

CIBAR ADVANCED TECHNOLOGIES

Information is strength. Technology is sovereignty.

Digital intelligence · Field coordination · Integrated systems.



A joint investment project / CODA & Iraq's Defence Industries Commission

THE CENTRE / AN IRAQI PARTNERSHIP

Technology expertise, for institutional needs.

CIBAR Advanced Technologies is a joint investment project between CODA and Iraq's Defence Industries Commission. The centre brings together artificial intelligence, digital security, communications, monitoring and automation to develop institutional solutions focused on data protection, system integration and national capacity building.



CODA



Iraq's Defence Industries Commission

01

Our vision

Iraqi technology capability that supports institutional decisions and sustainable systems.

02

Our mission

Translate requirements into design, integration, operation and knowledge transfer within a clear scope.

From institutional needs, to a connected system.

01	02	03
DATA & INTELLIGENCE	PROTECTION & CONNECTIVITY	OPERATIONS & CAPABILITY
CYBAR OSINT	04	CODACS Agent
Tracking & tracing	06	Ministry of Defence
Ministry of Interior	08	Iraqi National Security Service
Iraqi National Intelligence Service	10	Artificial intelligence & automation
Software & data sovereignty	12	Operations rooms & control
Cybersecurity	14	Security operations as a service
Monitoring & Internet of Things	16	Early warning & emergencies
Communications & integration	18	Access & vehicle movement
Laboratory systems & simulation	20	Training & knowledge transfer
CODA / Security & institutions	22	CODA / Buildings, commerce & education
Solution pathways	24	Delivery & acceptance
Contact CIBAR	26	

CODA SYSTEMS / DIGITAL INTELLIGENCE

CYBAR OSINT

CODA's open-source intelligence system for security agencies and media-monitoring channels.



01

Media monitoring

Open sources and searchable, classifiable content.

02

Situational awareness

Maps, events and critical infrastructure in one context.

03

Evidence & analysis

Source-linked findings and analysis supporting review.

04

Decision briefings

Summaries, dashboards and reports for teams and leaders.

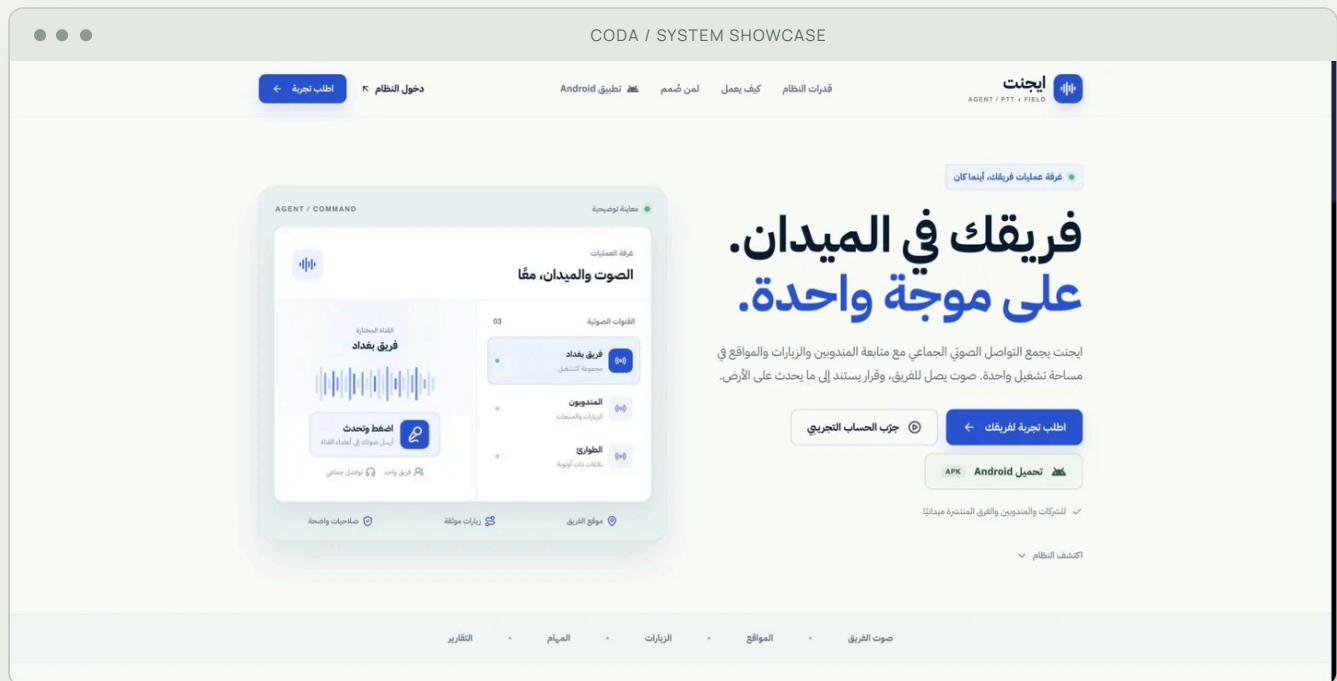
cn.go.iq ↗

CYBAR OSINT is CODA software; the CIBAR centre is the investment partnership with the Defence Industries Commission.

CODA SYSTEMS / FIELD TEAM COORDINATION

CODACS Agent

Team voice, location and tasks in one workflow.



Agent / Field communications and operations.

01

PTT voice channels

Channels for teams and supervisors, with live network-based communication.

02

Work orders

Assignment, follow-up, execution forms and arrival confirmation.

03

Locations & teams

Field visits, GPS checks and role-based permissions.

04

Task continuity

Save work orders and forms locally, then synchronise when connected.

FACILITY SECURITY

FIELD TEAMS

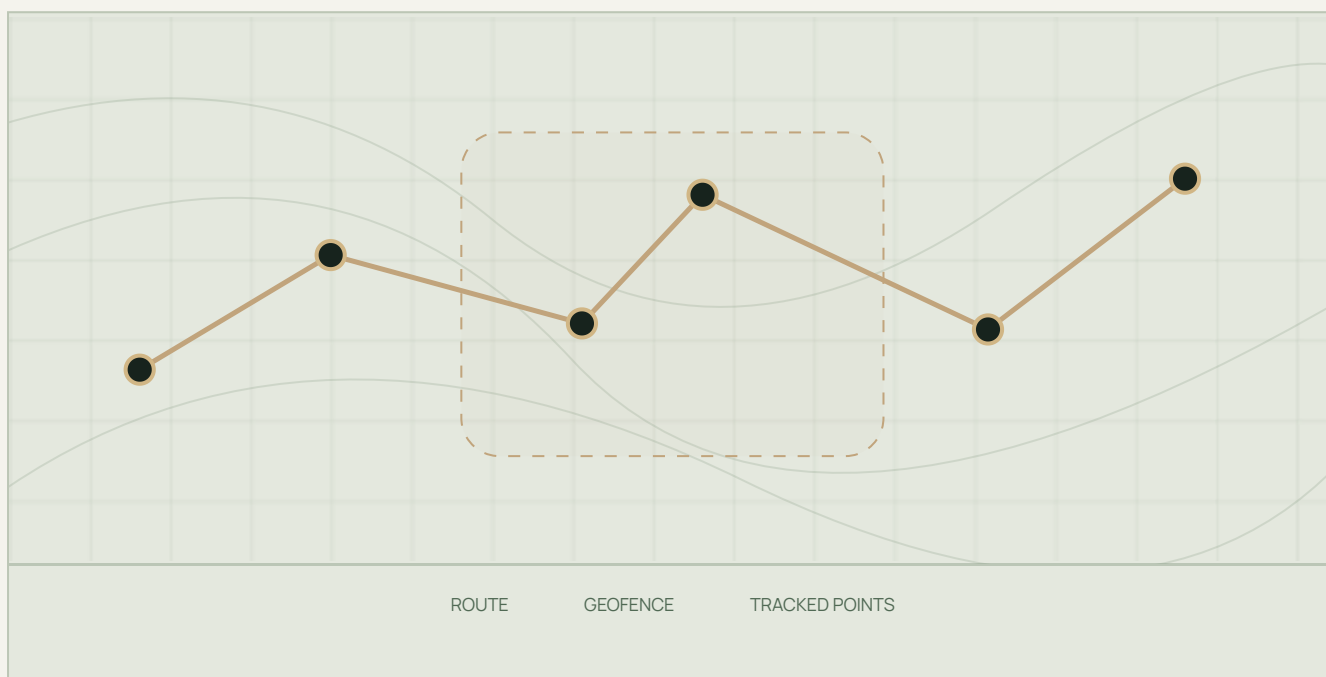
INSPECTION & SERVICES

agent.go.iq

Institutional trial edition • Live voice requires connectivity.

Clear movement. Connected monitoring.

Tracking systems connect location, movement and alerts to operations.



Vehicles

Fleets, equipment and vehicle movement.



Targets

Defined targets and assets within the mission scope.



Personnel

Personnel, field teams and location follow-up.



Containers

Containers, consignments and movement routes.

LOCATION & LAST CONTACT

MOVEMENT HISTORY

GEOFENCE ALERTS

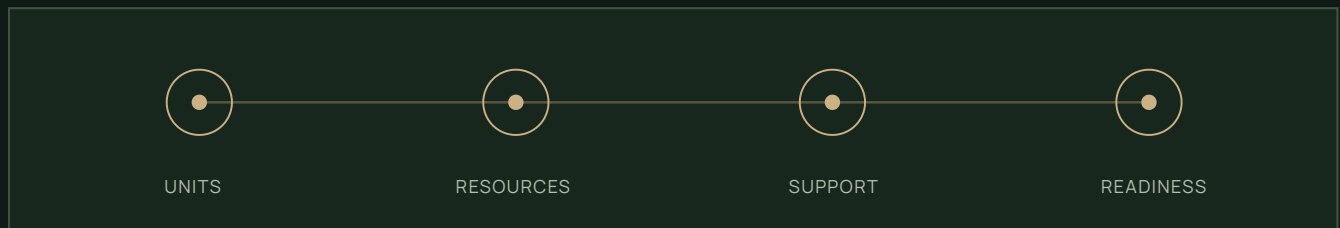
REPORTS & PERMISSIONS

GPS and IoT sensor integration with FAIZ modules; tracking devices selected for the asset and operating environment.

Ministry of Defence

For operations, support, resources, facilities and training functions.

Managed readiness. Connected support.



D01

Unit Readiness Management

Personnel, equipment, readiness indicators and leadership reports.

D02

Technical Support & Maintenance

Scheduled maintenance, work orders, spares and fault records.

D03

Asset Custody & Supply Stores

Assets, custody, stock movement and receipt or handover records.

D04

Transport & Fleet Movement

Vehicles, transport tasks, routes, tracking and utilisation.

D05

Base & Facility Security

Permits, visitors, gates, access zones and site events.

D06

Training, Simulation & Assessment

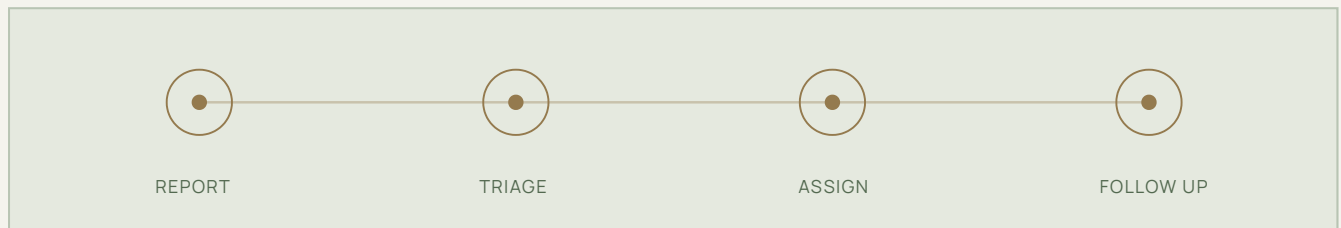
Training plans, learning scenarios, outcomes and competency assessment.

Development, customisation and integration to institutional requirements and project scope.

Ministry of Interior

For policing, traffic, emergency response, border-entry and evidence functions.

Recorded reports. Organised action.



I01

Reports & Emergency Dispatch

Intake, categorisation, assignment and response follow-up.

I02

Patrol & Duty Management

Teams, shifts, duties, locations and execution reports.

I03

Case & Procedure Management

Cases, tasks, documents, referrals and follow-up schedules.

I04

Evidence & Chain of Custody

Evidence identifiers, receipt and transfer records, permissions and audit trails.

I05

Traffic & Vehicle Administration

Vehicle records, service procedures, fleet movement and reports.

I06

Entry Points & Container Movement

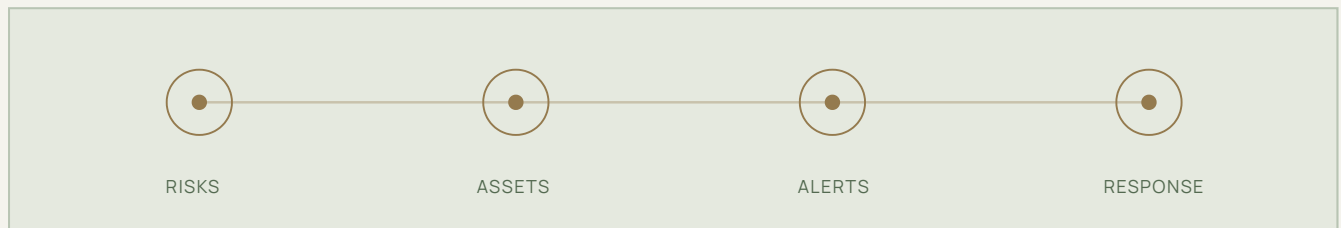
Entry records, containers, consignments, appointments and inspection follow-up.

Development, customisation and integration to institutional requirements and project scope.

Iraqi National Security Service

For risk, facility protection, reporting and coordination functions.

Understood risks. Institutional follow-up.



N01

Early Warning & Risk Management

Indicators, risk registers, alerts and review priorities.

N02

Critical Infrastructure Protection

Assets, sites, sensors, events and monitoring plans.

N03

Reports & Case Follow-up

Intake channels, categorisation, responsibilities and handling status.

N04

Coordination & Information Exchange

Referrals, information requests, approvals and role-based sharing.

N05

Field Monitoring & Inspection Teams

Field tasks, inspection forms, visits and completion reports.

N06

Access Governance & Audit

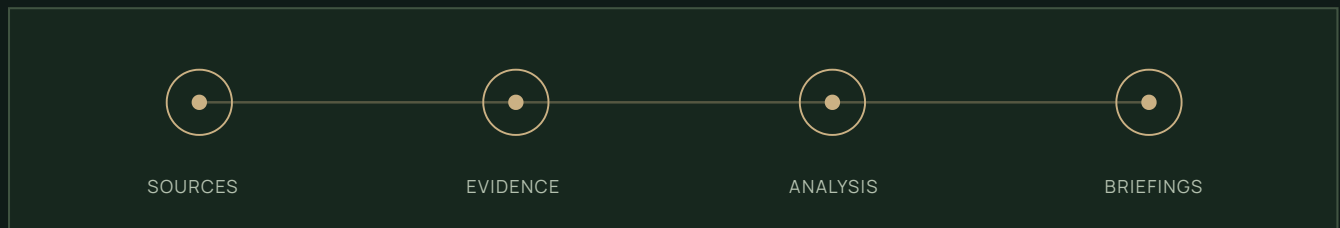
Roles, permissions, approvals, access logs and review.

Development, customisation and integration to institutional requirements and project scope.

Iraqi National Intelligence Service

For information, analysis, sources, reporting and knowledge functions.

Connected information. Precise briefings.



X01

Open-Source Intelligence

Media monitoring, search, categorisation and source linking through CYBAR OSINT.

X02

Information & Analysis Workflow

Information intake, organisation, assessment, review and referral.

X03

Sources & Knowledge Files

Documents, references, evidence, source links and update history.

X04

Temporal & Geospatial Analysis

Events, maps, timelines and reviewable trends.

X05

Leadership Briefings & Reports

Summaries, reports, approvals and distribution by permission.

X06

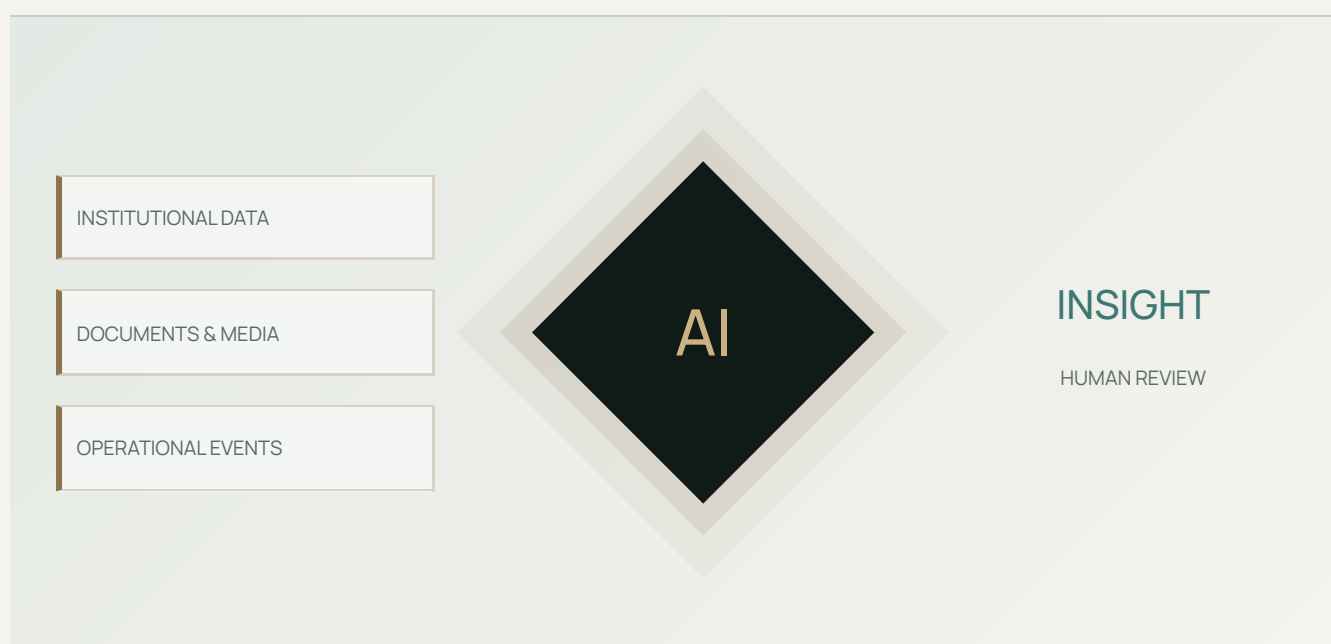
On-Premises Analysis Environments

Institutional workspaces, data, permissions and governed internal integration.

Development, customisation and integration to institutional requirements and project scope.

Data understood. Work moving forward.

Apply analytics and AI to data and media, and organise repetitive tasks, with human review of outputs that support decisions.



01

Analysis & classification

Organise information and surface patterns and indicators relevant to the institution.

02

Media analysis

Extract information from text, audio and images for a defined task.

03

Process automation

Connect workflow steps and reduce repetitive entry within permissions.

04

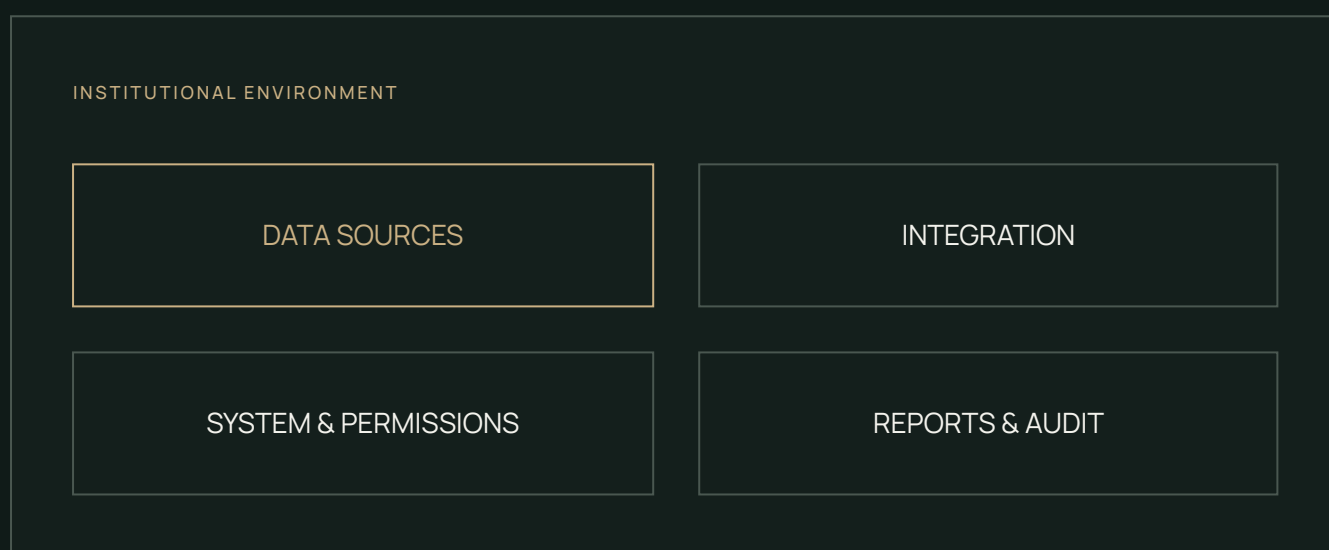
Review & approval

Clear criteria for data quality, output accuracy and intended use.

DATA & INTELLIGENCE / INSTITUTIONAL SOFTWARE

Data in its place. Permissions made clear.

Develop tailored systems and connect them to the existing environment, designing for data ownership, access, audit and the institution's hosting policy.



01 Tailored applications

Data models, workflows and interfaces aligned with the institutional task.

02 Deployment choices

On premises, private cloud or hybrid, under the approved design.

03 Operational governance

Roles, audit records, backup, recovery and change management.



OPERATIONS / CONTROL ROOMS

A shared view. A coordinated response.

Design and integrate operations rooms and central displays, connecting information and alerts to team responsibilities and response workflows.

01

Operational picture

Sources, assets and events arranged in a clear view.

02

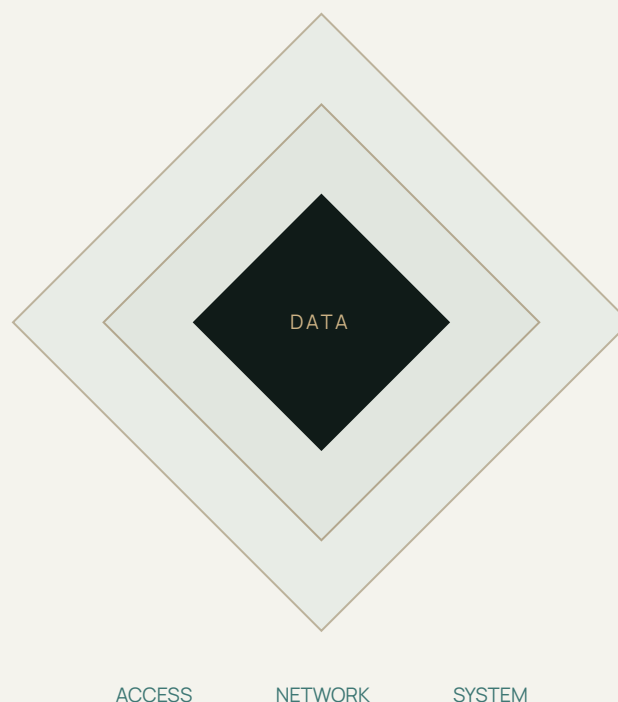
Control & coordination

Permissions, procedures and action follow-up within the integration scope.

PROTECTION & CONNECTIVITY / CYBERSECURITY

Protection designed, and reviewed over time.

Assess the digital environment, harden systems and networks, and organise access, with testing and follow-up linked to actual institutional risks and activities.



01

Risk assessment

Review assets, access and priority technical gaps.

02

Hardening & organisation

Configure accounts, networks and settings by role.

03

Testing & improvement

Authorised tests and a plan to resolve findings.

04

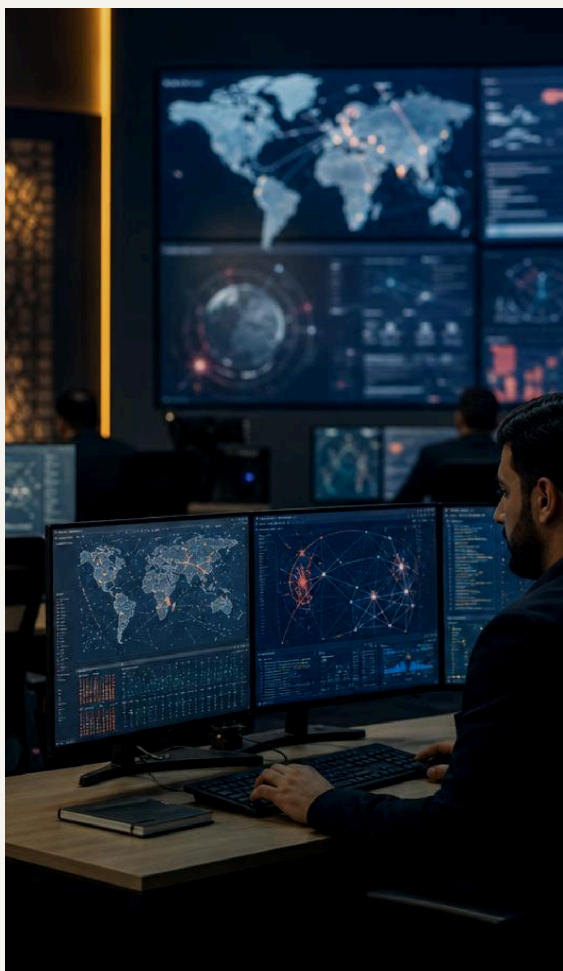
Recovery & continuity

Backup and recovery policies, with follow-up responsibilities.

PROTECTION / SECURITY OPERATIONS AS A SERVICE

The signal arrives. The team knows what follows.

Design a SOCaaS scope bringing together logs, alerts, analysis and response support, linked to clear responsibilities at the client institution.



Digital security operations, analysis and alerts.

01 Collect & monitor

Approved log sources and monitoring rules suited to the environment.

02 Triage & analyse

Assess indicators, priorities and information needs.

03 Escalate & respond

Communication and permissions for containment and follow-up.

04 Report & improve

Case reports, lessons learned and monitoring-rule updates.

A DEFINED OPERATING SCOPE

Service scope, coverage hours and escalation levels are defined in the agreement.

OPERATIONS / MONITORING & IOT

The site connects. Information comes together.

Connect cameras, sensors and assets to a monitoring system for clearer context around site status, equipment movement and operational events.



Field monitoring, sensing and connectivity.

01

Area monitoring

Select optical and thermal technologies suited to the site and task.

02

Asset sensing

Status and environmental readings, with sensor-based alerts.

03

Fleet movement

Tracking, routes and movement history for vehicles and equipment.

04

Unified monitoring

Sources, events and reports by permission and integration scope.

OPERATIONS / WARNING & EMERGENCIES

Earlier awareness. A clear response path.

Organise alerts and connect them to operations rooms and relevant teams under the institution's procedures, responsibilities and escalation levels.

01

Event captured

A signal from a sensor, system or report within approved sources.

02

Verification & priority

Assess context, urgency and the relevant team.

03

Coordinated action

Route the event and follow the response within permissions.

04

Closure & review

Record the action and review the process to improve performance.

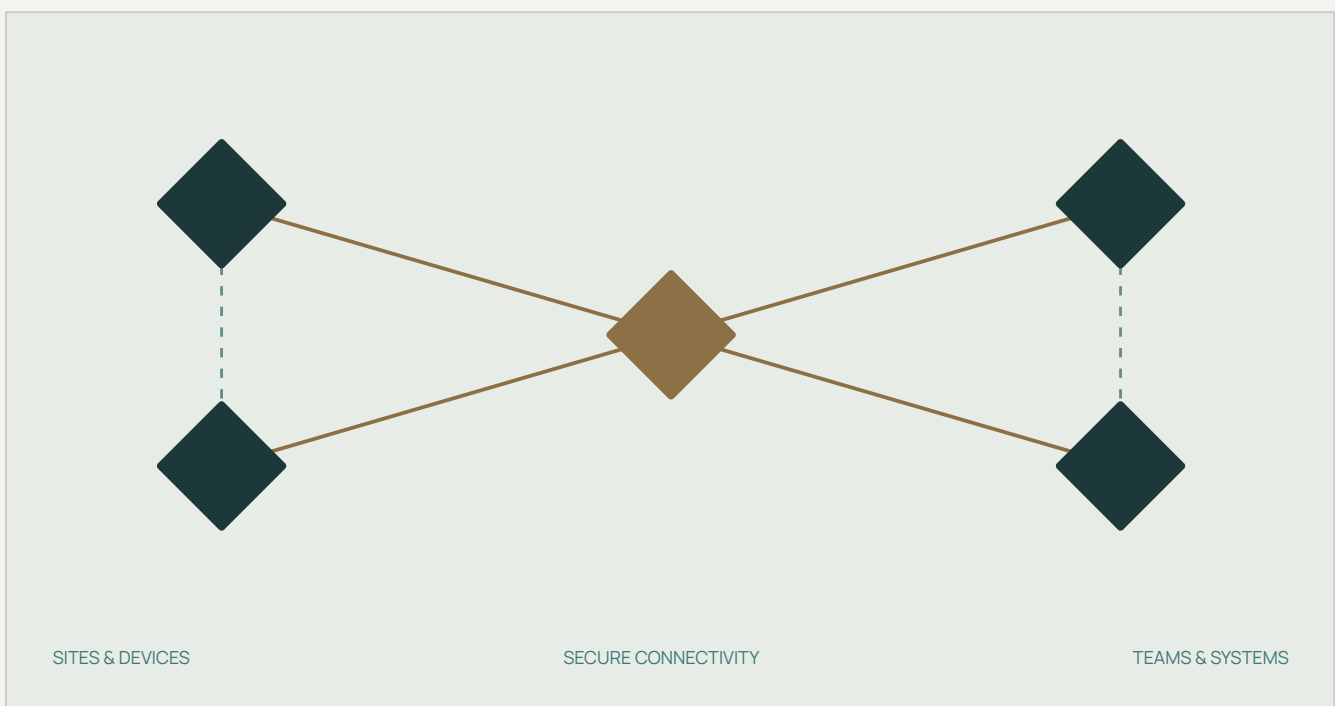
INSTITUTIONAL DELIVERABLES

Alert categories · Responsibility matrix · Escalation paths · Event log · Follow-up reports.

PROTECTION & CONNECTIVITY / COMMUNICATIONS

Connectivity maintained, through deliberate design.

Design and integrate networks and communication channels for sites and teams, defining encryption, isolation, connectivity and fallback needs for the operating environment.



01 Local & isolated networks

Network segmentation, access controls and required system connections.

02 Field communications

Radio or satellite options according to site coverage and use requirements.

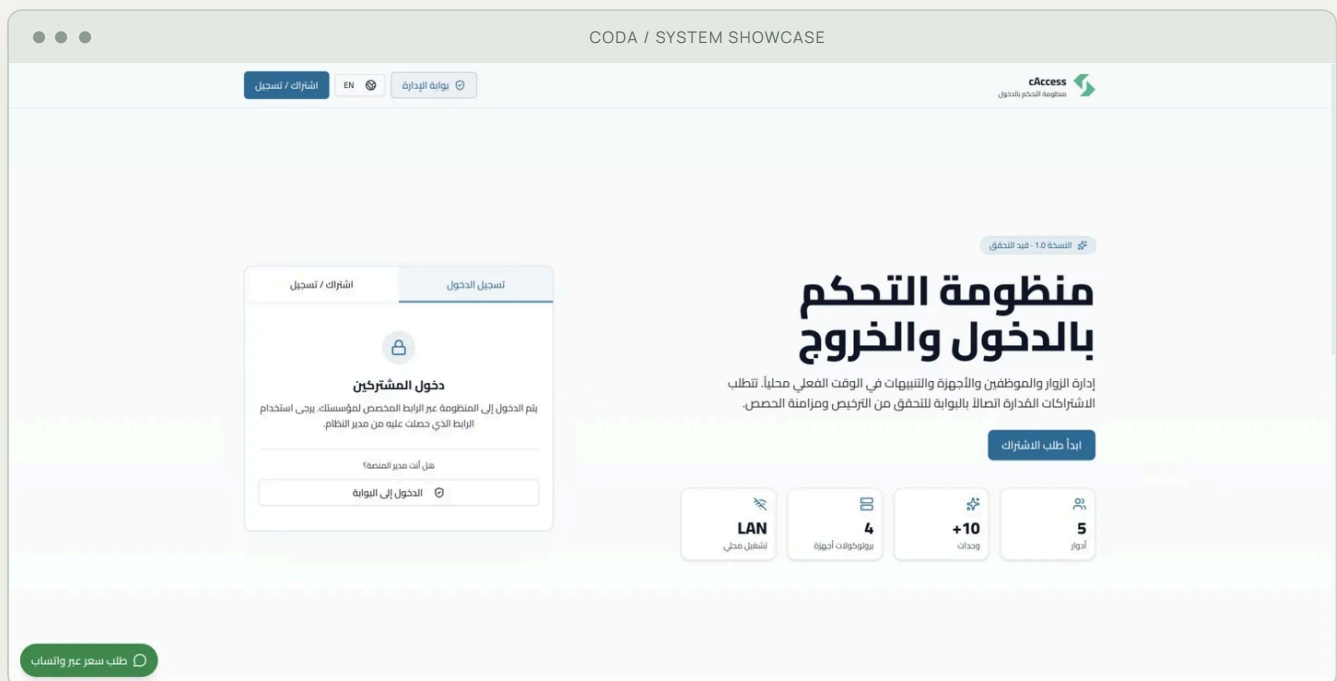
03 Test links & alternatives

Review performance, interruption points and connectivity recovery.

OPERATIONS / ACCESS & VEHICLE MOVEMENT

Movement recorded. Permissions organised.

Integrate access, attendance, gates and parking with roles and site rules, using components and systems compatible with the approved design.



cAccess / CODA software showcase for integration.

01 cAccess / Access & attendance

Visitor, employee and attendance management, with gate-device integration.

02 MAWAQIF / Vehicle movement

Organise vehicle movement, tickets and parking operations.

COMPATIBILITY IS PART OF THE DESIGN

Devices, protocols, permissions and movement workflows are reviewed before delivery approval.

DATA & INTELLIGENCE / LABORATORIES & SIMULATION

Testing grounded in reality. Learning before deployment.

Systems to organise laboratory data, results and reports, with operational and training simulations to assess requirements before field deployment.



Electronic integration and technical testing.

01

Laboratory data

Records, samples, results and reports within reviewable workflows.

02

Simulation & training

Models, scenarios and tests supporting learning and design evaluation.

CAPACITY BUILDING / TRAINING & KNOWLEDGE TRANSFER

Systems advance, when their teams do.

Training linked to the solution and its use environment helps teams operate, monitor and manage events and changes systematically.

KNOWLEDGE TRANSFER PATH

UNDERSTAND

PRACTISE

REVIEW

01 Role-based training

System operators, technical administrators and monitoring teams, each trained for their tasks.

02 Relevant exercises

Workplace scenarios with reviewable outcomes.

03 Usable documentation

Operating guides, follow-up steps, permissions and change management.

INTENDED OUTCOME

A team that understands the system, its roles and the support path when needed.

SOFTWARE DEVELOPED BY CODA / BY SECTOR

Security & operations. Institutional management.

Published systems serving institutions and complementing the centre's technology portfolio.

01

SECURITY & ACCESS

CYBAR OSINT

Media monitoring · Maps · Sources & evidence

cAccess / Access & attendance

Visitors · Employees · Gates · Reports

Bajat

Badges · Zones & gates · Approvals

02

SMART OPERATIONS

Mawaqif

Entry & exit · Parking operations · Collection

cFlow / Display management

Content · Scheduling · Devices & sites

03

INSTITUTIONAL MANAGEMENT

Aamal Hub

Business and financial operations

Qiyada

Directives · Tasks · Execution follow-up

Shuon

Requests, services and institutional follow-up

CODA HRM

Employees · Attendance · Payroll

SOFTWARE DEVELOPED BY CODA / BY SECTOR

Multiple sectors. One software expertise.

Published systems serving institutions and complementing the centre's technology portfolio.

01

BUILDINGS, PROPERTY & PROJECTS

Bunyan

Contracts · Projects · Costs · Work measurement

Osos

Building operations · Services & maintenance

Amlak

Property, listings and broker management

02

COMMERCE & CULTURAL SITES

Rofoof

Sales · Inventory · Purchasing · Cash desk

Qishla

Tickets · Sales · Bookings · Reports

03

EDUCATION & SCHOOL ADMINISTRATION

Sofoof

Students · Fees · Attendance · Family communication

SOLUTION PATHWAYS / FROM GOALS TO COMPONENTS

One operational need, components working together.

Solutions are built around the institutional goal, connecting software, communications, equipment and training within a testable delivery scope.

01 A site needs unified monitoring

Cameras, sensors and events, with a shared view, alerts and follow-up responsibilities.

02 A team needs clearer coordination

Operations room, information sources and communications, with escalation and documentation.

03 An institution needs governed digital operations

Tailored software, permissions and audit, with deployment, backup and recovery policies.

04 An organisation needs team readiness

Training, simulation, operating guides and assessment exercises aligned with the task.

DELIVERY APPROACH / DESIGN, TEST & HANDOVER

An agreed scope. Outcomes that can be verified.

From the first assessment to operation and knowledge transfer, each deliverable is linked to requirements, acceptance criteria and clear responsibilities.

01

Define requirements

Objectives, existing systems, risks and authorised stakeholders.

02

Design & prototype

Solution architecture, components, integration and test plan.

03

Integrate & test

Setup, integration, and testing of agreed performance and functions.

04

Accept & transfer knowledge

Acceptance records, operating documentation, training and a support plan.

AT THE START OF AN ENGAGEMENT

Share the task, site, existing systems, priorities and target schedule to define the appropriate engagement.



CONTACT CIBAR

Start with your needs.
Shape the path together.

For technical consultation and discussions on projects and institutional solutions.

EMAIL

cibar@coda.com.iq ↗

TELEPHONE

[+964 770 494 0494](tel:+9647704940494) ↗

WEBSITE

cibar.coda.com.iq ↗

A joint investment project between CODA and Iraq's Defence Industries Commission.

CIBAR