

# Platform Audit Report

## Executive Summary

- Platform: An ABA therapy operations platform covering scheduling, onboarding, session management, billing, and admin controls.
- Maturity: Growing Product (strong CI/security posture, but notable gaps and unresolved issues).
- Primary strengths: Documented security processes, CI/CD gates with coverage, tenant isolation focus, and operational runbooks.
- Primary risks: Documented missing org-scoped validations, accessibility gaps, unresolved test failures, and limited production ops/monitoring documentation.
- Overall readiness: Not fully production-ready for a real company without workarounds.
- Recommendation: Go with Conditions.

## Feature Completeness Assessment

Functional Area	What exists today	What is missing	Incomplete/fragile/manual
Core scheduling & sessions	Core session workflows and tests; session hold workflows described	Org assertions missing in key endpoints; some API validations	Documented gaps in schedule APIs and throttling
Client onboarding	Onboarding runbooks and status tracking	Org validation in /initiate-client-onboarding; incomplete automation	Status docs show outstanding items
Admin & roles	Role models, RLS policies, admin controls	Unclear therapist edit permission boundaries	Open questions in audit report
Security & RLS	Security audit completed; RLS hardening and checks	Audit triggers for soft deletes; ongoing verification	Some policies/validations still listed as gaps
Compliance readiness	Security checklist and runbooks	No evidence of formal compliance certification	Missing explicit compliance artifacts
Reliability & testing	CI gates: lint, typecheck, tests, coverage	Documented failing tests status unclear	Failures documented; remediation status unknown
Accessibility & UX	A11y tests exist	Known UI accessibility gaps	Manual fixes listed in reports
Monitoring & incident response	Staging ops runbook, smoke expectations	No clear production monitoring/alerting plan	Incident response plan not documented
Performance & scalability	Performance checks documented	No load testing or benchmarks	Advisor warnings still present
Integrations & APIs	Netlify, Supabase, scripts and docs	Formal integration catalog not documented	Extensibility unclear

## Gaps & Risks

### Known Risks

- Business: Missing org assertions in critical endpoints can disrupt multi-tenant workflows and trust.
- Technical: Known failing tests and missing throttling/validation signal instability under load.
- Security & compliance: Soft-delete audit triggers missing; compliance artifacts not documented.
- Operational: Monitoring/alerting and incident response runbooks are not clearly documented.

### Unknowns (due to missing information)

- Actual production uptime, SLA commitments, and on-call processes.
- Load-test results and scalability limits.
- Formal compliance posture (HIPAA, SOC2, etc.) and audit evidence.
- Integration coverage (EHR, billing systems, SSO) beyond current stack.

### Readiness for Company Use

- Can a real team use this today without workarounds? Likely no—documented gaps in validations and unresolved failures suggest workarounds.
- What would break at scale? Org-scoped validation gaps and lack of throttling could cause cross-tenant risks and performance issues.
- What would frustrate executives or operators? Missing monitoring/alerting, unclear incident response, and unresolved known gaps.
- What would require custom development or manual processes? Compliance readiness, integration cataloging, and some operational workflows.

### Required Improvements Before Adoption

#### Must-have before launch (Small–Medium)

- Fix missing org validations in critical endpoints.
- Resolve documented test failures and close audit open questions.
- Add audit triggers for soft deletes.

#### Strongly recommended (Medium)

- Formal monitoring/alerting and incident response runbook.
- Address known UI accessibility gaps.
- Document and enforce API throttling and rate limits.

## **Nice-to-have (Medium–Large)**

- Load/performance benchmarks and scalability plan.
- Formal compliance documentation or certifications.
- Integration catalog and partner readiness.

## **Final Recommendation to the CEO**

Recommendation: Go with Conditions. The platform is strong in security process and engineering discipline, but it is not yet fully production-ready for a real company. Key validation gaps, unresolved test failures, and missing operational readiness (monitoring and incident response) make immediate adoption risky. With focused remediation, a realistic path to production readiness is 4–8 weeks, depending on how quickly the must-have items are completed and verified.