



FUNCTIONAL BROCHURE

A digital infrastructure supporting the OSA methodology

Qualification · Opportunities · Due Diligence · Confidentiality · Monitoring



ILLUSTRATED FUNCTIONAL MOCKUP

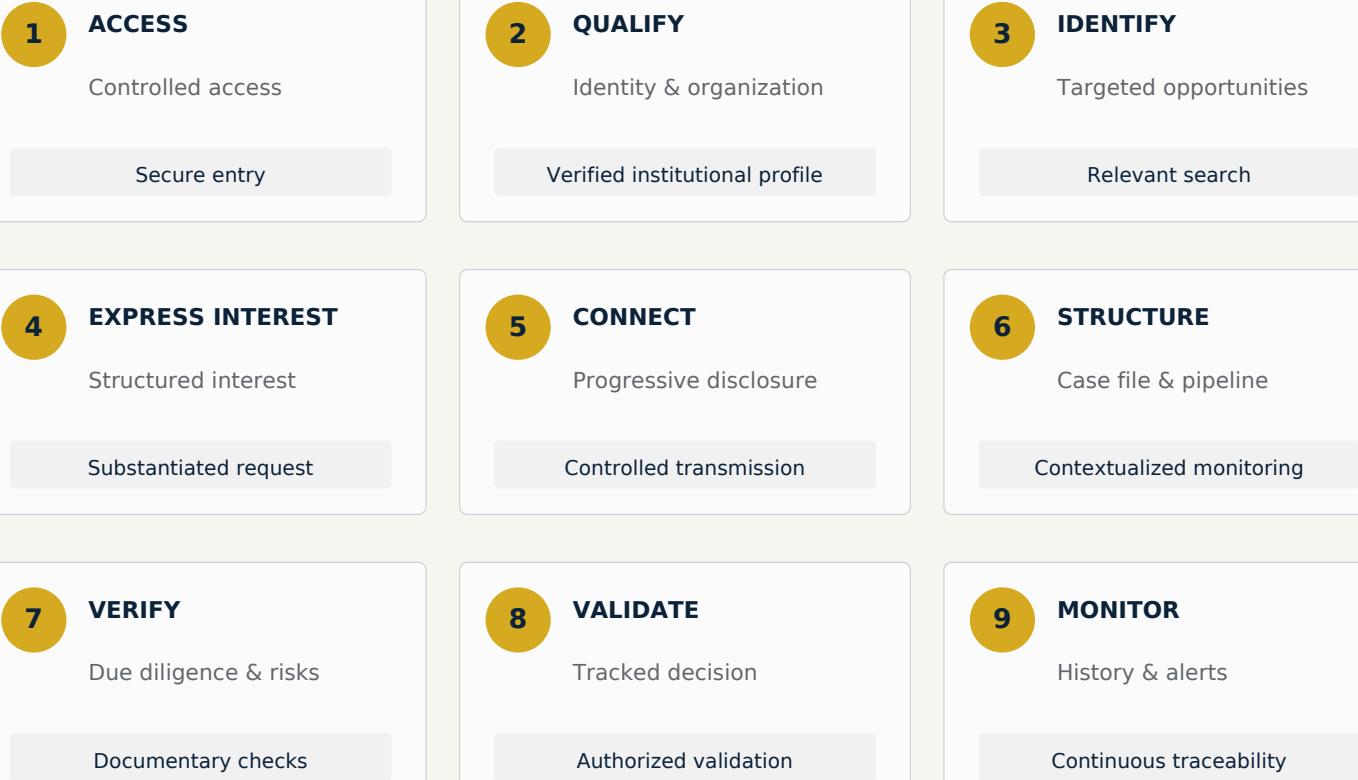
Demonstration interfaces and data · Features currently under design and development

Institutional project in preparation · Planned establishment: Riyadh, Saudi Arabia · August 2026

01 · OVERVIEW

A structured journey from qualification to ongoing monitoring

The OSA platform organizes the main stages of a qualified business relationship within a single digital environment, while keeping decision-making and oversight in the hands of authorized persons.



Three dimensions. Technology + institutional oversight + human support.
The platform facilitates the OSA methodology without replacing required approvals.

A controlled-access environment

Access to the platform is based on a professional identity, an organizational affiliation and appropriate authentication mechanisms.



A qualified professional environment.

OSA brings together companies, investors and institutions within a structured business environment. Each member is identified, verified and qualified before accessing opportunities.

- ◆ B2B institutional qualification
- ◆ Structured document due diligence
- ◆ Supervised introductions
- ◆ Permanent non-custodial scope

Connecting ambitions. Building lasting trust.

Sign in

Access request

Invitation code

Qualified member access

Sign in with your registered professional email address.

PROFESSIONAL EMAIL ADDRESS

a.traore@saheltrading.ne

PASSWORD

.....

☒ Remember this device

[Forgot password?](#)

Sign in >

Next step: two-factor authentication

Creating an account or receiving an invitation does not, by itself, constitute OSA qualification.

Professional identity

Access is linked to a professional email address and an identified organization.

Request or invitation

Access may follow an approved request or the use of a controlled invitation code.

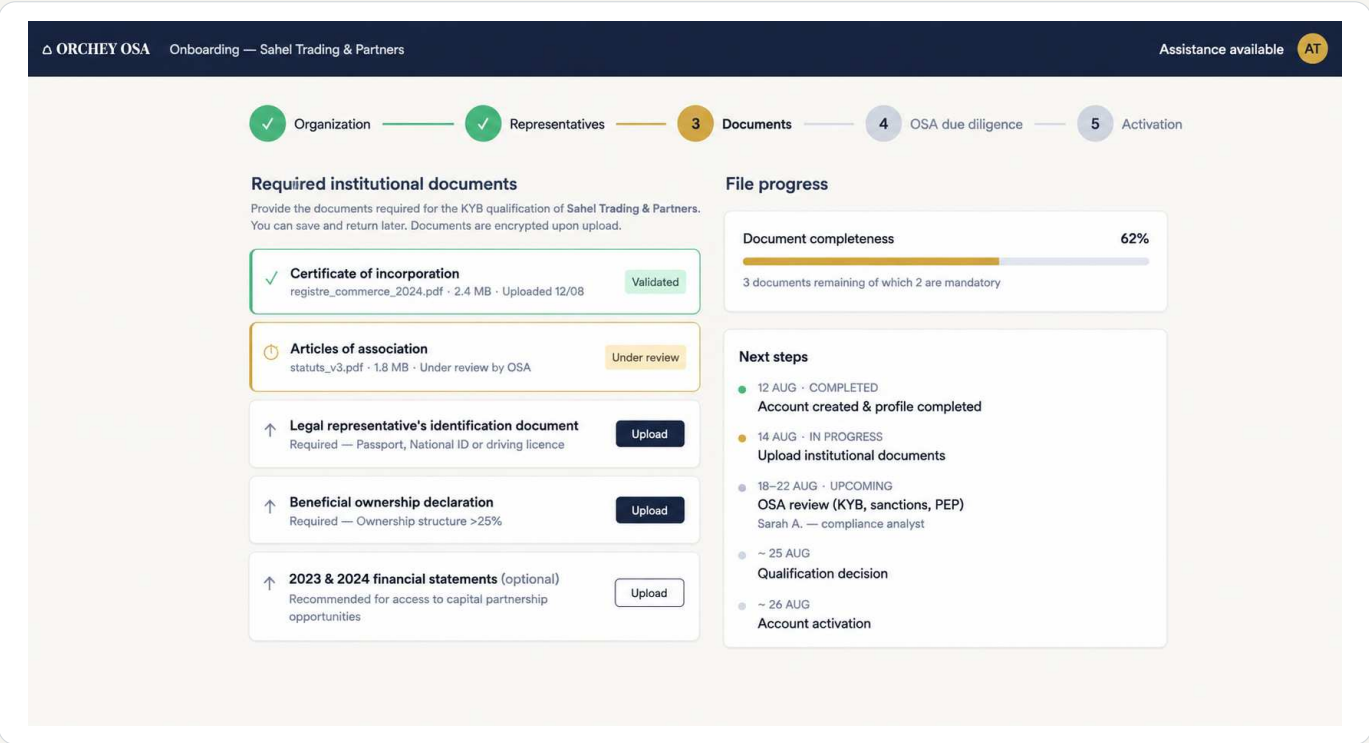
Enhanced authentication

Two-factor authentication may complement the password before a session is opened.

03 · ONBOARDING & QUALIFICATION

Build an actionable institutional file

The onboarding journey progressively gathers the information needed to understand the organization, its representatives and its ownership structure.



Qualification, due diligence and activation remain separate stages: document completeness does not create an automatic right of access.

Required documents

Institutional documents are uploaded, versioned and tracked according to their status.

Visible progress

The organization can see which items have been received, are under review or remain outstanding.

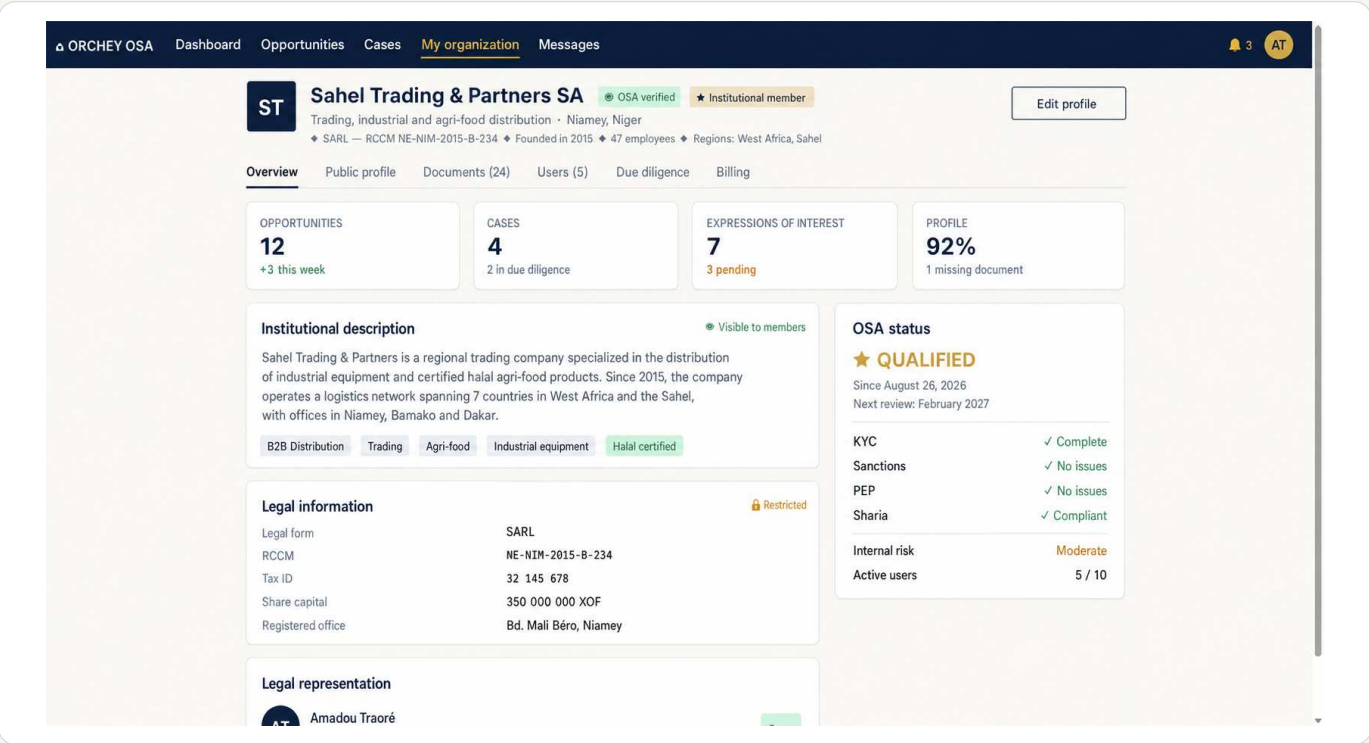
OSA review

Document completeness informs the review but does not prejudice the final decision.

04 · ORGANIZATION & PROFILE

An institutional profile linked to authorized users

Each member has an organizational space bringing together its profile, legal information, users, documents and relevant statuses.



Interface labels relating to Sharia, risks and controls remain subject to harmonization and institutional validation.

Institutional profile

Overview, sector, location and legal information are organized in a single space.

Users & roles

Internal access rights may be assigned according to responsibilities within the organization.

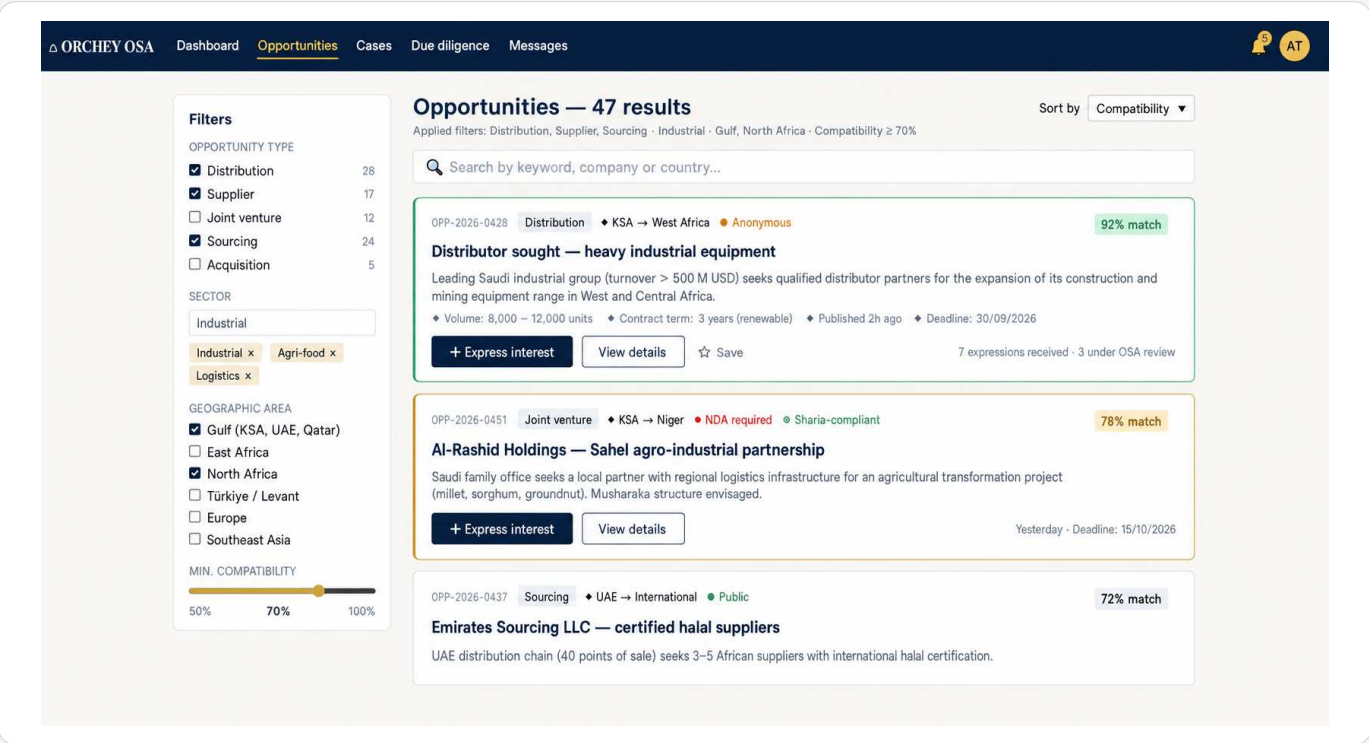
Readable statuses

Qualification, due diligence, documents and risk levels are presented in a concise format.

05 · OPPORTUNITIES

Identify the most relevant opportunities

Search combines business criteria, geography, sector and compatibility level to reduce noise and focus attention on the most relevant opportunities.



Scores and indicators support analysis. Their interpretation remains subject to human review and applicable controls.

Targeted search

Filters, sectors and geographic areas structure the discovery of opportunities.

Indicative compatibility

The score helps prioritize analysis; it is neither a recommendation nor a decision.

Graduated visibility

Some information may remain anonymized or restricted according to the level of access.

06 · PROGRESSIVE DISCLOSURE

Protect information before disclosing the parties

Identities and sensitive information may be disclosed in stages, following an expression of interest, OSA review and, where required, formalization of confidentiality arrangements.

ORCHEY OSA

Dashboard

Opportunities

Cases

Due diligence

Messages

5

AT

Opportunities > Distribution > OPP-2026-0428 — KSA industrial equipment distributor

OPP-2026-0428

Distribution B2B

Anonymous — identity disclosed after OSA validation

+ 92% match with your profile

Distributor sought — heavy industrial equipment

KSA — West and Central Africa

Published: 14 August 2026

Deadline: 30 September 2026

7 expressions received

3-year framework agreement

Description

A leading Saudi industrial group (revenue exceeding 500 M USD), present in 12 countries, seeks qualified distribution partners to support the expansion of its range of construction equipment, engines, site and material handling equipment in West and Central Africa.

The ideal partner should have an established logistics network covering at least 3 countries in the ECOWAS region, warehousing capacity suited to heavy equipment, and proven experience in the commercialization of industrial or mining equipment to public and private clients.

Selection criteria

Minimum 5 years' experience

B2B distribution in West Africa

Geographic coverage

Minimum 3 ECOWAS countries

Logistics capacity

Preferred certifications

Progressive disclosure

Information is disclosed in controlled stages by OSA and the opportunity sponsor.

1 STEP 1 · COMPLETED

Public description

2 STEP 2 · IN PROGRESS

Expression of interest

3 STEP 3

OSA review (48 business hours)

4 STEP 4

Mutual NDA signature

5 STEP 5

Identity disclosure

6 STEP 6

Data Room opening

Compatibility analysis

92%

Sector

Geography

Experience

Logistics capacity

✓ Match

✓ Match

✓ Strong

To be validated

Progressive disclosure seeks to balance the usefulness of information, confidentiality and control over introductions.

Initial anonymization

A useful description may be visible without immediately revealing the counterparty's identity.

Pre-transmission review

OSA may review the interest and admissibility conditions before any transmission.

NDA & disclosure

Named disclosure and access to a document space occur according to the applicable authorizations.

ORCHEY STRATEGIC ADVISORY · FUNCTIONAL BROCHURE

07 / 19

07 · EXPRESSION OF INTEREST

Move from interest to a structured request

An expression of interest requires the member to explain its motivation, experience, capabilities and the elements used to assess alignment with the stated criteria.

EXPRESSION OF INTEREST

OPP-2026-0428 — Industrial equipment distribution

Auto-save

1 Your profile

2 Motivation & capacity

3 References

4 Documents

5 Confirmation

Motivation & fit with the criteria

Explain concretely how Sahel Trading & Partners meets the stated criteria. OSA reviews this section before any submission to the counterparty.

STRATEGIC RATIONALE *

Since 2015, our company has operated a logistics network covering 7 ECOWAS countries. Distributing heavy industrial equipment for a leading Saudi partner is a natural extension of our current activities (construction, mining and agriculture) and complements our existing offering to our 340 active B2B clients.

368 / 1000 characters

RELEVANT EXPERIENCE *

Authorized Sany distributor since 2019 (construction equipment, 800 units/year). Exclusive partnership with Bell Equipment Sud for French-speaking Africa. Network of 4 logistics depots (Niamey, Bamako, Ouagadougou and Cotonou) totaling 8,500 m² of heavy-equipment storage.

PROJECTED OPERATING CAPACITY

Annual capacity: 5 000 – 8 000 units

Start-up time: 3 months — Niamey warehouse available

AREAS YOU PROPOSE TO COVER

Niger x Mali x Burkina Faso x Benin x + Add a country

+ OSA guidance.

A well-argued expression of interest significantly increases your chances of being presented to the counterparty. Be specific and factual.

After submission

- OSA reviews your profile and rationale (48 business hours).
- If approved, the expression of interest is submitted to the counterparty.
- If the counterparty accepts, a mutual NDA will be presented to you.
- An OSA-CASE business file is opened with an OSA case manager.

Confidentiality.

Your information is encrypted, visible only to OSA and, after validation, solely to the authorized counterparty.

An expression of interest does not guarantee transmission, acceptance, an introduction or completion of a transaction.

Substantiated rationale
The member sets out the operational and strategic reasons for its interest.

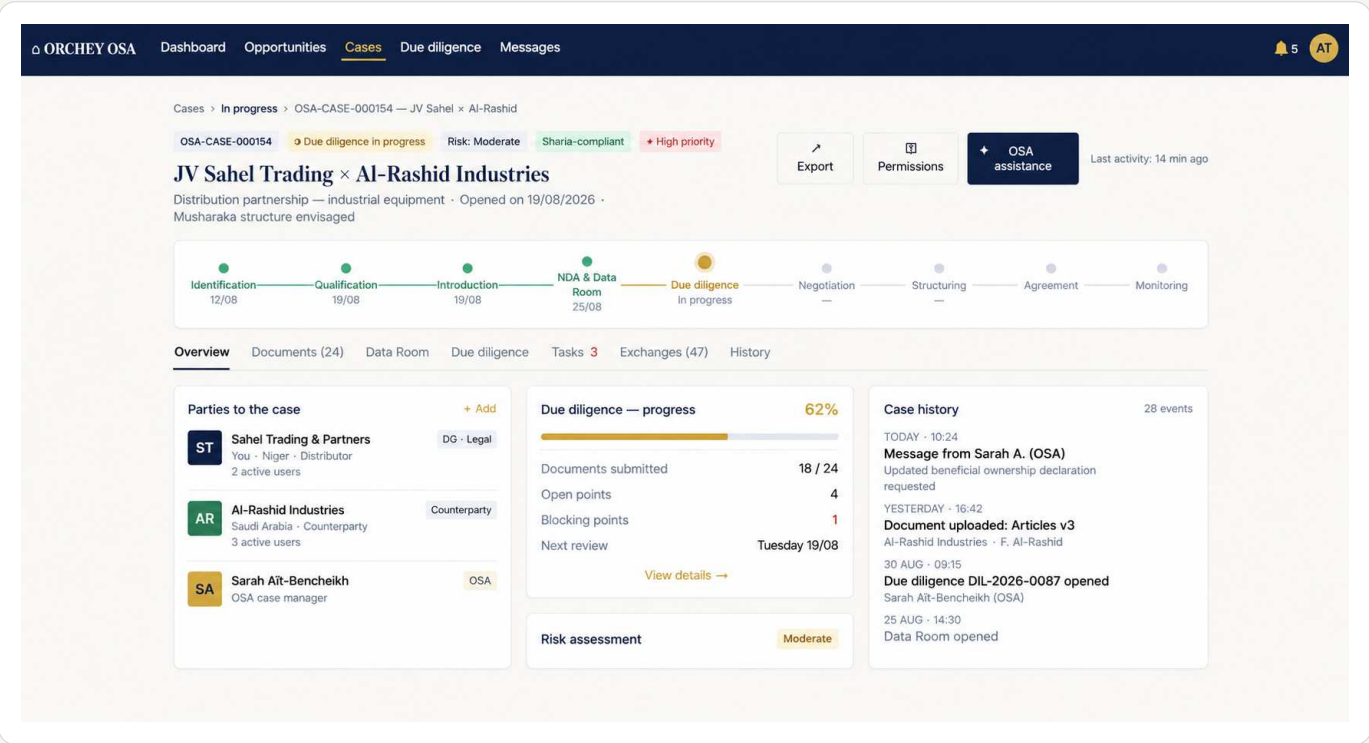
Demonstrable capacity
Volumes, timelines, location and resources are structured to facilitate review.

References & supporting documents
Additional references and documents may be requested before transmission.

08 · CASE FILE & PIPELINE

From introduction to a structured case file

As a relationship progresses, a dedicated case file presents the parties, stages, due diligence, tasks, exchanges and process history.



The digital case file structures monitoring; by itself, it does not execute the legal, financial or commercial transaction between the parties.

Shared pipeline

The main stages appear in a clear, shared chronology.

Parties & responsibilities

Organizations and authorized representatives are linked to the case file.

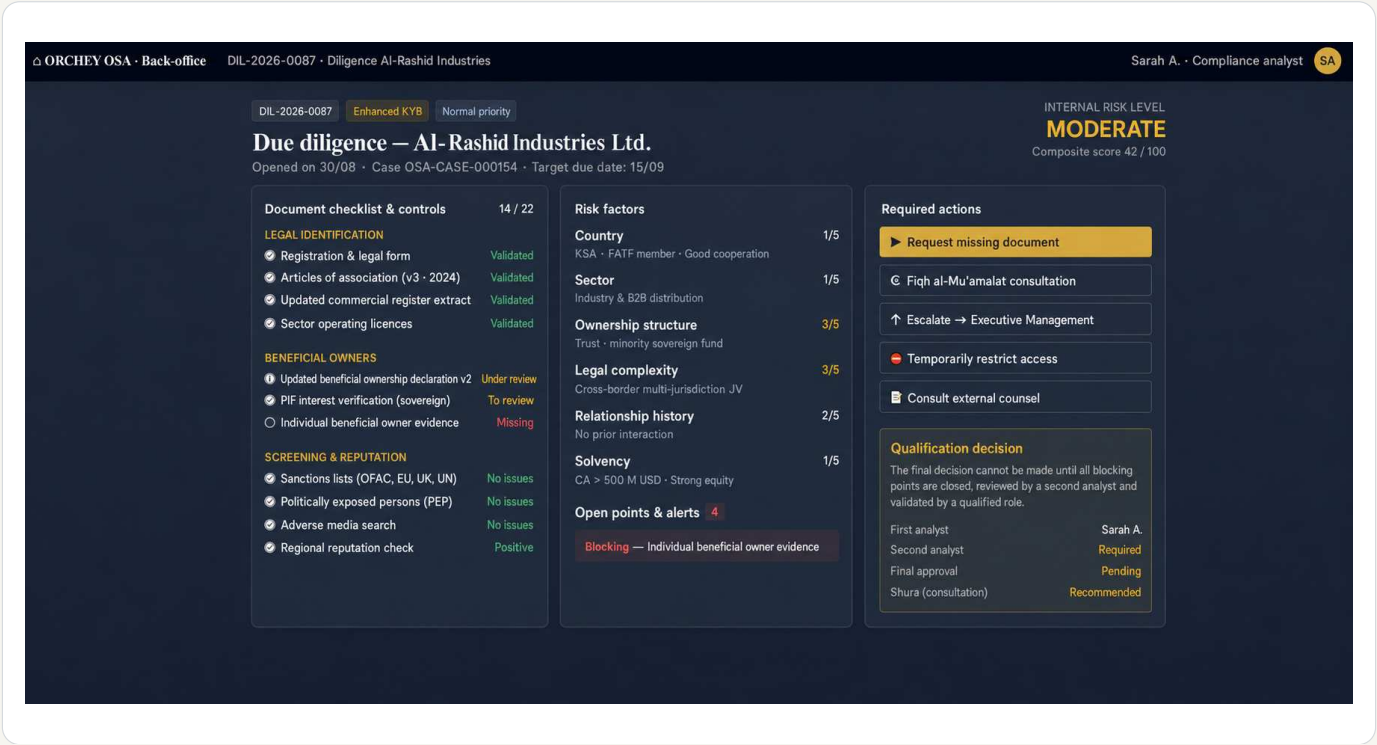
Consolidated history

Uploads, messages, due diligence and significant changes remain accessible in context.

09 · DUE DILIGENCE & RISKS

Structure checks before moving forward

Documentary checks, risk factors, open points and review requirements are brought together in one view to guide authorized analysts.



Risk indicators are decision-support tools. Questions of Fiqh al-Mu'amalat, law or regulation remain subject to competent advice when required.

Document checklist
Documents are classified by area and their review status is tracked.

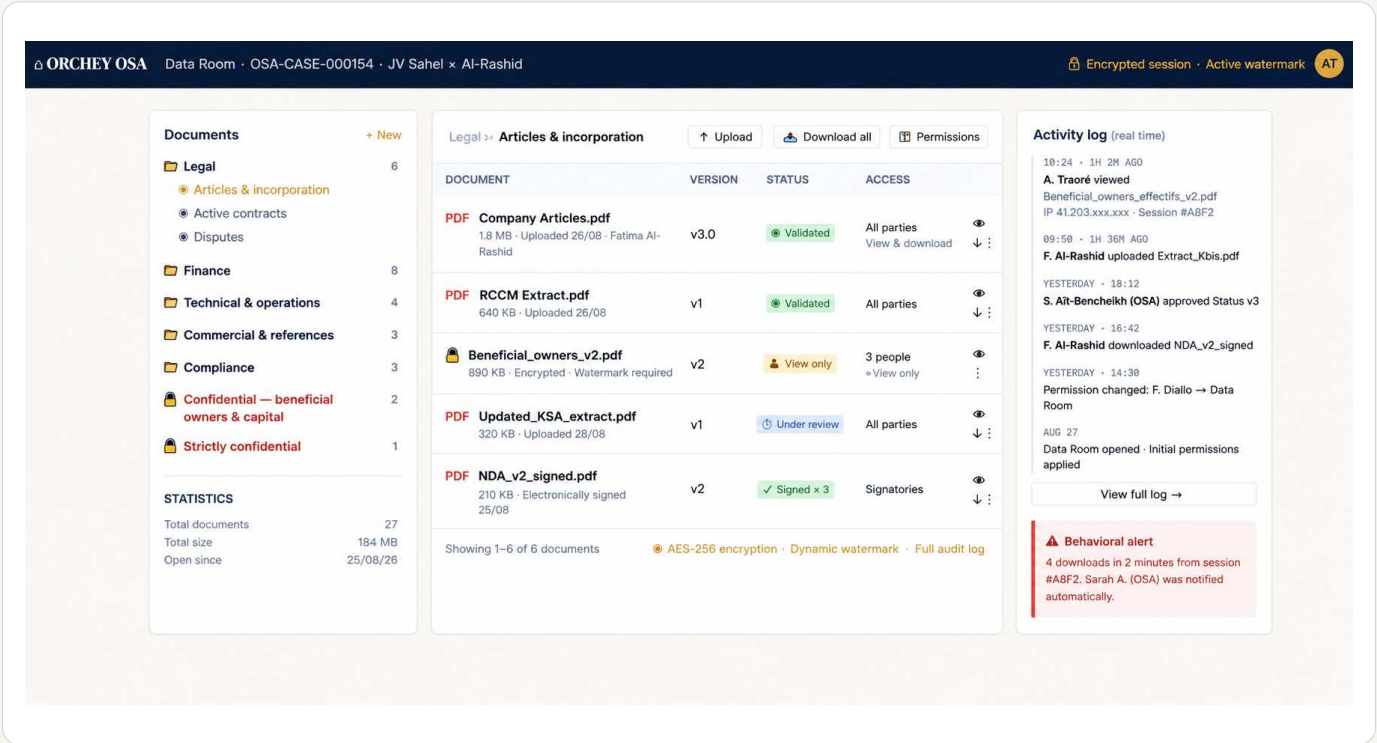
Risk factors
Country, sector, ownership, complexity and other factors may be analyzed and documented.

Blocks & second review
Blocking points, escalations and needs for specialist advice are identified before a decision.

10 • DATA ROOM

Share documents within a controlled environment

The Data Room organizes case documents by category, version and access level, while providing visibility into consultations and significant events.



Encryption, watermarking and usage-control mechanisms must match the capabilities actually deployed in the technical architecture.

Documents & versions

Documents may be classified, versioned and tracked according to their status.

Document permissions

Viewing, downloading and other actions depend on the rights applicable to each document.

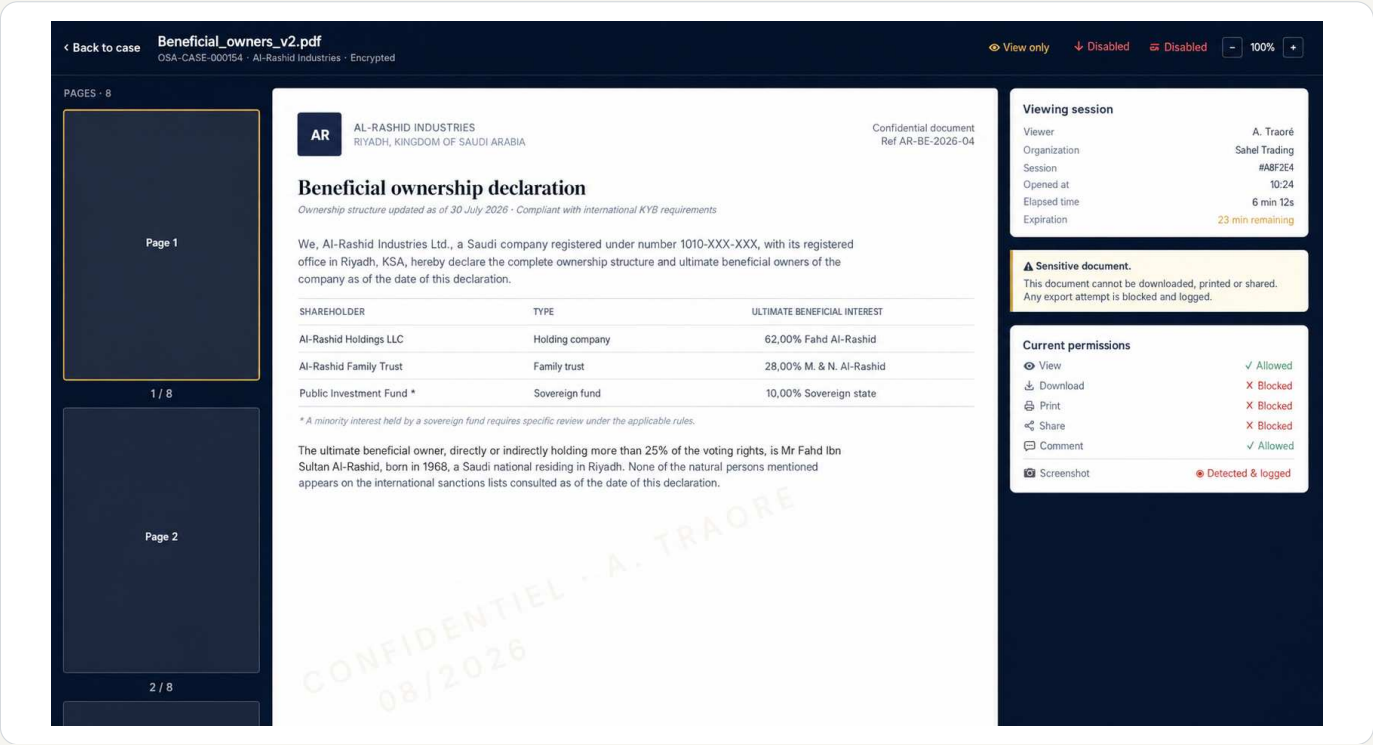
Activity log

Access and significant actions may be recorded to support monitoring and investigation.

11 · CONTROLLED VIEWING

Limit the use of the most sensitive documents

For certain documents, the platform may provide controlled viewing through session limits, restricted permissions, watermarking and export controls appropriate to the confidentiality level.



Protections such as screenshot detection must only be presented as available when they are genuinely supported by the technical environment.

Limited session

Access may be time-limited and linked to an identified session.

Restricted actions

Downloading, printing or sharing may be blocked when the confidentiality level requires it.

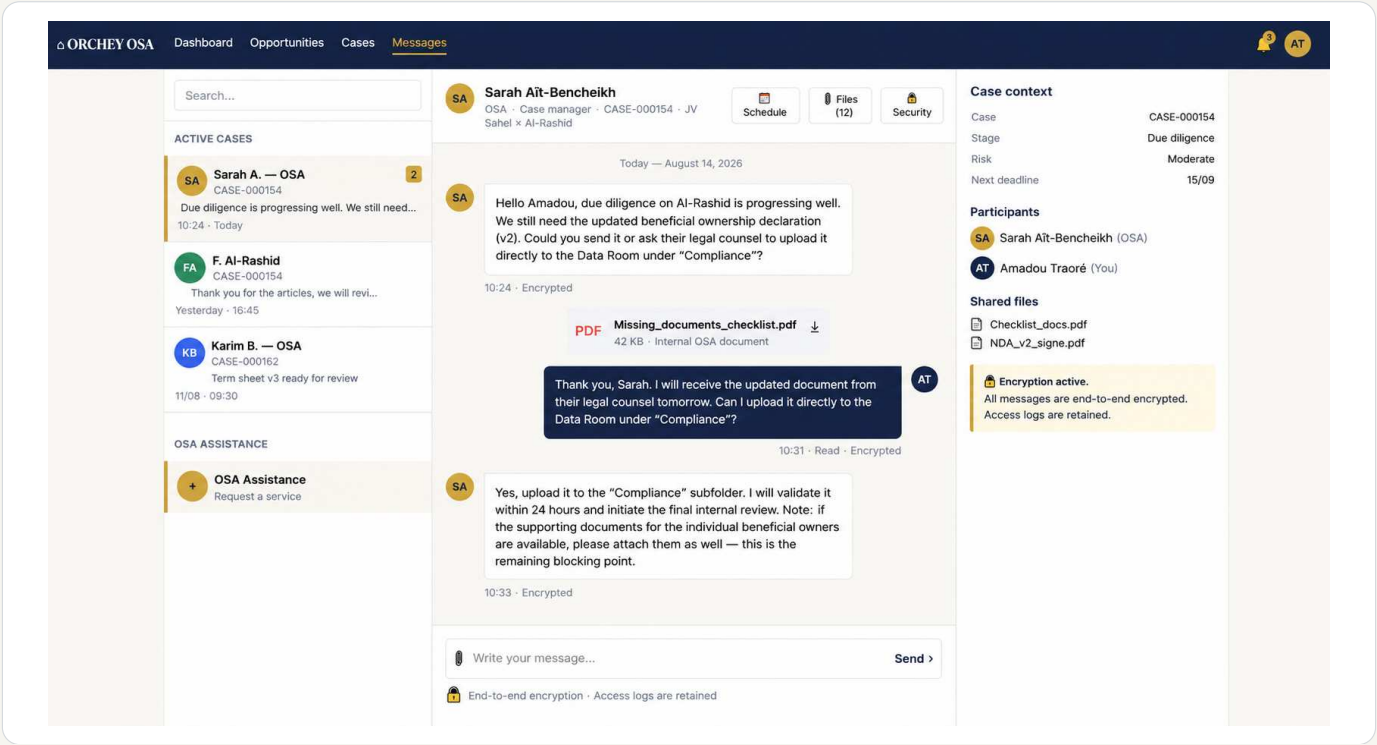
Enhanced traceability

Consultations and attempted actions may feed the case activity log.

12 · CONTEXTUALIZED EXCHANGES

Communicate within the case context

Messaging links exchanges to case files, participants and relevant documents, reducing fragmentation of working information.



The platform seeks to reduce fragmented exchanges without replacing applicable confidentiality, retention and authorization rules.

Preserved context

Each thread may be linked to a case file, a stage and identified participants.

Associated files

Exchanged documents remain connected to the case context and its access rules.

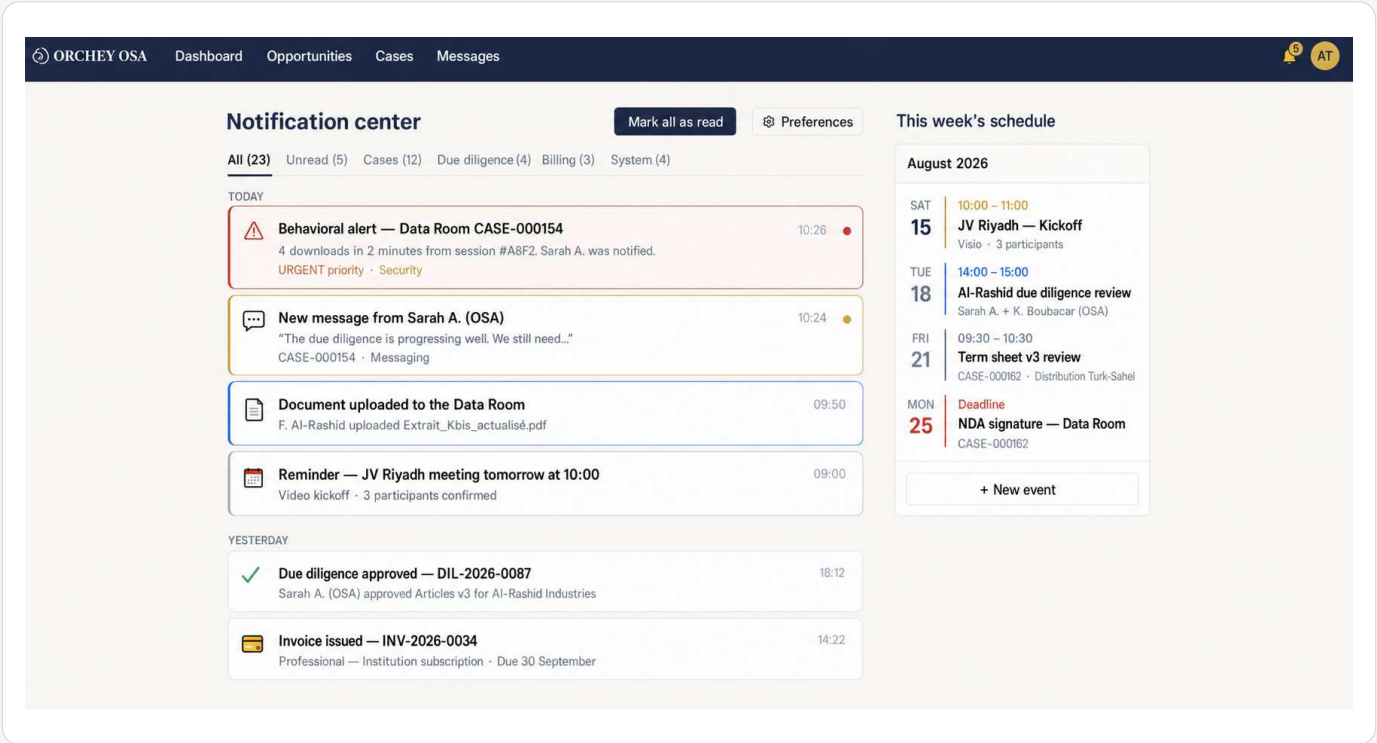
Appropriate security

Messages may be encrypted and logged according to the security architecture actually implemented.

13 · NOTIFICATIONS & DEADLINES

Turn events into priority actions

The notification center brings together alerts, messages, document uploads, deadlines and meetings to help each user address matters requiring attention.



Displayed priority helps organize work; it does not replace the assessment of the authorized user.

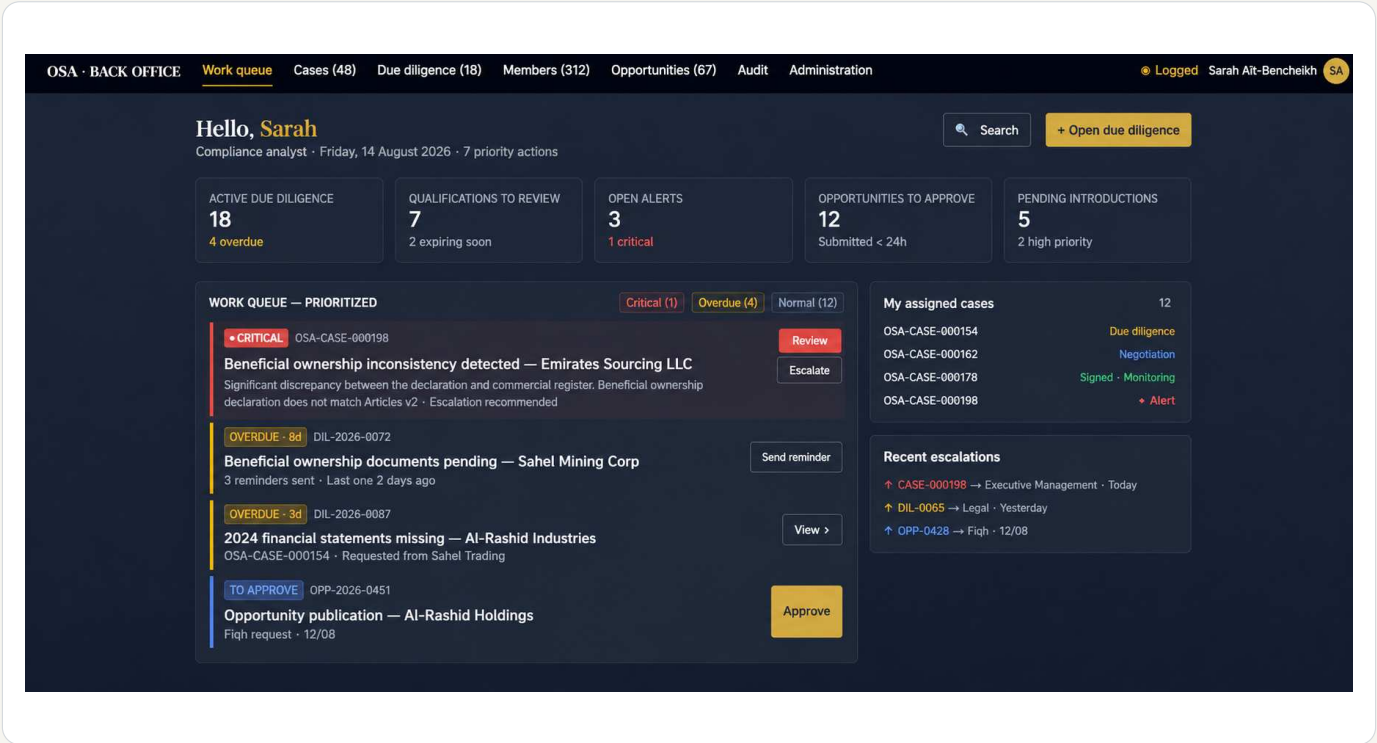
Priority alerts
Sensitive events may be distinguished from ordinary notifications.

Visible deadlines
Reviews, signatures, meetings and due dates are linked to the relevant case file.

Operational agenda
Weekly actions may be presented in a contextualized calendar.

A work queue guided by risk and urgency

The back office turns platform information into concrete action queues for analysts, case managers and authorized internal functions.



The back office organizes internal work; the competent authority retains responsibility for decisions under the applicable governance framework.

Prioritized queue

Critical, overdue, standard or pending review: case files are ordered according to operational needs.

Assigned case files

Each analyst can retrieve assigned cases, due diligence items and alerts in a concise view.

Tracked escalations

Sensitive situations may be routed to the competent function with a trace of the escalation path.

15 · PERMISSIONS & CONFIDENTIALITY

Define who can do what, on which resource, and until when?

Permissions combine role, resource, context and time limits to restrict access to what is strictly necessary and make sensitive operations controllable.

ORCHEY OSAAdministrationPermissionsAudit

AT

Granular permissions matrix

Each access right is defined across four dimensions: WHO (user/role), WHAT (resource), WHY (context), and UNTIL WHEN (time limit). Server-side enforcement, deny-by-default principle.

LEVEL 1
Authorized members
Trade name, sector, country, overview, public products

LEVEL 2
Restricted
Verified members, specific sector, geographic area, subscription

LEVEL 3
Confidential
Expressly authorized parties, masked identity, prior NDA

LEVEL 4
Strictly confidential
Specific authorization, enhanced NDA, watermark, view only

LEVEL 5
OSA internal
Internal notes, risk analyses, qualification grounds, internal exchanges

Roles & permissions matrix						
ACTION	COMPANY USER	COMPANY ADMIN	OSA CASE MANAGER	COMPLIANCE ANALYST	OSA ADMIN	LIMITED & LOGGED SUPER ADMIN
View own profile	✓	✓	By case	As needed	✓	✓
Edit company profile	Limited	✓	Limited	X	✓	✓
View KYC/KYB documents	X	Limited	By case	✓	✓	✓
View internal OSA notes	X	X	By permission	By permission	✓	✓
Publish an opportunity	By permission	✓	✓	X	✓	✓
Approve an opportunity	X	X	By permission	X	✓	✓
Qualify a member	X	X	X	✓ Propose	✓ Approve	✓
Change global permissions	X	X	X	X	Limited	Dual approval
Create/activate Data Room	X	By service	✓	By permission	✓	✓
Revoke access	X	Own users	Own cases	By permission	✓	✓

Server-side enforcement. All permissions are applied server-side (NestJS guards). Hiding a button in the interface is never a security measure — endpoints remain protected.

Confidentiality levels and permissions are enforced server-side; hiding a button in the interface is not, by itself, an adequate security measure.

Granular access
Rights are attached to roles, case files, resources and conditions of use.

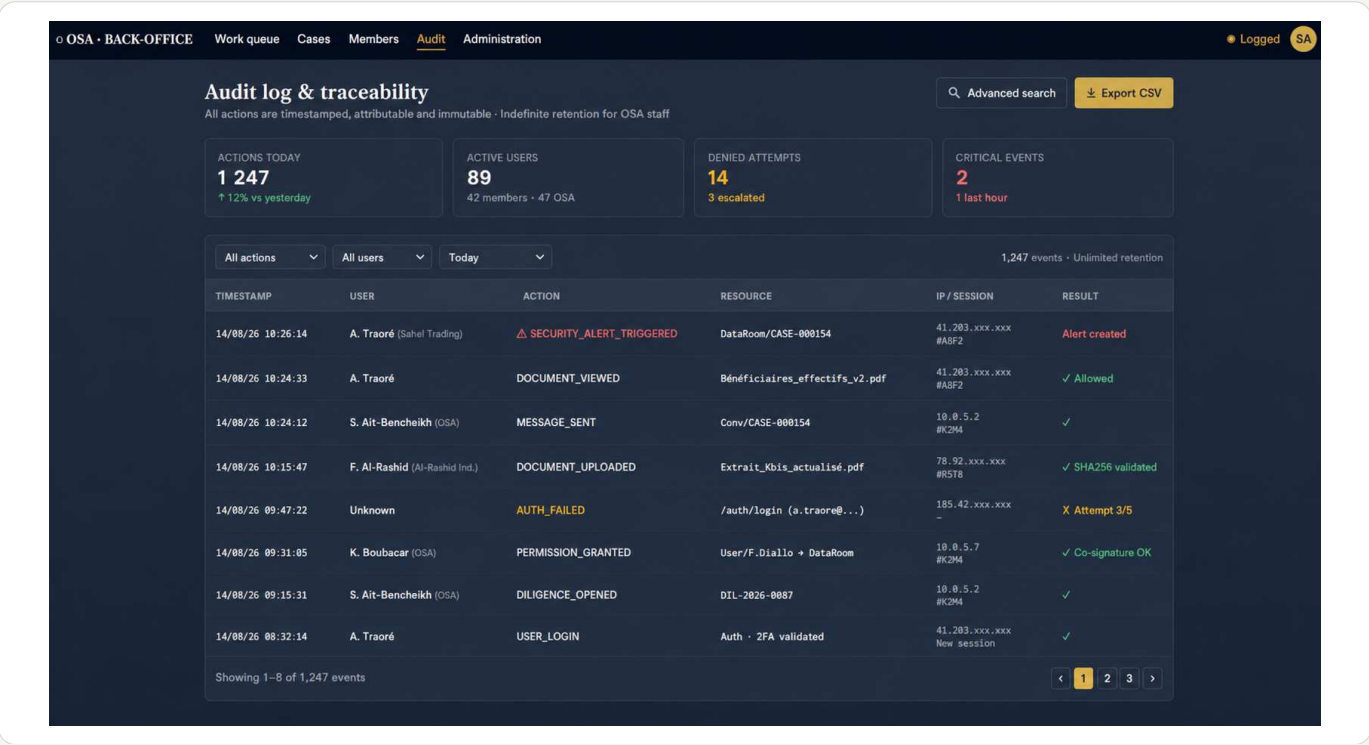
Default denial
The absence of explicit authorization results in denial rather than implicit access.

Enhanced validation
Certain sensitive operations may require dual validation and specific traceability.

16 · AUDIT & TRACEABILITY

Know who did what, when and on which resource

The audit log reconstructs significant actions: user, timestamp, resource, session, outcome and any security alert.



Log-retention periods and immutability levels must be defined through an appropriate retention policy and technical architecture.

Timestamp

Each significant event may be linked to a precise date and time.

Identity & session

The user, session and technical context may be retained according to applicable rules.

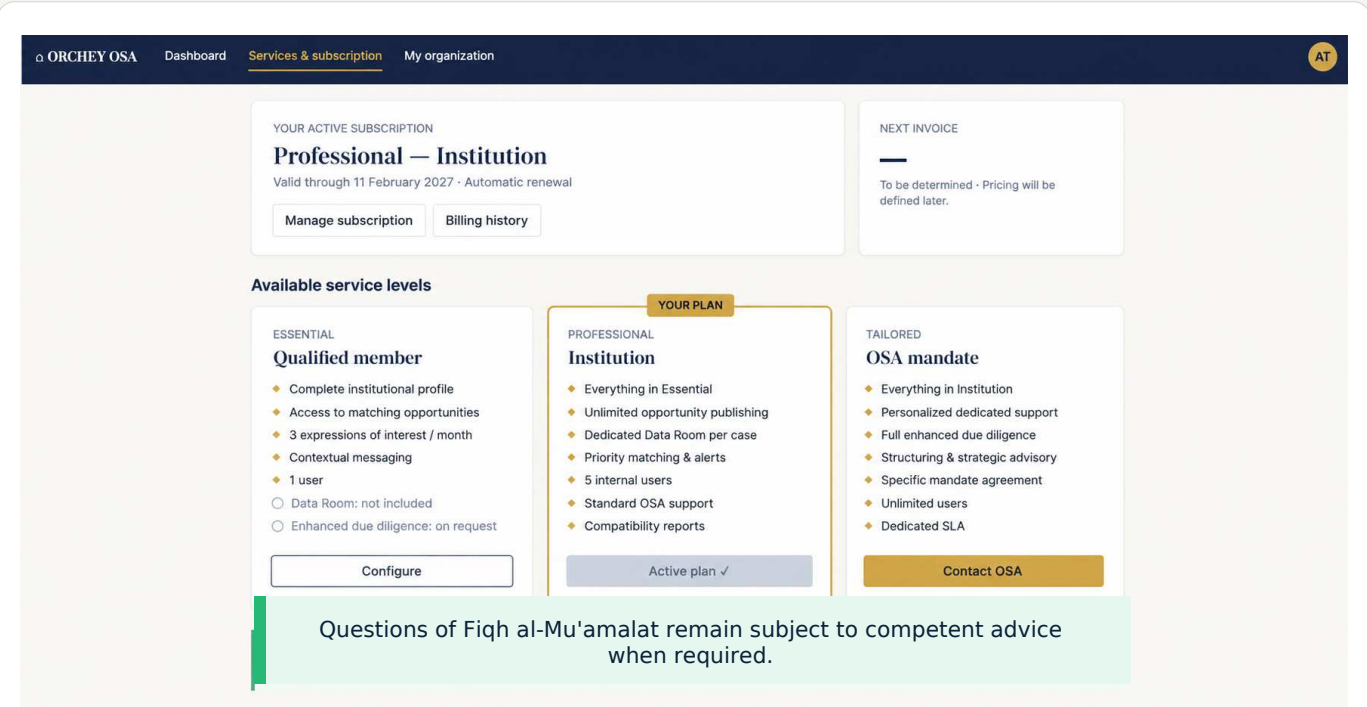
Outcome & alert

Authorized, refused or sensitive actions may be distinguished to facilitate control.

17 · SERVICES & SCOPE

Distinct service levels, one consistent scope of responsibility

Platform access, institutional services and tailored mandates may be differentiated without conflating OSA's services with the financial or commercial operations carried out by the parties.



Illustrative interface · Service levels and pricing under definition

Platform access

Qualified access to digital functions provided according to service level and permissions.

OSA support

Qualification, coordination, due diligence and assistance may be provided under the agreed mandate.

Tailored mandate

Complex needs may be addressed through a defined scope, deliverables and specific terms.

Non-custodial scope. OSA charges only for its own services. The platform neither receives nor holds the parties' funds, offers no investment accounts, and guarantees no return.



18 • CONTACT & CLOSING

Present your need or your opportunity

An initial exchange helps determine whether the request falls within OSA's scope of intervention and which working framework would be appropriate.

EMAIL

contact@orcheyadvisory.com

WEBSITE

orcheyadvisory.com

STATUS

Institutional project in preparation

PLANNED ESTABLISHMENT

Riyadh, Saudi Arabia

SCOPE

Africa · Gulf Countries · International Markets

Visit the website



orcheyadvisory.com

Solid principles for lasting trust.

This brochure presents Orchey Strategic Advisory in its current form: an institutional project in preparation. It does not constitute an investment offer or financial solicitation and provides no guarantee of financing, returns, or completion of any transaction.

Connecting ambitions. Building lasting trust.