CYBERSECURITY & IT

Cynthra

COMPANY PROFILE

Confidence, engineered.

Governance, security testing, awareness, cybersecurity strategy and specialist talent.

Cynthra Company
Riyadh, Saudi Arabia

Contents

Our company, services and approach to delivery

About Cynthra & how we work 03 - 04

Organizations & their needs 05

Saudi frameworks 06

Services & deliverables 07 - 11

Method & illustrative example 12 - 13

Contact & getting started 14

About Cynthra

A Saudi cybersecurity and information technology company

Cynthra helps organizations assess controls, test systems and develop cybersecurity policies and plans, with each engagement shaped around the organization’s needs.

Our vision

Make cybersecurity decisions clear and connected to business objectives.

Our services at a glance

Service	Key deliverables
Governance & compliance	Policies & action plan
Security testing	Findings & guidance
Awareness & training	Materials & assessments
Strategy	Initiative roadmap
Specialist talent	Shortlist & assignment plan

Our mission: help organizations assess risk and address gaps through clearly defined services and deliverables.

How Cynthra works

Agree scope, deliverables and responsibilities before delivery begins

Agreed scope

Before delivery

We review the systems and documents in scope, the schedule and service boundaries. We then document roles, contact points and how findings will be approved.

Reviewable deliverables

Set deliverables and acceptance criteria in the proposal and scope of work.

Connect findings with evidence, recommendations and a remediation owner.

Explain the outputs and document feedback and agreed follow-up.

Organizations & their needs

Service scope shaped around the operating environment and requirements

Target organizations	Examples of needs
Construction & project management	Contractor access and project security
Technology & service companies	Application testing and change governance
Organizations with multiple sites	Consistent controls and evidence across sites
Organizations with regulatory requirements	Gap assessment and remediation planning

We support private and public sector needs, subject to service scope and contracting requirements.

Saudi frameworks

Confirm applicability before the assessment begins

Reference	How it informs the scope
NCA ECC 2:2024	Review controls, gaps, evidence and remediation actions
NCA CCC-2:2024	Review cloud security and responsibilities for the organization’s role
SAMA CSF	Review governance and maturity where applicable
PDPL	Assess gaps against the law and its regulations

These are work references, not Cynthra certifications. Applicable requirements are defined within each engagement.

Governance, Risk & Compliance

GRC

Assess controls, develop policies and prioritize cybersecurity risks

	SERVICE SCOPE		WHAT YOU RECEIVE
1	Assess gaps against applicable controls.	→	Policies, procedures and a requirements and evidence matrix.
2	Develop policies and procedures, and review evidence.	→	A gap assessment report and risk register.
3	Assess risks and prioritize treatment actions.	→	An action plan with owners, deadlines and closure status.

Example output: a documented finding linking the control, evidence, action and remediation owner.

Vulnerability Assessment & Penetration Testing

VAPT

Validated technical findings, with business impact and remediation priorities

	SERVICE SCOPE		WHAT YOU RECEIVE
1	Agree assets, test boundaries and written authorization.	→	An executive summary for management.
2	Test applications or infrastructure within the agreed scope.	→	A technical report with evidence and remediation guidance.
3	Validate findings and assess their impact.	→	Agreed finding retests and a status report.

Before testing: agree testing windows, operating constraints and escalation channels.

Cybersecurity & IT Talent

TALENT

Support project needs with defined roles and selection criteria

	SERVICE SCOPE		WHAT YOU RECEIVE
1	Define the role, skills, duration and work location.	→	A role description and evaluation criteria.
2	Assess candidates against the assignment requirements.	→	A candidate shortlist and skills assessment summary.
3	Coordinate assignment scope and onboarding.	→	An assignment plan and delivery checkpoints.

The engagement model, availability and contracting arrangements follow a review of the project's needs.

Awareness & Training

AWARENESS

Content connected to employee roles and the risks they encounter

	SERVICE SCOPE		WHAT YOU RECEIVE
1	Define target audiences and program objectives.	→	An awareness plan and delivery schedule.
2	Develop content and workshops for leaders and teams.	→	Arabic or English materials, as agreed.
3	Assess understanding and identify follow-up topics.	→	Pre- and post-assessments and a results report.

Potential topics: phishing, data protection, file sharing and the responsibilities of privileged users.

Strategy & Roadmaps

STRATEGY

Cybersecurity initiatives aligned with objectives, risk and delivery capacity

	SERVICE SCOPE		WHAT YOU RECEIVE
1	Review the current position and business objectives.	→	A cybersecurity strategy and initiative roadmap.
2	Prioritize initiatives and their dependencies.	→	Delivery sequencing and indicative resource needs.
3	Assign responsibilities and performance measures.	→	Performance measures and a periodic review approach.

The plan sets out what starts first, why it matters, who owns it and how progress is measured.

Delivery & Quality Assurance

Approved scope, documented evidence and clear acceptance criteria

01	**Understand**	Confirm owners, assets, frameworks and scope boundaries.
02	**Assess & validate**	Gather evidence and review findings with stakeholders.
03	**Plan remediation**	Prioritize by risk and assign owners and target dates.
04	**Deliver & follow up**	Explain outputs and document acceptance and agreed follow-up.

Agree evidence-sharing channels, access permissions and data retention as part of the engagement.

Illustrative Example: Access Review

A hypothetical scenario to explain the method, not a completed client engagement

The need	An organization wants to verify that user and contractor access matches approved roles and documented requests.
Our approach	Match accounts to roles and access requests, document exceptions and review them with system owners.

Review area	Illustrative output
Accounts & access	Account, role and approval-request matrix
Findings & remediation	Exception register with owners and target actions

Follow-up measures: account-to-request coverage and exception closure confirmed by the responsible owner.



Let’s discuss your needs

Tell us the service, systems in scope and your target date

info@cynthra.sa

+966 55 127 6880

cynthra.sa

LinkedIn X

Cynthra Company

Cybersecurity & information technology

Riyadh, Saudi Arabia

We review your needs and eligibility requirements, then propose a scope and deliverables for discussion.