CHANGE PLAN FOR MANAGEMENT | NO REBUILD, EXTEND WHAT EXISTS

Client Portal, Invitation & Marketing Chat

What the CRM already does, what has to be added, and exactly which parts of the system change. Nothing existing is removed or rewritten.

The goal in one line

> After Marketing schedules an audit, they press **Invite Client**. The client activates a portal login, sees only their own company data, and can chat in real time with **the Marketing Executive who invited them**. Every step is written to the database as an activity, chat, email and invitation log.

What we already have, and what we still need

Area	Already in the CRM	What we add
Audit Request	Create, submit, schedule, assign auditor	An **Invite Client** button that appears only after the audit is scheduled
Client Portal	Portal + mobile app exist: audits, findings, certificates, reports, checklists	Invitation-based account creation tied to the audit request
Authentication	JWT + roles; client email-code login already works	CLIENT role permissions tightened; invitation token flow
Real-time	Socket gateway for internal notifications and chat	Client ↔ Marketing conversation rooms on the same gateway
Chat	Internal / SuperAdmin chat with messages stored in the DB	Extend the same tables with a client conversation type
Email	Invitation and OTP emails are sent	An **email log** table so every send is traceable
Logging	Partial logging in places	One central **activity log** used by client, marketing and chat events
Reporting	Audit and certificate reporting	Client timeline, chat log, email log and activity screens in the CRM

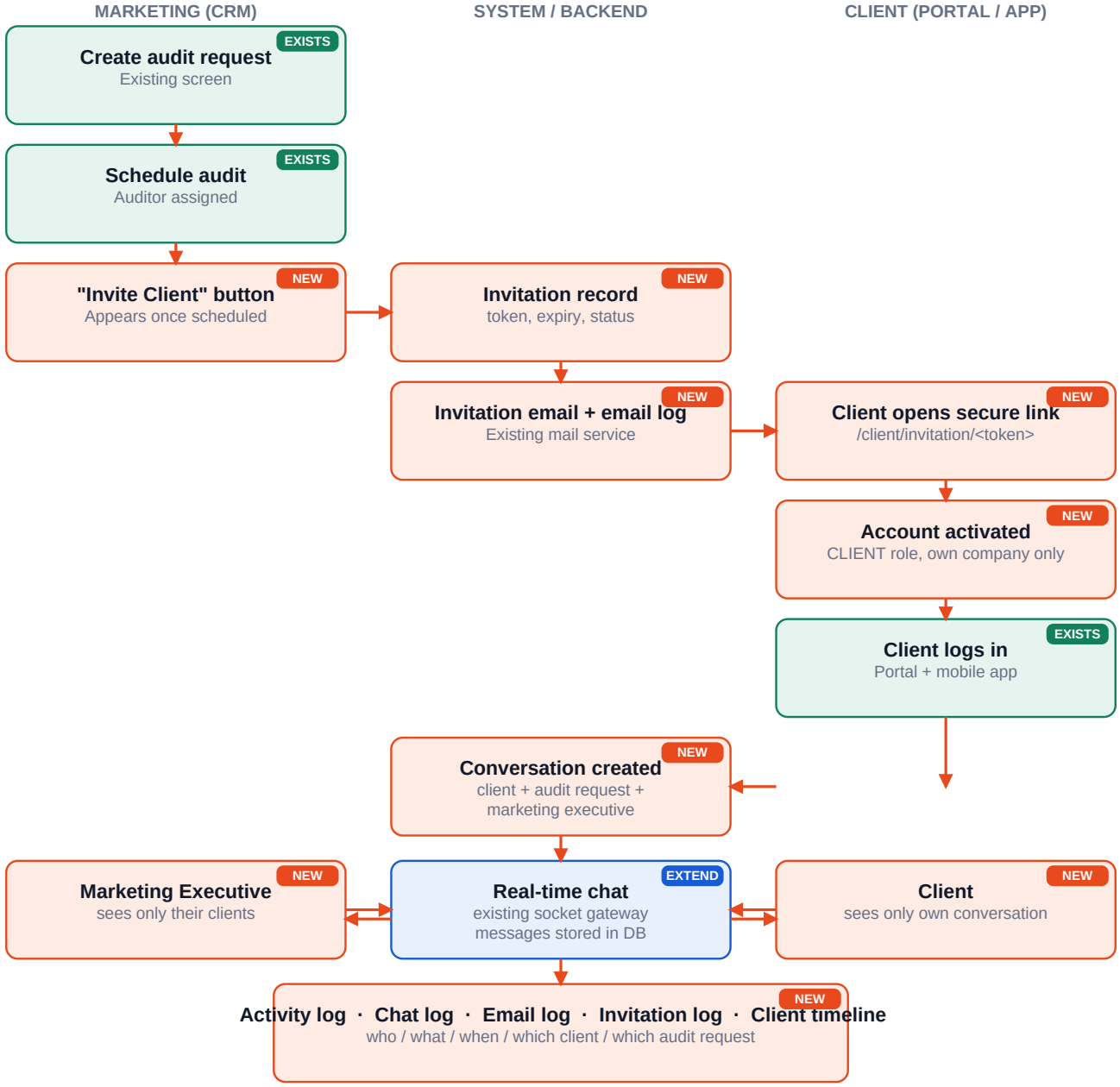
Effort at a glance

Work package	Where	Size
Invitation (entity, API, email, token, statuses)	Backend + CRM web	Medium
Client ↔ Marketing chat on the existing gateway	Backend + CRM web + portal + mobile	Medium / Large
Central activity, chat, email logging + timeline	Backend + CRM web	Medium
CLIENT role permissions and menu visibility	Backend + portal + mobile	Small
Client log screens (tabs, filters, export)	CRM web	Medium

Sizes are indicative. They assume the existing chat gateway, email service and role system are reused rather than rebuilt.

1. The complete flow

Green = already works today. Orange = new in this change.



2. Exactly what changes, module by module

File and module names follow the existing project. The development team confirms the exact paths during step 1 (inspection) before writing code.

Backend (NestJS)

Module	Change	Type
audit-request	Endpoints: invite client, read invitation, resend invitation. Invite allowed only when the audit is scheduled.	**Modify**
client-invitation *(new)*	Entity, service, controller: token, expiry, status (PENDING / SENT / ACCEPTED / EXPIRED / CANCELLED), accept endpoint, duplicate-account guard.	**New**
chat / conversations	Add a client conversation type linked to client + audit request + marketing user. Reuse the existing message table and gateway.	**Extend**
socket gateway	Client joins only its own conversation room. Marketing joins their own. Auditors are excluded.	**Extend**
client-portal	Conversation + message endpoints for the client, scoped to one company (already fixed).	**Modify**
notifications	New events: invitation accepted, new client message, document uploaded.	**Extend**
mail service	Invitation + resend templates, and every send written to the email log.	**Extend**
activity-log *(new or existing)*	One service used everywhere: user, client, audit request, action, description, metadata, IP, device, timestamp.	**New**
auth / RBAC	CLIENT role permissions; ownership checks on every client endpoint (company, audit request, conversation).	**Modify**

Database (TypeORM migrations — nothing dropped)

Table	Purpose	Action
client_invitations	audit_request_id, company_id, email, token, status, expires_at, accepted_at, invited_by, client_user_id	**Create**
conversations	Add type (INTERNAL / CLIENT), client/company id, audit_request_id, marketing_user_id	**Add columns**
messages	Reuse as is; add read_at / sender_role only if missing	**Reuse**
activity_logs	Central log for client + marketing + chat events	**Create**
email_logs	type, to, subject, client, audit request, sent_by, status, provider id, error	**Create**

CRM web (Next.js)

- **Audit request screen:** Invite Client button + invitation modal (company, contact, email, phone, audit reference, scheduled date, marketing executive, auditor) prefilled from existing data.
- **Invitation status:** the button becomes Invitation Sent / Accepted / Portal Active, with Resend.
- **Client log screen:** tabs for Overview, Audit Requests, Invitations, Chat, Activity, Emails, Documents, with filters and a date range.
- **Marketing inbox:** conversations with that executive's own clients, on the existing chat UI.

Client portal & mobile app

- **Messages screen** in the portal and the app, using the same backend conversation and the same socket events — no separate mobile chat data.
- **Unread badge** and push/live notification for new marketing messages.
- **Menu visibility** driven by the CLIENT role (next page).

3. Client role — what the client may see

Permissions are enforced in the **backend**. Hiding a menu item is only the second layer; every client API also checks company, audit request and conversation ownership.

Feature / menu	Client	Marketing Exec	Auditor	SuperAdmin
Own company profile, sites, team	Yes	Yes	Assigned	Yes
Own audit requests & schedule	Yes	Yes	Assigned	Yes
Audit report (once uploaded)	Yes	Yes	Yes	Yes
Findings / NC — respond & evidence	Yes	Yes	Yes	Yes
Audit checklist — upload documents	Yes	Yes	Yes	Yes
Digital certificates	Yes	Yes	Assigned	Yes
Chat with own marketing executive	Yes	Yes	No	Yes
Other companies' data	No	Own accounts	Assigned	Yes
Internal / SuperAdmin chat	No	Own	Own	Yes
Internal audit notes, auditor worksheets	No	Limited	Yes	Yes
Pricing, proposals, invoices (internal view)	No	Yes	No	Yes
CRM menus: leads, users, roles, settings	No	Limited	No	Yes
Activity / email / chat logs	No	Own clients	No	Yes

How menus are hidden

- The login response already returns the user's role and company. The portal and the app build the menu from that, so a client never renders internal CRM items.
- Client-side menus are hidden **and** the matching endpoints reject the request with 403/404 — hiding alone is not security.
- Anything not explicitly allowed for CLIENT is denied by default.

> **Already fixed in the backend:** every client portal endpoint is now scoped to a single company, so a client linked to more than one company can no longer see another company's NCs, audits or certificates. Notifications are likewise limited to the client's own user id.

4. What gets logged (the audit trail)

Log	Events recorded
Client activity	Invitation accepted · account activated · login · logout · viewed audit request · viewed schedule · opened chat · sent message · uploaded document · downloaded report · profile change
Marketing activity	Created audit request · scheduled audit · invited client · resent invitation · viewed client · sent message · downloaded client document · updated audit request
Chat log	Conversation id, client, marketing executive, audit request, every message with sender, role, time, read status, attachments
Email log	Invitation, resend, activation, password reset, important notifications — recipient, subject, client, audit request, sent by, status, provider id, error
Invitation log	Created · sent · opened · accepted · expired · cancelled, with who and when

All of this feeds one **client timeline**: “10:30 invitation sent · 10:45 accepted · 10:50 first login · 10:56 first message · 11:10 document uploaded”, giving a complete record of who did what, when, for which client and which audit request.

5. Suggested delivery order

Phase	Delivers	Why first
0 · Inspection	Map of existing audit request, chat, gateway, mail, roles and logs; file list for every change	No code is written until the reuse points are confirmed
1 · Invitation	Invite Client button, invitation record, email + email log, accept and activate	Marketing sees value immediately
2 · Permissions	CLIENT role, ownership checks, menu visibility in portal and app	Security before more data is exposed
3 · Chat	Client ↔ marketing conversation on the existing gateway, in portal, CRM and mobile	Builds on phases 1 and 2
4 · Logs & timeline	Central activity logging, chat/email/invitation logs, CRM log screens and filters	Complete audit trail once the events exist

6. How we will know it works

- Marketing schedules an audit and the **Invite Client** button appears — not before.
- The client receives the email, activates the account and sees **only their own** company, audits, findings and certificates.
- Client and marketing exchange messages in real time; after a browser refresh the full history is still there, because it is in the database.
- A client trying to open another client's conversation gets 403/404.
- Every one of those steps appears in the client timeline, the chat log and the email log.

> **Nothing existing is rebuilt.** The audit request module, the internal chat, the email service, authentication and the mobile app all keep working as they do today. This plan only adds the invitation, the client conversation, and the logging around them.