

Digital Maturity Assessment — ServiceCore Software

Sector: Vertical SaaS — Field Service Management (Trades / Home Services) | **Tier:** Express |
Thesis: Roll-up | **Lead:** Rob Freele | **Date:** 2026-06-01

Executive Summary

2026-06-01

EXECUTIVE SUMMARY — ServiceCore Software

Maturity Profile: ServiceCore Software exhibits an overall weighted digital maturity score of 1.35 / 3.00, placing the organization in the Low-to-Emerging band. Eight of eight material digital pillars show evidence of emerging or ad-hoc posture: architecture is monolithic and fragile (12-year-old Rails, manual deployments, no CI/CD); data foundation is operationally endemic to manual entry (60% contract rekeying, 5-6 hours/week lead re-entry); governance is informal and undocumented despite stated strategic priorities; security and resilience controls are incomplete (MFA on 3 of 6 systems, untested DR) and lack executive oversight; process automation is ad-hoc; analytics capability is stalled (failed PoC); and people/change management lacks formal program accountability despite recent capability hires. This is a high-capability team executing in a low-maturity operational structure.

Thesis Fit Assessment (Roll-up): ServiceCore's roll-up thesis requires organizational readiness for acquisition, integration into a larger parent platform, and margin expansion through operational leverage. Current maturity presents a mixed picture: **Strong alignment** exists around the strategic intent for automation, data cleanup, and security hardening (CEO, COO, CFO all acknowledge these priorities), and the team has demonstrated cultural commitment to execution (structured change management, recent RevOps hire). **Critical misalignment** is evident in the absence of formal governance structures and program accountability required for institutional buyer confidence and post-acquisition integration: no consolidated digital spend tracking, no documented decision-making forums, no roadmap with defined benefits, incomplete security controls, and architectural constraints that will impede scalability during a roll-up. The organization has solid engineering talent and clear operational pain points (3-day onboarding, 9-day close, manual rekeying, recurring outages), meaning the opportunity set is large and well-understood—but institutional maturity must increase significantly before close to meet buyer expectations.

Top 3 Risks (Deal-Breakers First):

1. **[Deal-breaker] Untested & Incomplete Security/Resilience Posture:** DR/BCP plan exists only as a paper tabletop exercise (October 2024) with documented RTO 4h/RPO 24h, but no live failover test has been executed. Database failover runbook contains a known gap that remains unremediated. MFA is not enforced on 3 of 6 critical systems, leaving privilege access vectors exposed to password-only authentication. For a business-critical SaaS platform supporting field service operations, untested DR and incomplete access controls represent material operational and reputational risk that must be remediated before close. **Mitigation:** Execute live DR failover test with full end-to-end validation and document measured RTO/RPO before close. Enforce MFA across all 6 critical systems as a hard requirement. Remediate all known runbook gaps and validate with CFO and COO that recovery windows align with business requirements.
2. **[Deal-breaker] Monolithic, Fragile Architecture Constrains Scalability & Operability:** The 12-year-old Rails monolith with zero CI/CD pipeline, manual SSH deployments (2x/week), and no infrastructure-as-code creates operational fragility (documented outages during month-end billing stress) and deployment risk. Point-to-point integrations (Stripe, Twilio, Salesforce-to-NetSuite) were built with inconsistent patterns, creating integration debt. For a roll-up platform that will integrate multiple acquired entities and scale customer volume, this architecture is a structural impediment to post-acquisition integration and margin expansion. **Mitigation:** Conduct architectural modernization assessment defining an 18–24 month roadmap to decompose monolith into domain-driven services with standardized APIs. Establish CI/CD pipeline (GitHub Actions or equivalent) and infrastructure-as-code (Terraform/CloudFormation) as immediate post-close priority. Implement standardized API/iPaaS layer to replace point-to-point integrations.
3. **[Deal-breaker] Formal Governance & Program Accountability Absence:** Budget and benefits tracking for digital/technology spend is fragmented across stale spreadsheets with no consolidated plan or formal monthly review. CFO has requested formal governance for over a year without traction. CEO acknowledges lower confidence in formal tracking discipline and prefers informal syncs. Governance meeting minutes are absent. Prior lesson from billing system rollout (lack of dedicated project owner) has not been formalized into process. For an institutional buyer conducting post-acquisition integration and value capture, this absence of formal governance, documented decisions, and benefit realization tracking is incompatible with fiduciary standards and board reporting requirements. **Mitigation:** Establish a formal monthly digital governance forum (CFO, COO, CTO, CEO) with consolidated initiative spend tracking, variance reporting, and benefits KPIs. Document all governance decisions with assigned owners and stage gates. Implement this forum by day 30 post-close as a condition of integration readiness.

Top 3 Opportunities (Quick Wins First, with Thesis-Alignment):

1. **[Quick Win] Enforce MFA Across All 6 Critical Systems:** Low effort, high impact, addresses deal-breaker security gap. Enforcement eliminates password-only authentication on 3 unprotected systems and materially improves access control posture within 30 days. **Thesis alignment:** Neutral (risk mitigation, not growth lever), but table-stakes for buyer governance.
2. **[Quick Win] Establish Formal Critical Vulnerability Patching SLA:** Define and document a formal patching cadence (target: 7–14 days for critical CVEs, replacing current informal 2–3 week window) and implement automated vulnerability scanning. Low effort, high impact on operational risk posture and cyber insurance requirements. Establish monthly executive reporting to CFO/board. **Thesis alignment:** Neutral (risk mitigation), but enables buyer to satisfy institutional risk governance.
3. **[Primary Thesis-Aligned Opportunity] Automate Order-to-Cash & Customer Onboarding Workflows:** Currently, 60% of new contracts are manually rekeyed from Salesforce into NetSuite, and customer onboarding requires 3 days of manual setup across CRM-billing-FSM. Implement Salesforce-to-NetSuite integration and automated provisioning workflow to eliminate manual rekeying and reduce onboarding to <1 day. **Thesis alignment:** Primary. This is a scalability lever for the roll-up—automated O2C reduces margin drag, eliminates operational bottleneck that constrains customer acquisition capacity, and provides a replicable operating model for acquired entities. Benefits: margin expansion (reduced labor), faster customer time-to-value (competitive moat), and replicable process template across portfolio. Target 60–90 days post-close with dedicated COO ownership.

Recommended Next Steps with Owner Roles:

- **[By close] CTO & CEO:** Remediate critical security gaps: (1) Test live DR failover, (2) Enforce MFA on 3 unprotected systems, (3) Document all pen-test findings and establish remediation backlog. Contingent on pass/fail before close.
- **[Days 1–30 Post-Close] CFO:** Establish formal monthly digital governance forum (attendees: CFO, COO, CTO, CEO). Consolidate existing digital initiative spend and map against strategy roadmap. Implement standardized initiative tracking template (budget, resource allocation, benefit realization KPIs).
- **[Days 1–90 Post-Close] COO:** Define and execute customer onboarding automation roadmap (Salesforce-to-NetSuite integration, automated provisioning). Assign dedicated ownership and resource (suggest Director of RevOps or newly-hired equivalent) to eliminate 3-day onboarding bottleneck.
- **[Days 1–90 Post-Close] CTO:** Implement CI/CD pipeline and infrastructure-as-code (GitHub Actions + Terraform) to reduce deployment friction and outage risk. Begin

architectural modernization assessment for 18–24 month monolith decomposition roadmap.

- **[Days 30–60 Post-Close] CTO:** Hire or assign dedicated Head of Security and establish security governance committee (CFO, CTO, COO) with quarterly board reporting. Establish formal patching SLA and vulnerability scanning cadence with monthly executive review.

Overall Investment Readiness: ServiceCore is a **Conditional Proceed** for roll-up acquisition contingent on **hard remediation of deal-breaker security and governance gaps before close and board-level commitment to formal governance and architecture modernization roadmap in first 100 days**. The organization has substantial value-creation potential (automation backlog, operational leverage, talented engineering team, clear pain points), but institutional maturity must increase significantly to meet buyer governance standards and de-risk post-acquisition integration. High execution risk in first 100 days if governance and architectural modernization are not formalized with dedicated resources and board accountability."

Cross-Pillar Commentary

CROSS-PILLAR PATTERN SYNTHESIS — ServiceCore Software

Root Cause #1: Absence of Formal Program Governance as System-Level Impediment

A single root cause cascades across Digital Strategy & Governance, Data Foundation, Process Automation, and People & Change: the absence of consolidated, formal governance discipline. The CFO has requested monthly digital spend tracking and governance review for over a year without "traction"—not because the CFO's request was unreasonable, but because the organization lacks the structural discipline to maintain formal forums, consolidated tracking, and documented decision-making. This gap manifests differently across pillars: in Strategy & Governance as missing governance meeting minutes and consolidated budgets; in Data Foundation as unknown ownership of data quality defects (orders table formatting flagged in audit but unassigned); in Process Automation as approximately 12 identified opportunities that remain unscoped and unprioritized; and in People & Change as absence of benefit realization tracking and program accountability. Strikingly, the CEO acknowledges the governance lesson from the prior billing system rollout (lack of dedicated project owner) but states this "hasn't [been] formalized that into a process yet"—suggesting the organization is aware of this gap but interprets informal execution as acceptable at current scale. For a roll-up thesis requiring institutional buyer confidence and post-acquisition integration, this is a deal-breaker: buyers cannot integrate ServiceCore into a

larger platform without formal governance infrastructure (monthly strategy reviews, consolidated spend tracking, documented decisions with assigned owners, stage-gated portfolio management). This gap compounds other pillars' immaturity rather than being isolated to governance.

Root Cause #2: Technical Debt as Foundation for Operational Manual Workarounds

A second system-level root cause—architectural and data foundation technical debt—drives the Process Automation and Data Foundation Low scores and constrains the roll-up thesis directly. The 12-year-old monolithic Rails architecture with no CI/CD, manual SSH deployments, and zero infrastructure-as-code creates deployment risk and constrains agility. The absence of a master data model, data lineage, and automated integrations forces manual data rekeying (60% of contracts manually re-entered from Salesforce into NetSuite, 5-6 hours/week of lead re-entry, customer onboarding requiring 3 days of manual setup). These are not independent failures—the monolithic architecture and fragmented integrations (point-to-point Stripe, Twilio, Salesforce-to-NetSuite) make automated, event-driven workflows infeasible. Thus, the organization "runs on people working hard to compensate for missing automation" (per COO), not because automation wasn't prioritized, but because the underlying technical foundation cannot support automated workflows without substantial modernization. For the roll-up thesis, this compounds scalability risk: as the parent platform acquires additional entities or scales customer volume, the monolithic core and manual O2C workflows will be a structural constraint on margin expansion. The initiative backlog correctly identifies this as Primary thesis-aligned (modernize architecture, automate O2C, implement MDM), but evidence shows that modernization has been "perpetually deprioritized against feature work due to lack of dedicated time and budget"—a symptom of root cause #1 (absent governance discipline) preventing resource allocation to technical debt paydown.

Root Cause #3: Critical Skill Gaps in Security & DevOps/SRE

A third root cause affecting Security & Resilience and People & Change is the absence of dedicated, in-house security and DevOps/SRE functions. Per CTO: the organization relies on a part-time external security consultant and lacks in-house DevOps/SRE capability; this "never had a strong enough business case to get budget prioritized." Security governance is absent at the executive level (per CFO: security has never been a budget line, and CFO is unfamiliar with DR status). This gap manifests as: untested DR with known runbook gaps, MFA not enforced on 3 of 6 critical systems, informal patching with no SLA, inability to produce pen-test report from "a couple years back," and no formal vulnerability scanning cadence. These are not technical oversights—they are governance and accountability gaps rooted in the absence of dedicated ownership. For the roll-up thesis, institutional buyers require formal security governance, board-level resilience reporting, and demonstrated operational maturity in risk management. ServiceCore's current posture (part-time consultant, no dedicated security budget, untested DR) is incompatible with this requirement and poses reputational

and operational risk during a roll-up acquisition where customer platform continuity is a buyer value-creation lever.

Compounding Effects: How Pillars Reinforce Each Other

These three root causes compound to create system-level risk:

- **Architecture → Automation → Data Foundation:** The monolithic architecture and absence of standardized integrations make process automation infeasible, forcing manual workflows (O2C, onboarding) that consume engineering and operations capacity. This prevents the organization from executing against the COO's identified automation opportunities, reinforcing manual operational drag. The manual workflows in turn create data quality issues (manual rekeying introduces transcription errors, inconsistent formatting in orders table goes unremediated due to unassigned ownership) and require 9-day month-end close periods due to manual reconciliation. Each pillar's Low score (Architecture, Process Automation, Data Foundation) is not independent—they reinforce each other into a mutually reinforcing cycle of operational friction.
- **Governance → People/Change → Security:** The absence of formal governance creates accountability and resource allocation failures. The CFO cannot establish consolidated spend tracking, the COO cannot formally prioritize automation opportunities, and the CTO cannot secure budget for security modernization or DevOps/SRE hiring. This cascades into People & Change gaps: the organization hires for capability (Director of RevOps, structured change management) but cannot formalize ownership or assign resources to critical risk mitigation (DR testing, MFA enforcement, security hiring). The result is emerging capabilities undermined by structural accountability gaps, with critical security work remaining undone due to "no business case strong enough to get budget."
- **Analytics Stalled by Architecture & Data Foundation:** The Analytics & AI PoC (lead-scoring model) stalled not because the analytics team lacked capability, but because "no clear owner, no monitoring infrastructure" existed—reflecting both governance failure (no owner assigned) and data/architecture immaturity (no monitoring infrastructure for operationalizing models in a fragmented integration landscape). This reinforces the cycle: without data foundation and monitoring capability, analytics cannot scale; without formal governance, analytics investments cannot be prioritized or sustained.

Thesis-Readiness Implications: Why This Maturity Profile Creates Deal-Breaker Risk for Roll-Up

ServiceCore's roll-up thesis positions the organization for acquisition and integration, requiring three parallel value-creation levers:

1. **Risk & Resilience:** Remediating critical security and operational gaps (DR testing, MFA enforcement, patching SLA, formal security governance)

2. **Scalability:** Modernizing monolithic architecture (CI/CD, API layer, infrastructure-as-code) and automating manual workflows (O2C, onboarding) to create margin expansion and replicable operating model
3. **Portfolio Integration:** Establishing formal governance and program accountability to integrate ServiceCore into parent platform with consolidated budget tracking, defined benefits realization, and executive alignment

Current maturity (1.35 / 3.00) shows the organization is **partially capable on strategic intent but structurally immature on execution discipline:**

- **Intent is clear:** CEO, COO, CFO all articulate automation, data cleanup, and security hardening as top priorities. The team understands the problems (9-day close, 3-day onboarding, untested DR, monolithic bottlenecks).
- **Execution is ad-hoc:** Governance is informal and undocumented. Resource allocation follows "no traction" patterns (CFO's governance requests) or perpetual deprioritization (CTO's modernization pleas). Ownership of critical work (data quality remediation, DR testing, security hiring) is ambiguous or absent.
- **Technical capability exists but is constrained:** The engineering team is strong on backend; the COO has introduced structured change management; the CEO and CFO are operationally engaged. But these capabilities cannot drive scale without formal governance, architectural modernization, and security function hiring.

The core deal-breaker risk is not technical capability—it is institutional immaturity. A buyer acquiring ServiceCore for roll-up requires:

- Formal monthly governance forums with consolidated spend tracking and benefits realization KPIs (to integrate into parent platform governance)
- Tested DR and complete security controls (to meet institutional risk and insurance requirements)
- Modernized architecture and automated workflows (to provide margin expansion and replicable operating model for acquired entities)

ServiceCore's current state shows strategic alignment on all three, but structural unreadiness on execution discipline. The organization needs its own "100-day program" of governance formalization (formal monthly reviews, consolidated tracking, dedicated program ownership) and critical risk remediation (live DR test, MFA enforcement, security hiring) **before close** to be acquisition-ready. Without this, the buyer inherits not just technical debt, but governance and accountability debt that will impede integration velocity and value realization.

Recommended Framing for IC: ServiceCore is a **Conditional Proceed**—strong strategic fit and operational pain-point clarity, substantial value-creation upside in automation and margin expansion, but **hard preconditions on deal-breaker governance and security remediation before close**. Formalize these preconditions in SPA and include holdback/escrow

contingent on post-close governance and architecture modernization milestones. The 100-day plan is not a nice-to-have—it is a structural prerequisite for integration success."

Pillar Score Heatmap

Pillar	Score	Weighted	Confidence	Re-scored
Digital Strategy & Governance	Medium	0.300	Medium	
Data Foundation	Low	0.150	Medium	
Architecture	Low	0.150	Medium	
Application Portfolio Health	Medium	0.200	High	
Process Automation	Low	0.150	Medium	
Analytics & AI	Low	0.100	Medium	
Security & Resilience	Low	0.100	Low	✓
People & Change	Medium	0.200	Medium	
Overall		1.350 / 3.000	(45.0%)	

Overall weighted score: 1.350 / 3.000 (45.0%)

Pillar-by-Pillar Detail

Digital Strategy & Governance

Score: Medium | Confidence: Medium | Weighted: 0.300

Score: Medium | Confidence: Medium. ServiceCore exhibits emerging but fragmented digital governance. The CEO maintains a strategic roadmap with quarterly OKR reviews and documented top-three priorities (automation, data cleanup, security hardening), supported by informal weekly leadership syncs. However, CFO-provided evidence reveals a material

accountability gap: budget tracking is fragmented across stale spreadsheets with no consolidated plan, and a formal monthly governance review requested over a year ago has received 'no traction.' Governance meeting minutes are absent from artifacts. The CEO acknowledges the lesson from the prior billing system rollout (lack of dedicated project owner) but states this 'hasn't [been] formalized that into a process yet.' While strategic intent is communicated, the absence of consolidated spend tracking, formal monthly reviews with documented decisions, and stage-gated portfolio management prevents the organization from managing digital initiatives as a coherent product roadmap with measurable benefits—a material governance gap for investor-stage maturity. **Recommendation:** Establish a formal monthly digital governance forum (CFO, COO, CTO, CEO) with consolidated initiative spend tracking, variance reporting (actual vs. budget), and benefits realization KPIs. Assign a single executive owner for portfolio backlog prioritization and formalize governance decision-making with stage gates and documented owners.

Data Foundation

Score: Low | **Confidence:** Medium | **Weighted:** 0.150

Score: Low | Confidence: Medium. The data foundation is solidly in the Ad-hoc category despite the CTO's statement that the core data model is 'reasonably solid.' Evidence reveals pervasive operational and governance failures: (1) known data quality defects—inconsistent currency and state field formatting on the orders table flagged in recent audit—remain unaddressed and unowned; (2) manual data entry is operationally endemic—60% of new contracts are manually rekeyed from Salesforce into NetSuite, leads are manually re-entered across HubSpot-Salesforce-NetSuite (5-6 hours/week), and churn is tracked in a manually-maintained shared spreadsheet with inconsistent updates; (3) no master data management, documented lineage, or single source of truth exists; (4) multiple point-to-point integrations (Stripe, Twilio, Salesforce-to-NetSuite) were built with inconsistent patterns, and a lead-scoring proof-of-concept stalled due to lack of ownership and monitoring infrastructure. Month-end close takes 9 business days largely due to manual reconciliation, indicating that manual processes are a functional necessity rather than edge cases. The absence of data governance infrastructure and reliance on workarounds confirm Low maturity.

Recommendation: Immediately conduct root-cause analysis for the orders table data quality defects and establish remediation plan with clear ownership before close. In parallel, establish a data governance committee with assigned Data Owner, document integrations and lineage, and implement an automated order-to-cash provisioning workflow to eliminate manual rekeying by day 100.

Architecture

Score: Low | **Confidence:** Medium | **Weighted:** 0.150

Score: Low | Confidence: Medium. The core platform architecture is a 12-year-old monolithic Rails application with no modularity, no API-first design, and fragile point-to-point integrations built inconsistently over time. Per CTO: no infrastructure-as-code exists, environments are managed manually via SSH scripts, and deployments occur roughly twice weekly with zero automated CI/CD pipeline. This manual, ad-hoc foundation is operationally validated—per COO, the platform has experienced documented outages during high-traffic periods (month-end billing runs) directly attributed to monolithic bottlenecks. The CTO acknowledges a desire to modernize toward API-first/modular architecture but reports this has been perpetually deprioritized against feature work due to lack of dedicated time and budget. The team is strong on backend engineering but thin on DevOps/SRE. The absence of formal instrumentation (deploy frequency, lead time) and the recurrence of outages under production stress patterns indicate operational fragility masked by informal capability.

Recommendation: Conduct an architectural modernization assessment defining an 18–24 month roadmap to decompose the core monolith into domain-driven services with standardized APIs and event-driven patterns. Immediately implement infrastructure-as-code (Terraform/CloudFormation) and an automated CI/CD pipeline (e.g., GitHub Actions) as a post-close priority to reduce deployment friction, improve lead time, and eliminate outage risk.

Application Portfolio Health

Score: Medium | Confidence: High | Weighted: 0.200

Score: Medium | Confidence: High. Application Portfolio Health demonstrates mixed maturity with clear evidence supporting a Medium rather than Low rating. Strengths: the core platforms are on current versions, SLOs are reportedly met, and the supporting SaaS portfolio is well-managed—the COO recently consolidated from 14 tools to 6 with quarterly license utilization reviews now in place, indicating disciplined vendor governance. However, critical gaps prevent a High score: the 12-year-old monolithic Rails core (per CTO) with manual SSH-based deployments twice weekly and zero CI/CD pipeline creates deployment risk; no formal instrumentation of deploy frequency or lead time metrics exists despite SLO claims; and per COO, the platform has experienced several documented outages in the past year, typically during high-traffic windows like month-end billing runs—a recurrent pattern tied to monolithic architecture constraints. This tension between CTO's claim that SLOs are 'generally met' and COO's observation of recurring outages suggests the portfolio meets bare technical metrics but cannot reliably handle production stress patterns. This is operational fragility masked by selective metrics—a hallmark of Emerging portfolio maturity. **Recommendation:** Establish formal SLO/RTO instrumentation and capacity planning discipline. Load-test month-end billing processes and implement circuit-breaker patterns, horizontal scaling (containerization, orchestration), and monitoring/alerting to eliminate the recurring outage

pattern. Document SLOs and RTO/RPO targets and track lead time and deployment frequency metrics.

Process Automation

Score: Low | **Confidence:** Medium | **Weighted:** 0.150

Score: Low | Confidence: Medium. Evidence demonstrates a predominantly manual operational posture across customer-facing and financial processes. Per COO: customer onboarding requires 3 days of manual rekeying across CRM, billing, and FSM with no automated provisioning workflow; support ticket triage is entirely manual with no routing rules. Per CFO: month-end close takes 9 days due to manual reconciliation, and 60% of new contract data is manually re-entered from Salesforce into NetSuite. Per CTO: no CI/CD pipeline exists; deploys occur via SSH scripts twice weekly. The COO explicitly states the business 'runs on people working hard to compensate for missing automation'—a direct indicator of ad-hoc operational posture. While the COO has informally identified approximately 12 automation opportunities, none are formally sized, prioritized, or included in a documented automation backlog. This is consistent with Low-maturity operations where manual workarounds are the dominant pattern and the absence of process maps or automation governance. **Recommendation:** Develop and formally scope a phased customer onboarding automation roadmap targeting CRM-billing-FSM integration within 60–90 days post-close. Assign dedicated ownership to eliminate the manual rekeying bottleneck. Simultaneously, implement Salesforce-to-NetSuite middleware or integration to automate contract re-entry and reduce month-end close cycle time from 9 days to target 3 days.

Analytics & AI

Score: Low | **Confidence:** Medium | **Weighted:** 0.100

Score: Low | Confidence: Medium. The organization exhibits no deployed predictive models or evidence of analytics-driven decision making at scale. Per CTO: a lead-scoring AI model was built as a proof-of-concept approximately one year ago but 'never made it to production—no clear owner, no monitoring infrastructure, the project quietly stalled.' CMO_CRO corroborates this stalled state, citing lack of resources to operationalize. The organization relies primarily on Salesforce dashboards that CMO_CRO characterizes as 'good enough for forecasting' but which 'lack granular attribution by channel.' Campaign performance is reviewed 'manually in spreadsheets monthly' (CMO_CRO) with no multi-touch attribution capability; budget allocation decisions 'lean more on instinct than data.' Per CFO: budget visibility is 'fragmented across spreadsheets that go stale within a month' and 'can't report ROI on prior automation investments because no consistent tracking exists.' Churn driver analysis 'currently requires manual cross-checking with the CS team' (COO), indicating analytics capability is insufficient even for core operational questions. All structured reporting

is ad-hoc and manual, falling well below the Emerging/Optimizing threshold.

Recommendation: Operationalize the stalled lead-scoring model with clear ownership, production monitoring, and defined KPIs within 60 days post-close. Build a churn driver analytics dashboard and establish a formal monthly business review cadence tied to consolidated budget and benefits tracking to enable data-driven decision making.

Security & Resilience (*re-scored after follow-up*)

Score: Low | **Confidence:** Low | **Weighted:** 0.100

Score: Low | **Confidence:** Low. [RE-SCORED after follow-up.] Evidence quality is Low, triggering the Low default rule; however, the underlying risk profile warrants explicit articulation. Critical gaps are pervasive: (1) Per CTO, MFA is enabled on only 3 of 6 critical systems, leaving remaining privilege access vectors protected by password-only authentication; (2) DR/BCP plan is untested in live execution—only a tabletop exercise was conducted in October 2024 with documented RTO (4h) and RPO (24h), but no live failover test has been executed, and the database failover runbook contains a known gap that has not been remediated; (3) Patching is informal with no SLA, addressing critical CVEs within 2–3 weeks with no formal cadence; (4) Pen-test report cannot be produced ('couple years back'), findings are not recalled, and no artifact trail of remediation exists; (5) Security staffing is thin, relying on a part-time external consultant rather than an in-house function; (6) Per CFO, security has never been a budget line, indicating no tracked governance or investment discipline, and CFO is unfamiliar with DR status, indicating weak resilience oversight at the executive level. The combination of untested DR with known runbook gaps, incomplete MFA coverage, informal patching, missing governance artifacts, and unclear executive visibility indicates systems-level immaturity that poses operational risk for a business-critical SaaS platform. **Recommendation:** Before close, enforce MFA across all 6 critical systems, execute a live DR failover test with full end-to-end validation and documented RTO/RPO, and remediate all known runbook gaps. Define a formal critical vulnerability patching SLA (target: 7–14 days) with monthly reporting. Commission an independent penetration test with full documentation and establish annual pen-test cadence. Hire a dedicated Head of Security pre-close or establish firm post-close hiring milestones with board accountability.

People & Change

Score: Medium | **Confidence:** Medium | **Weighted:** 0.200

Score: Medium | **Confidence:** Medium. People & Change demonstrates emerging capability with intentional efforts to professionalize digital operations, but material gaps in formal governance and accountability prevent a High rating. Positive evidence: CEO recently approved hiring a Director of RevOps (reporting to COO) following lessons from a prior billing system rollout, and COO has implemented structured change management for major

releases including training, office hours, and release notes—these represent active, structured investments in capability. However, critical gaps undermine these efforts: (1) CFO has requested formal monthly governance and budget tracking for 'over a year without getting traction,' describing budget visibility as 'fragmented across spreadsheets that go stale within a month' with 'nothing getting tracked formally after Monday syncs'; (2) CEO acknowledges lower confidence in 'formal tracking and reporting discipline' and prefers informal weekly syncs, which COO finds insufficient given operational friction from missing automation prioritization; (3) CTO reports the engineering team is 'thin on DevOps/SRE and security,' relying on a part-time external consultant, and states this 'never had a strong enough business case to get budget prioritized'—reflecting skill gaps and resource allocation discipline failures at leadership level. The leadership team demonstrates strategic alignment on priorities and cultural commitment to execution, but formal governance, program accountability, and strategic resource allocation remain ad hoc. **Recommendation:** Establish formal program governance with consolidated digital initiative tracking, defined resource ownership, and quarterly benefits realization reviews. Conduct a security and DevOps/SRE capability assessment and budget for a dedicated Head of Security and Senior DevOps Engineer pre-close or establish firm post-close hiring milestones with board accountability.

Risk Register

Architecture — 12-year-old monolithic Rails application with no modularity, no API-fi

- **Severity:** High | **Category:** Deal-breaker
- **Owner:** CTO
- **Mitigation:** Conduct architectural modernization assessment and define 18–24 month roadmap to decompose core monolith into domain-driven services with standardized APIs and event-driven patterns where appropriate. Establish automated CI/CD pipeline and infrastructure-as-code (Terraform/CloudFormation) as immediate post-close priority to reduce deployment friction and outage risk.

Security & Resilience — DR/BCP plan is untested in live execution. CTO confirmed only a tablet

- **Severity:** High | **Category:** Deal-breaker
- **Owner:** CTO
- **Mitigation:** Conduct a live DR failover test with full end-to-end validation before close, document results with measured RTO/RPO, and remediate all known runbook gaps.

Include post-test review with CFO and COO to validate recovery window assumptions against business requirements.

People & Change — Critical skill gaps in security and DevOps/SRE functions. Security fun

- **Severity:** High | **Category:** Deal-breaker
- **Owner:** CTO
- **Mitigation:** Conduct a security risk and DevOps/SRE capability assessment as a condition of close. Budget and hire a dedicated Head of Security and Senior DevOps Engineer pre-close or establish firm post-close hiring milestones with accountability to board. Without in-house security leadership, the company cannot meet institutional buyer governance requirements.

Digital Strategy & Governance — Budget and benefits tracking for digital/technology spend is fragmente

- **Severity:** High | **Category:** 100-Day Priority
- **Owner:** CFO
- **Mitigation:** Establish a formal monthly governance review forum with documented attendees, decisions, and owners. Implement consolidated digital initiative spend tracking tied to the strategic roadmap, with monthly variance reporting (actual vs. budget, benefits realized vs. plan) visible to leadership and board.

Digital Strategy & Governance — Governance decision-making and portfolio prioritization remain informa

- **Severity:** High | **Category:** 100-Day Priority
- **Owner:** CEO
- **Mitigation:** Document and formalize governance decision-making with a structured forum that meets at defined cadence, records decisions and owners, and includes stage gates for major initiatives. Assign a single executive owner (likely COO or Chief Digital Officer role) for portfolio backlog prioritization and resource allocation.

Data Foundation — Known data quality defects (inconsistent currency and state field form

- **Severity:** High | **Category:** 100-Day Priority
- **Owner:** CTO

- **Mitigation:** Establish root-cause analysis and data remediation plan for orders table before close. Define and assign clear ownership for data quality governance and establish automated validation checks for currency and state fields.

Data Foundation — Manual data entry consumes 5-6 hours per week across revenue operation

- **Severity:** High | **Category:** 100-Day Priority
- **Owner:** CFO
- **Mitigation:** Audit the Salesforce-to-NetSuite integration for data leakage points and validate completeness. Establish an automated order-to-cash provisioning workflow and a master customer data model to eliminate manual rekeying by day 100.

Data Foundation — No documented data lineage, data dictionary, or master data management

- **Severity:** High | **Category:** 100-Day Priority
- **Owner:** CTO
- **Mitigation:** Establish a data governance committee and assign a Data Owner/CDO-equivalent role. Document current integrations, create a data lineage diagram, and define standards for future integration patterns. Implement a data quality monitoring dashboard covering high-risk sources (orders, customer, churn).

Architecture — Platform has experienced documented outages during high-traffic period

- **Severity:** High | **Category:** 100-Day Priority
- **Owner:** COO
- **Mitigation:** Establish monitoring, alerting, and capacity planning discipline post-close. Identify month-end billing bottlenecks through load testing and implement circuit-breaker patterns and horizontal scaling capability (containerization, orchestration) to handle peak traffic. Document SLOs and RTO/RPO targets.

Process Automation — Customer onboarding requires 3 days of manual rekeying with no automat

- **Severity:** High | **Category:** 100-Day Priority
- **Owner:** COO
- **Mitigation:** Develop and scope a phased customer onboarding automation roadmap targeting CRM-billing-FSM integration within 60–90 days post-close. Assign dedicated

ownership to eliminate manual rekeying bottleneck.

Process Automation — Month-end financial close requires 9 days due to manual reconciliation

- **Severity:** High | **Category:** 100-Day Priority
- **Owner:** CFO
- **Mitigation:** Implement Salesforce-to-NetSuite integration or middleware to eliminate manual contract re-entry. Establish formal monthly governance cadence to track automation benefits and digital spend against plan.

Security & Resilience — MFA is not enforced across all critical systems. Per CTO: only 3 of 6

- **Severity:** High | **Category:** 100-Day Priority
- **Owner:** CTO
- **Mitigation:** Audit all critical systems, identify the 3 without MFA, and enforce MFA across 100% of critical systems before close or as a post-close condition with escrow holdback. Document the rollout plan and test MFA enforcement in each environment.

Security & Resilience — Patching process lacks formal SLA or cadence. Per CTO: critical CVEs a

- **Severity:** High | **Category:** 100-Day Priority
- **Owner:** CTO
- **Mitigation:** Define and document a formal patching SLA for critical CVEs (target: 7–14 days from disclosure). Implement automated vulnerability scanning and establish a monthly patch cadence with playbooks for emergency patches. Assign accountability to CTO and track metrics post-close.

People & Change — Absence of formal program governance and benefits tracking for digital

- **Severity:** High | **Category:** 100-Day Priority
- **Owner:** CFO
- **Mitigation:** Establish a formal monthly digital program governance forum (CFO, COO, CTO, CEO) with a standardized tracker linking approved initiatives to budget, resource allocation, and benefit realization. Begin with a 90-day sprint to consolidate existing spend and map against strategy.

Digital Strategy & Governance — Digital initiatives are communicated informally and tracked as project

- **Severity:** Medium | **Category:** 100-Day Priority
- **Owner:** CFO
- **Mitigation:** Transition from project-based tracking to product/initiative roadmap with stage gates and benefits KPIs (e.g., ROI, process time savings, cost reduction). Establish a mandatory benefits realization checkpoints at 90 days post-launch for all material initiatives.

Data Foundation — Churn tracking relies on a manually-maintained shared spreadsheet upda

- **Severity:** Medium | **Category:** 100-Day Priority
- **Owner:** CMO_CRO
- **Mitigation:** Build or integrate a churn tracking dashboard tied to CRM systems with automated alerts. Define churn calculation logic and assign ownership for data maintenance and accuracy validation.

Architecture — No infrastructure-as-code, formal architecture decision records, or te

- **Severity:** Medium | **Category:** 100-Day Priority
- **Owner:** CTO
- **Mitigation:** Hire or assign dedicated DevOps/SRE resource post-close. Implement IaC tooling (Terraform, CloudFormation) and establish CI/CD platform (GitHub Actions, GitLab CI, or equivalent). Create and maintain architecture decision record (ADR) log and living tech debt register to guide modernization roadmap.

Security & Resilience — Security governance is absent at executive level. Per CFO: security ha

- **Severity:** Medium | **Category:** 100-Day Priority
- **Owner:** CFO
- **Mitigation:** Establish a security governance committee with CFO, CTO, and COO as core members. Create a dedicated security budget line and quarterly security/resilience reporting cadence to the board. Assign ownership of DR status, patch metrics, and compliance posture.

Security & Resilience — Pen-test findings are undocumented and untracked. Per CTO: previous pe

- **Severity:** Medium | **Category:** 100-Day Priority
- **Owner:** CTO
- **Mitigation:** Commission an independent, current penetration test with full scope and documented findings. Create a remediation backlog with severity levels and timelines. Establish annual or bi-annual pen-test cadence and archive all findings and remediation evidence.

People & Change — Operational drag from missing automation creating unsustainable margin

- **Severity:** Medium | **Category:** 100-Day Priority
- **Owner:** COO
- **Mitigation:** Prioritize automation roadmap within the first 100 days post-close. COO to produce a detailed automation business case linking margin impact to resource requirements and escalate to CEO/board for formal prioritization and funding commitment.

Process Automation — No infrastructure-as-code, CI/CD pipeline, or deployment automation: p

- **Severity:** Medium | **Category:** Post-Close Watch Item
- **Owner:** CTO
- **Mitigation:** Within 6 months post-close, establish a CI/CD pipeline and basic infrastructure-as-code to reduce manual deployment risk and improve cycle time. Prioritize this in tandem with modernization planning.

Initiative Backlog

1. Enforce multi-factor authentication (MFA) across all 6 critical systems and eliminate password-only access 🏃 Quick Win ⚠️ Deal-Breaker Link

Pillar: Security & Resilience | **Lever:** Risk & Resilience | **Effort:** Low | **Impact:** High | **Thesis:** Neutral | **Placement:** 100-Day

Assumptions: Assumes MFA is technically feasible on systems currently lacking it (3 of 6 have MFA, 3 do not); assumes rollout effort is primarily user enablement and policy enforcement

rather than infrastructure; confidence is Low due to incomplete visibility on actual system compliance and technical constraints.

2. Establish formal critical vulnerability patching SLA with defined cadence and monthly executive reporting 🏃 Quick Win ⚠️ Deal-Breaker Link

Pillar: Security & Resilience | **Lever:** Risk & Resilience | **Effort:** Low | **Impact:** Medium | **Thesis:** Neutral | **Placement:** 100-Day

Assumptions: Assumes 2–3 week informal critical patch cycle can be formalized into an SLA without undue operational burden; assumes CTO or external security consultant can define and enforce cadence; confidence is Low due to sparse evidence on actual current patch capability and risk exposure window.

3. Test live DR failover and remediate known database failover runbook gaps; document RTO/RPO for all critical systems ⚠️ Deal-Breaker Link

Pillar: Security & Resilience | **Lever:** Risk & Resilience | **Effort:** Medium | **Impact:** High | **Thesis:** Neutral | **Placement:** 100-Day

Assumptions: Assumes tabletop exercise RTO/RPO (4h/24h) are realistic targets for live failover; assumes database runbook gap is scoped and remediable; assumes CTO can orchestrate live test without unacceptable downtime risk; confidence is Low due to sparse evidence on current failover capability and infrastructure readiness.

4. Replace point-to-point integrations (Stripe, Twilio, Salesforce-to-NetSuite) with standardized API/iPaaS layer ⚠️ Deal-Breaker Link

Pillar: Architecture | **Lever:** Risk & Resilience | **Effort:** High | **Impact:** High | **Thesis:** Neutral | **Placement:** 100-Day

Assumptions: Assumes point-to-point integrations are major source of operational fragility (per CTO on inconsistent patterns); assumes modernization deprioritization reflects resource constraint rather than technical disagreement; assumes 6–12 month implementation on 12-year monolith.

5. Implement infrastructure-as-code and automated CI/CD pipeline for 12-year-old Rails monolith ⚠️ Deal-Breaker Link

Pillar: Architecture | **Lever:** Scalability | **Effort:** High | **Impact:** High | **Thesis:** Primary | **Placement:** 100-Day

Assumptions: Assumes manual SSH deployments are directly constraining feature velocity and reliability (recurring outages during month-end runs); assumes engineering team has backend

strength but lacks DevOps capacity; assumes 6–12 month engagement with external DevOps support likely required.

Full Opportunity Inventory

Digital Strategy & Governance

Establish formal monthly digital governance forum with consolidated budget and benefits tracking [Quick Win]

Lever: Multiple & Narrative Readiness | Effort: Low | Impact: High | Confidence: Medium |

Thesis: Secondary

Assumes CEO will commit to monthly cadence and documented decisions; current informal preference for weekly syncs suggests cultural resistance to formalization.

Build consolidated digital/technology initiative roadmap with stage gates, approval criteria, and assigned portfolio owners

Lever: Multiple & Narrative Readiness | Effort: Medium | Impact: High | Confidence: Medium |

Thesis: Secondary

Assumes CEO and CFO align on portfolio governance model and acceptance of formal decision framework; current lesson from billing system stall (no owner assigned) indicates willingness but no follow-through.

Implement monthly digital benefits realization tracking against approved plan with accountability by initiative owner [Quick Win]

Lever: Multiple & Narrative Readiness | Effort: Low | Impact: Medium | Confidence: Medium |

Thesis: Secondary

Assumes CFO leadership and willingness to enforce tracking discipline post-approval; fragmented spreadsheet tracking suggests data exists but is not consolidated.

Data Foundation

Remediate known data quality defects in orders table (currency, state field formatting) and assign ownership [Quick Win]

Lever: Cost Reduction | Effort: Low | Impact: Medium | Confidence: Medium | Thesis:

Secondary

Assumes defects are well-scoped and documented from recent audit; assumes CTO or data team can prioritize remediation within 100-day window.

Implement master data management for core entities (customers, orders, products) with single source of truth and documented lineage

Lever: Cost Reduction | Effort: High | Impact: High | Confidence: Medium | Thesis: Secondary
Assumes manual rekeying is the largest operational drag (per COO); assumes existing data model ('reasonably solid' per CTO) can serve as foundation; assumes 3–6 month implementation horizon given infrastructure and process change required.

Deploy automated data quality monitors on top revenue-driving tables (orders, leads, contracts) with alerting

Lever: Cost Reduction | Effort: Medium | Impact: Medium | Confidence: Medium | Thesis: Secondary

Assumes monitoring infrastructure can be built on top of existing integrations; assumes known quality issues (currency, state formatting) are representative of broader data hygiene risk.

Build searchable data catalog with automated lineage documentation for core systems (NetSuite, Salesforce, billing)

Lever: Scalability | Effort: Medium | Impact: Medium | Confidence: Medium | Thesis: Primary
Assumes multiple point-to-point integrations (Stripe, Twilio, Salesforce-to-NetSuite) create sufficient lineage complexity to justify catalog investment; assumes stalled lead-scoring PoC reflects ownership/documentation gap that catalog would mitigate.

Establish formal data governance forum with assigned MDM owner and monthly data quality review cadence [Quick Win]

Lever: Cost Reduction | Effort: Low | Impact: Medium | Confidence: Medium | Thesis: Secondary

Assumes CTO and CFO can dedicate monthly review time; assumes known issues (orders table, churn spreadsheet) represent governance rather than technical gaps.

Architecture

Replace point-to-point integrations (Stripe, Twilio, Salesforce-to-NetSuite) with standardized API/iPaaS layer

Lever: Risk & Resilience | Effort: High | Impact: High | Confidence: Medium | Thesis: Neutral

Assumes point-to-point integrations are major source of operational fragility (per CTO on inconsistent patterns); assumes modernization deprioritization reflects resource constraint rather than technical disagreement; assumes 6–12 month implementation on 12-year monolith.

Implement infrastructure-as-code and automated CI/CD pipeline for 12-year-old Rails monolith

Lever: Scalability | Effort: High | Impact: High | Confidence: Medium | Thesis: Primary

Assumes manual SSH deployments are directly constraining feature velocity and reliability (recurring outages during month-end runs); assumes engineering team has backend strength but lacks DevOps capacity; assumes 6–12 month engagement with external DevOps support likely required.

Establish tech debt register and prioritized burn-down plan with assigned engineering owner

Lever: Multiple & Narrative Readiness | Effort: Medium | Impact: Medium | Confidence: Medium | Thesis: Secondary

Assumes monolithic architecture and manual deployments represent substantial undocumented debt; assumes formal register would support investor narrative and prioritization discipline that currently lacks.

Application Portfolio Health

Rationalize and consolidate redundant/overlapping applications in supporting SaaS portfolio

Lever: Cost Reduction | Effort: Low | Impact: Low | Confidence: High | Thesis: Secondary

COO has already reduced portfolio from 14 to 6 tools with quarterly license reviews in place; assumes further consolidation opportunity is limited and low-impact; includes this for completeness but not as priority.

Implement formal right-sizing and shelfware elimination program for licensing across core platforms (Salesforce, NetSuite)

Lever: Cost Reduction | Effort: Low | Impact: Low | Confidence: High | Thesis: Secondary

Evidence shows quarterly license utilization reviews already in place; additional optimization likely marginal; included for completeness.

Process Automation

Automate customer onboarding workflow (CRM, billing, FSM provisioning) to eliminate 3-day manual rekeying cycle

Lever: Cost Reduction | Effort: High | Impact: High | Confidence: Medium | Thesis: Secondary

Assumes 3-day manual rekeying is accurately scoped and repeatable across new customers; assumes workflow orchestration capability can be added to monolithic platform or via iPaaS; assumes 6–9 month implementation horizon given current architecture state and DevOps capacity constraint.

Automate order-to-cash financial close workflow to eliminate 60% manual contract re-entry and reduce 9-day close cycle

Lever: Cost Reduction | Effort: High | Impact: High | Confidence: Medium | Thesis: Secondary

Assumes 60% manual re-entry and 9-day close cycle are well-documented operational constraints; assumes CFO can specify automation requirements; assumes integration across Salesforce, NetSuite, and billing system required; assumes 6–12 month implementation horizon given complexity.

Build formal process maps and automation backlog for top 10 opportunities; establish automation governance and prioritization framework

Lever: Multiple & Narrative Readiness | Effort: Medium | Impact: Medium | Confidence: Medium | Thesis: Secondary

Assumes COO has identified ~12 opportunities but lacks formal scoping or prioritization; assumes business cases and effort estimates will support investment decisions and investor-facing narrative.

Implement support ticket routing automation with SLA-driven triage rules to replace manual sorting

Lever: Cost Reduction | Effort: Medium | Impact: Low | Confidence: Medium | Thesis: Secondary

Assumes 6-person support team manually triages tickets with no tooling; assumes impact is contained to operational efficiency within a single function rather than business-wide; assumes medium effort due to workflow configuration and training required.

Analytics & AI

Operationalize lead-scoring model stalled at PoC with assigned ownership, monitoring infrastructure, and integration to CRM

Lever: Revenue Growth | Effort: Medium | Impact: Medium | Confidence: Low | Thesis: Neutral
Assumes PoC model is salvageable and business case is compelling; assumes lack of ownership and monitoring was the stall reason (not model performance); assumes CMO_CRO and CTO can dedicate resourcing post-100-day window; actual revenue impact uncertain without model performance data.

Deploy operational dashboards for top 3 decision drivers (sales pipeline, churn risk, margin by customer segment) in regular use [Quick Win]

Lever: Revenue Growth | Effort: Low | Impact: Medium | Confidence: Medium | Thesis: Neutral
Assumes Salesforce dashboards exist but lack granular attribution and are not actively used for decisions (CMO_CRO: 'good enough for forecasting' but missing channel detail); assumes dashboard build can leverage existing data and configuration; assumes adoption and habit-change will drive impact.

Implement churn prediction model and at-risk account alerting integrated to CRM workflow

Lever: Revenue Growth | Effort: Medium | Impact: High | Confidence: Low | Thesis: Neutral
Assumes churn drivers can be extracted from manual CS team cross-checks and formalized into predictive features; assumes model would directly support retention strategy and identify at-risk cohorts; assumes lack of systematic churn tracking (spreadsheet-based) means model is currently infeasible but high-value if data gaps are closed.

Build multi-touch campaign attribution model and implement A/B testing framework for marketing spend optimization

Lever: Revenue Growth | Effort: High | Impact: Medium | Confidence: Low | Thesis: Neutral

Assumes CMO_CRO budget allocation decisions currently rely on instinct rather than data, but model accuracy and adoption risk are high; assumes fragmented lead re-entry (HubSpot → Salesforce → NetSuite) introduces data quality risk that must be resolved first; assumes 6–9 month horizon including data cleanup and model validation.

Security & Resilience

Test live DR failover and remediate known database failover runbook gaps; document RTO/RPO for all critical systems

Lever: Risk & Resilience | Effort: Medium | Impact: High | Confidence: Low | Thesis: Neutral

Assumes tabletop exercise RTO/RPO (4h/24h) are realistic targets for live failover; assumes database runbook gap is scoped and remediable; assumes CTO can orchestrate live test without unacceptable downtime risk; confidence is Low due to sparse evidence on current failover capability and infrastructure readiness.

Enforce multi-factor authentication (MFA) across all 6 critical systems and eliminate password-only access [Quick Win]

Lever: Risk & Resilience | Effort: Low | Impact: High | Confidence: Low | Thesis: Neutral

Assumes MFA is technically feasible on systems currently lacking it (3 of 6 have MFA, 3 do not); assumes rollout effort is primarily user enablement and policy enforcement rather than infrastructure; confidence is Low due to incomplete visibility on actual system compliance and technical constraints.

Establish formal critical vulnerability patching SLA with defined cadence and monthly executive reporting [Quick Win]

Lever: Risk & Resilience | Effort: Low | Impact: Medium | Confidence: Low | Thesis: Neutral

Assumes 2–3 week informal critical patch cycle can be formalized into an SLA without undue operational burden; assumes CTO or external security consultant can define and enforce cadence; confidence is Low due to sparse evidence on actual current patch capability and risk exposure window.

Conduct current penetration test and document remediation roadmap for identified findings

Lever: Risk & Resilience | Effort: Medium | Impact: Medium | Confidence: Low | Thesis: Neutral

Assumes previous pen-test (couple years old) is stale and findings are unknown; assumes current test will surface material risks that should be tracked and remediated; confidence is Low due to absence of artifact trail and inability to assess current exposure from prior findings.

People & Change

Hire or develop dedicated in-house security function; transition from part-time external consultant to lead security ownership

Lever: Risk & Resilience | Effort: High | Impact: High | Confidence: Medium | Thesis: Neutral
Assumes current reliance on part-time consultant is unsustainable at scale and post-acquisition; assumes market for security talent will support hire; assumes 2–3 month recruitment horizon plus 6-month ramp to productivity.

Hire or develop DevOps/SRE capability in-house; establish infrastructure and deployment discipline as core engineering function

Lever: Scalability | Effort: High | Impact: High | Confidence: Medium | Thesis: Primary
Assumes engineering team is thin on DevOps/SRE and infrastructure modernization has been deprioritized due to capacity; assumes dedicated hire or external augmentation is required to unblock CI/CD and IaC implementation; assumes 2–3 month recruitment plus 3–6 month knowledge transfer and delivery.

Build formal skills matrix and structured learning paths for digital capability across operations, analytics, and security

Lever: Scalability | Effort: Medium | Impact: Medium | Confidence: Medium | Thesis: Primary
Assumes Director of RevOps hire and COO's structured onboarding program signal readiness to formalize capability development; assumes business case exists for data and security skills given identified gaps; assumes 3–4 month design and rollout horizon.

Implement structured change management framework and governance process for major digital releases post-100-day

Lever: Multiple & Narrative Readiness | Effort: Medium | Impact: Medium | Confidence: Medium | Thesis: Secondary
Assumes COO has established informal change management (release notes, training, office hours) that can be formalized into a governance process; assumes framework will support investor narrative on disciplined digital delivery and adoption risk mitigation.

Methodology Note

This assessment used the HellerHiveAI Digital Maturity Assessment rubric (8 pillars) under the **Express** engagement tier. Evidence sources: CEO, CFO, COO, CTO, and CMO/CRO interview notes, evidence checklist, DRS data profiling, and integration inventory.

The following pillar(s) were scored twice — once in pass 1 and again after targeted follow-up responses were provided: **Security & Resilience**. Final scores reflect pass-2 evidence.

Scoring: High = 3, Medium = 2, Low = 1. Weighted score = raw score × pillar weight. Overall score = sum of weighted scores (max 3.000).

