log delivery and owner response.	Must

7.6 Plan generation and orchestration

ID	Requirement	Priority
FR-040	AI shall generate a constraint-aware recovery plan using location capacity, inventory, staffing, vehicles, deadlines, and authority.	Must
FR-041	Plan shall show assumptions and unresolved dependencies.	Must
FR-042	Consequential actions shall remain pending until required human approval.	Must

ID	Requirement	Priority
FR-043	After approval, system shall send manager assignment messages and record responses.	Must
FR-044	Plan shall recalculate when a location declines or a new constraint arrives.	Should
FR-045	System shall prepare a customer update and recurring-account follow-up task.	Should

7.7 Decision and evidence graph

ID	Requirement	Priority
FR-050	UI shall visualize people, locations, systems, events, commitments, decisions, evidence, risks, approvals, and outcomes as connected nodes.	Must
FR-051	Clicking a finding shall reveal the supporting transcript excerpt or event payload.	Must
FR-052	Graph shall distinguish fact, inference, recommendation, human decision, and executed action.	Must
FR-053	Graph shall show the active persona and authority for each human action.	Must
FR-054	Graph should highlight single points of failure, unowned responsibilities, or cross-location dependencies.	Should

7.8 Blockchain decision lineage

ID	Requirement	Priority
FR-060	System shall create a canonical JSON decision record after owner approval and action dispatch.	Must
FR-061	Raw transcripts, phone numbers, customer names, and private messages shall remain off-chain.	Must
FR-062	System shall hash the canonical record and submit the hash to Solana through QuickNode.	Must
FR-063	UI shall retrieve the transaction and compare the current record hash with the anchored hash.	Must
FR-064	A demo-only tamper action shall alter a local copy and visibly fail verification.	Should
FR-065	Decision lineage shall preserve policy version, evidence root, analysis result, human response, actions, and outcome.	Must

8. Event and Risk Taxonomy

The product must detect positive opportunities and negative exposure. It must label legal or compliance-related issues as potential risk signals requiring human review, not as conclusions of liability.

Category	Example signal	Default handling
Major opportunity	Order is 10x normal size; customer mentions recurring events.	Immediate owner alert plus proposed fulfillment and sales follow-up.
Capacity failure	Promise exceeds local production, staffing, or delivery capacity.	Find group-wide resources and request approval.
Unauthorized commitment	Discount, refund, delivery guarantee, or reimbursement exceeds actor authority.	Flag decision, preserve evidence, route to authorized approver.
Food / customer safety	Customer reports illness, burn, contamination, or unsafe condition.	Immediate review; preserve records; notify manager; avoid admission of fault.
Employee safety / HR	Employee reports injury, harassment, threat, or unsafe equipment.	Immediate restricted escalation and evidence preservation.

Category	Example signal	Default handling
Financial anomaly	Unusual refunds, voids, cash mismatch, or purchase pattern.	Manager review; owner alert only when materiality threshold is crossed.
Customer escalation	Chargeback threat, attorney mention, social-media escalation, repeated unresolved complaint.	Customer recovery and management review.
Data exposure	Customer or employee information shared across locations or businesses without clear purpose.	Restrict access, flag transfer, request review.
Operational dependency	One person is the only bridge for a critical process.	Recommend backup ownership and documented handoff.
Responsibility gap	A commitment exists but no person owns the next action.	Assign or escalate before deadline.

9. AI Analysis Contract

Required structured output

Illustrative analysis schema

```
{
  "case_id": "ORDER-300-HACKATHON",
  "materiality": {
    "score": 91,
    "impact": 24,
    "urgency": 24,
    "confidence": 18,
    "owner_authority_needed": 18,
    "blast_radius": 7
  },
  "facts": [],
  "inferences": [],
  "people_and_personas": [],
  "commitments": [],
  "decisions": [],
  "constraints": [],
  "risk_signals": [],
  "opportunities": [],
  "missing_owners": [],
  "recommended_plan": [],
  "required_approvals": [],
  "evidence_refs": [],
  "confidence_notes": []
}
```

AI safety and quality rules

- Never state that the company is legally liable; state the observable event, policy conflict, and need for human review.
- Never infer an employee's intent, honesty, health, protected status, or character.
- Do not recommend discipline or termination in the MVP.
- Separate explicit evidence from inference. Every material finding requires evidence references.
- Do not expose private data to a recipient who lacks a defined business need.
- Do not execute payments, purchases, refunds, or external commitments without human approval.
- When evidence conflicts, surface the conflict and request clarification.

Example extracted decision

```
{
  "decision": "Promise 7:00 PM delivery",
  "actor": "Sofia Alvarez",
  "persona": "Brickell cashier",
  "authority_status": "outside_scope",
  "evidence": "call:00:42-00:48",
  "reason": "Orders over 75 pizzas require manager confirmation before a delivery promise.",
  "downstream_effect": "Customer expectation established before capacity validation."
}
```

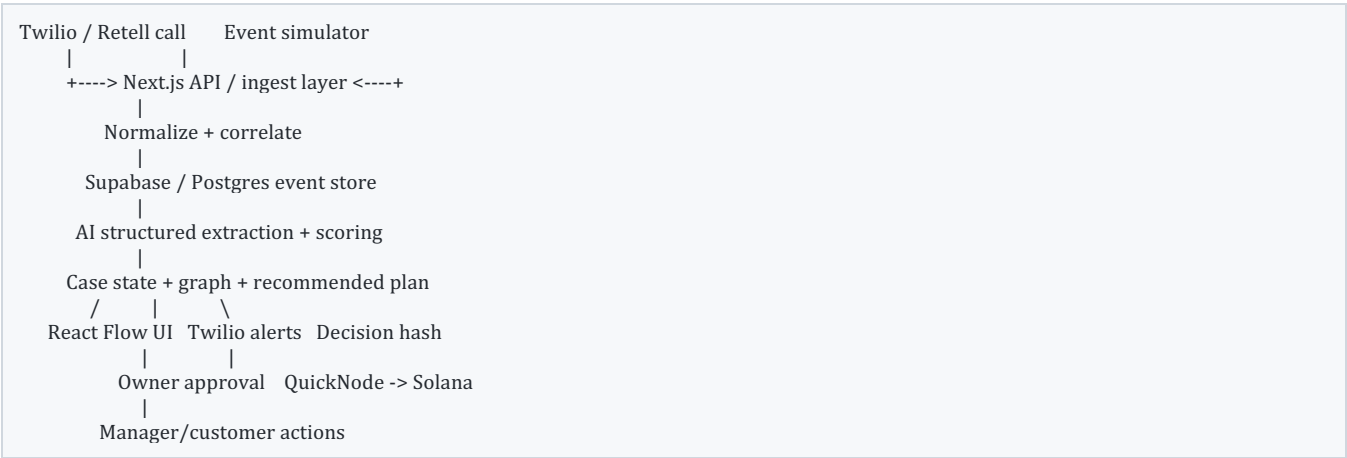
10. Conceptual Data Model

Entity	Purpose	Key fields
Organization	Parent operating company or independently managed business.	id, name, industry, policies, owner contacts
Location	Physical or operating unit.	id, organization_id, address, capacity, inventory, hours
Person	Canonical human identity.	id, display_name, communication handles
Persona	A person acting within a specific business context.	person_id, organization_id, location_id, role, authority, effective dates
Policy / mandate	Machine-readable business rule active at a point in time.	scope, thresholds, prohibited actions, version, hash
Event	Normalized evidence from any connected channel.	source, type, timestamp, actor, location, payload, correlation_id
Case	A correlated operational situation.	id, title, state, materiality, deadline, owner
Commitment	A promise made to a customer, employee, vendor, or partner.	actor_persona, beneficiary, terms, deadline, evidence
Decision	Choice or authorization with downstream effect.	actor_persona, inputs, authority_status, result
Finding	AI-generated fact, inference, risk, or opportunity.	type, severity, confidence, evidence_refs
Plan	Proposed set of coordinated actions.	steps, assumptions, dependencies, required approvals
Action	Executed message, assignment, or update.	actor, recipient, channel, status, result
Decision receipt	Canonical record anchored on-chain.	record_hash, tx_signature, policy_hash, evidence_root

Relationship model

Person -> has Persona -> belongs to Organization/Location -> receives Authority
 Event -> references Person/Persona/Location -> joins Case
 Case -> contains Commitments + Decisions + Findings + Plan + Actions
 Decision Receipt -> hashes Policy + Evidence + Analysis + Approval + Outcome

11. Technical Architecture



Recommended hackathon stack

Layer	Choice	Reason
Frontend	Next.js, TypeScript, Tailwind, React Flow	Fast single-page build with strong graph visualization.
Database	Supabase Postgres	Realtime subscriptions, rapid schema, easy webhook persistence.
Voice	Twilio number routed to Retell	Real call and reliable post-call transcript webhook.
Messaging	Twilio SMS	Proactive owner alert and reply-command loop.
AI	Structured-output LLM	Entity/decision extraction, materiality reasoning, plan generation, explanations.
Simulator	Node/TypeScript script or server route	Deterministic event stream without building real integrations.
Blockchain	QuickNode Solana RPC + memo/hash transaction	Fast sponsor integration and visible tamper-evident proof.
Hosting	Vercel	Rapid deployment and webhook endpoints.

Canonical decision record

```
{
  "decision_id": "DEC-ORDER-300-01",
  "case_id": "ORDER-300-HACKATHON",
  "policy_version": "catering-v3",
  "policy_hash": "...",
  "evidence_root": "...",
  "analysis_hash": "...",
  "recommendation": "split_production_across_three_locations",
  "owner_response": "approved",
  "actions_hash": "...",
  "outcome": "confirmed",
  "previous_receipt_hash": "...",
  "created_at": "2026-08-06T22:14:00Z"
}
```

12. User Experience Requirements

Primary screen: command center

- Ten location cards with status, active event count, material alerts, and capacity snapshot.
- Live event stream showing source and location; routine events visually subdued.

- Central decision graph that expands when a material case is selected.
- Right-side “Owner attention” panel with evidence, materiality score, risk/opportunity summary, and proposed plan.
- Visible state progression: Unseen -> Detected -> Escalated -> Approved -> Coordinating -> Resolved -> Verified.

Required screens / states

Screen / state	Required content
Network overview	Ten locations, status, order volume, capacity, active risks, current major case.
Case detail	Timeline, people/personas, commitments, constraints, decisions, risks, opportunities.
Decision graph	Clickable evidence and action nodes; colored distinctions between fact, inference, decision, and outcome.
Owner alert preview	Exact SMS, reason for interruption, confidence, commands.
Coordination panel	Production allocation, manager responses, delivery assignment, customer update.
Verification panel	Record hash, transaction signature, confirmation, verify button, tamper failure state.

Visual hierarchy

- Green: normal or resolved
- Amber: watch, ambiguity, or manager action
- Red: immediate owner attention or high-impact unresolved risk
- Blue: AI recommendation or informational context
- Purple/neutral: verified blockchain evidence

13. MVP Acceptance Criteria

AC	Given / When / Then
AC-01	Given routine events across ten locations, when the simulator runs, then the owner receives no immediate alert.
AC-02	Given a live call requesting 300 pizzas, when Retell posts the transcript, then the system creates or updates one correlated major-order case.
AC-03	Given the order plus capacity and vehicle constraints, when analysis completes, then the case scores above the immediate-alert threshold.
AC-04	Given a high-materiality case, when the owner has taken no action, then Twilio proactively sends an SMS containing opportunity, risk, evidence, and commands.
AC-05	Given the owner replies APPROVE, when the command is received, then assignments are sent to three locations and the driver/vehicle owner.
AC-06	Given manager acceptances, when responses arrive, then the plan and projected completion time update.
AC-07	Given a cashier discount beyond authority, when the case is analyzed, then the UI labels it as an unauthorized commitment with evidence.
AC-08	Given the event organizer mentions recurring events, when analyzed, then the system creates a recurring catering opportunity.
AC-09	Given an approved plan, when the decision receipt is finalized, then its hash is anchored and retrievable from Solana through QuickNode.
AC-10	Given the local decision record is altered after anchoring, when verification runs, then the UI clearly reports a mismatch.

14. Time-Boxed Build Plan

Block	Focus	Deliverable
0-30 min	Project scaffold, schema, seeded locations and people	App loads ten-location network with realistic seed data.
30-75 min	Simulator, event endpoint, realtime feed	Routine events stream and correlate into cases.
75-120 min	Retell webhook, transcript persistence, AI structured output	Live call appears with commitments and decision events.
120-165 min	Materiality scoring, owner SMS, inbound command handling	Proactive alert and APPROVE loop work end-to-end.
165-210 min	Coordination messages and state transitions	Three managers accept; case moves toward resolved.
210-255 min	React Flow decision graph and evidence drawer	Visual product is clear without explanation.
255-285 min	QuickNode/Solana hashing and verification	Decision receipt confirms; tamper demo fails.
285+ min	Polish, seed fallback, rehearse, record backup	Stable three-minute live path and recovery plan.

Build order rule

Do not begin with the graph or blockchain.

First make the live operational loop work: call -> transcript -> material event -> proactive SMS -> APPROVE -> coordination. Add visual depth and blockchain verification only after the core loop is stable.

15. Three-Minute Live Demonstration

Time	Action	What judges understand
0:00-0:20	Show ten locations and normal event stream. Owner does nothing.	This is a multi-location intelligence layer, not a single-call bot.
0:20-0:55	Judge calls Brickell and requests 300 pizzas.	A real conversation becomes operational data.
0:55-1:20	Constraint events arrive; graph connects order, promise, capacity, discount, and delivery risk.	AI understands cross-system context and employee roles.
1:20-1:45	Owner's phone receives proactive alert.	The owner did not know to ask; the system knew to interrupt.
1:45-2:05	Owner replies APPROVE.	Human authority remains explicit.
2:05-2:30	Managers receive assignments and accept; status turns green.	AI coordinates the business, not just summarizes it.
2:30-2:45	Show recurring-catering opportunity and protected revenue.	The product sees upside and downside.
2:45-3:00	Verify decision receipt, then demonstrate tamper failure.	Blockchain preserves the decision process rather than decorating the app.

Fallback strategy

- Keep one prerecorded call and transcript available, but continue the AI analysis, SMS approval, coordination, and blockchain steps live.
- Provide a "Replay event stream" button that deterministically restores the demonstration state.
- Allow manual injection of the call webhook payload if Retell delivery is delayed.
- Keep the Solana transaction signature from one successful run as a fallback while attempting a fresh anchor live.

16. Success Metrics and Business Model

Product metrics

Metric	Definition	Early target
Material-event precision	Share of immediate alerts judged worthy of owner interruption.	>80% in pilot review
Time to detection	Time from relevant evidence arrival to alert.	<60 seconds for calls
Evidence coverage	Material findings with traceable evidence.	100%
Resolution time	Time from alert to approved coordinated plan.	<5 minutes for supported cases
Noise suppression	Routine events that remain out of immediate alerts.	>95%
Revenue protected / created	Value of saved orders and identified opportunities.	Tracked per case
Risk intervention	High-severity events escalated before deadline or further action.	Tracked per case

Commercial hypothesis

OwnerRadar can begin as a managed intelligence layer for owner-operated groups that have five to fifty locations but lack a dedicated operations command center. Initial pricing should align with locations, connected channels, and event volume rather than individual employee seats.

Offer	Illustrative scope	Pricing hypothesis
Pilot	Up to 5 locations, phone + SMS + one operating feed, weekly tuning	Implementation fee plus \$750-\$1,500/month
Growth	6-20 locations, proactive alerts, cross-location coordination, analytics	Approximately \$150-\$400/location/month
Enterprise / operator group	Custom data sources, governance, audit, dedicated workflows	Annual contract and implementation

Pricing is a hypothesis for validation, not a committed public price list.

17. Privacy, Security, and Responsible Use

- Use only business communications and systems the organization is authorized to monitor and analyze.
- Provide clear employee notice and role-based access. Avoid covert consumer-style surveillance.
- Restrict sensitive HR, medical, payment, and customer data to recipients with a defined business need.
- Encrypt data in transit and at rest; use short retention for raw audio where possible.
- Store only cryptographic hashes and non-sensitive references on public blockchain infrastructure.
- Require human review for safety, employment, legal, financial, or reputational escalations.
- Log AI analysis versions and human overrides so the organization can audit mistakes and improve policies.
- Provide correction mechanisms when identity, role, or evidence correlation is wrong.

Language standards

Avoid	Use instead
"The company is liable."	"Potential exposure detected; human review required."
"The employee committed fraud."	"The refund pattern differs materially from the location baseline."
"The manager lied."	"The manager statement conflicts with the POS record."

Avoid	Use instead
"The AI made the decision."	"The AI recommended; the authorized person approved or overrode."

18. Post-Hackathon Roadmap

Phase	Capabilities
Phase 1 - Operational awareness	Real phone and SMS ingestion, alert tuning, role graph, owner approvals, daily digest.
Phase 2 - Business integrations	POS, inventory, scheduling, email, CRM, accounting, delivery and ticketing systems.
Phase 3 - Learned operating model	Infer recurring handoffs, bottlenecks, informal authority, single points of failure, and cross-location best practices.
Phase 4 - Coordinated execution	Approved inventory transfers, staffing offers, customer recovery, purchasing requests, and enterprise-account follow-up.
Phase 5 - Governance and assurance	Policy simulation, AI-agent oversight, insurer/auditor access, verified decision lineage across business entities.

Expansion beyond restaurants

- Roofing: major lead, insurance promise, crew capacity, permit and material dependencies
- Dental group: high-value patient inquiry, clinical boundary, appointment capacity, insurance preauthorization
- Property management: emergency maintenance, vendor authorization, resident communications, payer responsibility
- Auto repair: safety complaint, parts delay, estimate approval, loaner availability, warranty responsibility
- Home health: uncovered shift, caregiver qualification, payer coverage, family approval

19. Open Product Questions

- Should the initial commercial wedge be multi-location restaurants, home services, or fractional operating teams?
- Which event types can be acted upon automatically after a manager approves a standing policy?
- How should each owner tune alert thresholds without recreating a complex rules engine?
- What is the minimum evidence required before the system sends an immediate alert?
- How should employee notice, consent, and access vary by jurisdiction and communication channel?
- Is blockchain verification most valuable to owners, franchise networks, insurers, auditors, or cross-company partners?
- Should the product lead with "AI regional manager," "operational intelligence," or "business early-warning system"?

Appendix A. Seed Data for the Demo

Person	Personas / hats	Relevant authority
Sofia Alvarez	Brickell cashier; occasional catering coordinator; Downtown weekend employee	May accept routine orders; discounts up to 5%; orders over 75 pizzas require manager confirmation.
Luis Torres	Doral manager; regional delivery coordinator; emergency driver	May reassign Doral van and approve delivery routing.
Maya Chen	Coral Gables manager; purchasing approver	May accept production transfers and authorize emergency ingredients under \$1,000.
Andre Williams	Downtown kitchen lead; acting manager after 5 PM	May commit production capacity but cannot change customer price.
Marco Rivera	Owner; regional operator; final approver	May authorize cross-location plan, discount exception, and customer recovery.

Appendix B. Example Simulated Events

```

17:18:02 POS   Brickell   Order draft created: 300 pizzas
17:18:18 CALL  Brickell   Cashier promises 7:00 PM delivery
17:19:05 SMS   Brickell mgr "We only have dough for about 120"
17:19:44 CHAT   Doral     "Van 2 is back and available"
17:20:10 POS   Coral Gables Capacity forecast shows 100-pizza headroom
17:20:23 POS   Downtown  Capacity forecast shows 80-pizza headroom
17:20:42 CALL  Brickell   Cashier offers 12% discount
17:21:10 AI    Group     Materiality score crosses 90
17:21:14 TWILIO Owner     Proactive alert sent
17:21:51 SMS   Owner     APPROVE
17:22:02 TWILIO Managers  Production assignments dispatched

```

Appendix C. Definition of Done

- A person unfamiliar with the project can understand the business problem from the first screen in under ten seconds.
- The owner receives a real unsolicited text after the major order is detected.
- The alert explains both the upside and the risk, with specific evidence.
- Replying APPROVE produces visible coordination across multiple locations.
- The decision graph shows who made the original commitment and under which role.
- The case reaches a resolved state and creates a recurring-business opportunity.
- The verified record succeeds before tampering and fails after tampering.
- The entire live path fits within three minutes, with a deterministic fallback.