CYBERSECURITY ASSESSMENTS

FOR ORGANIZATIONS IN LIBYA

Know what is exposed. Know what matters first. Know what to do next.

ASSESS	PRIORITIZE	IMPROVE

Service	Cybersecurity Assessments
Designed for	Organizations operating in Libya
Approach	Assess • Prioritize • Improve
Engagement	Confidential and scope-defined

ALKABAS GLOBAL

Engineering-led technology, managed services, and cybersecurity

Confidential service overview

Cybersecurity Assessments for Organizations in Libya

Know what is exposed. Know what matters first. Know what to do next.

What this assessment provides

A focused, evidence-based cybersecurity assessment from Alkabas Global helps leadership understand the organization's real security posture, prioritize the risks that matter, and move forward with a practical improvement plan.

Security decisions need evidence, not assumptions

Many organizations have firewalls, antivirus, backups, policies, and technical teams. The difficult question is whether management can prove that the right controls are in place, working as intended, monitored, documented, and improved when gaps are found.

A cybersecurity assessment replaces assumptions with a clear picture of what is protected, what is exposed, what could disrupt operations, and what should be addressed first. The goal is not to create fear or produce a long list of technical findings. The goal is to give the organization clarity, ownership, and a defensible plan.

What Alkabas Global can assess

Each engagement is scoped around the organization's environment, risk profile, sector, and operational priorities. Depending on the agreed scope, the assessment may include:

Governance and compliance readiness

Policies, responsibilities, risk ownership, awareness, third-party controls, evidence quality, and readiness against relevant Libyan requirements. Where appropriate, findings can be mapped to the NISSA Essential Cybersecurity Controls and supported by recognized international frameworks.

Network and infrastructure security

Network architecture, segmentation, firewall policy, VPN and remote access, wireless security, management exposure, server hardening, endpoint controls, and critical infrastructure dependencies.

Identity and privileged access

User lifecycle controls, privileged accounts, multi-factor authentication, role-based access, dormant accounts, administrative paths, and least-privilege practices.

Vulnerability and exposure management

External and internal exposure, authenticated and unauthenticated vulnerability scanning where authorized, patching gaps, unsupported systems, prioritization, and remediation validation.

Logging, monitoring, and incident readiness

Log coverage, alerting, escalation, incident-response procedures, evidence preservation, monitoring maturity, and the organization's ability to detect and explain abnormal activity.

Backup, recovery, and operational resilience

Backup coverage, restoration readiness, disaster-recovery dependencies, business-continuity controls, recovery ownership, and the ability to maintain or restore essential services.

Applications, cloud, and operational technology

Web applications, APIs, cloud or SaaS environments, hosting exposure, workload access, data protection, and OT or industrial environments when included in the authorized scope.

How the assessment works

1. Scope and authorization

We define the systems, locations, objectives, testing boundaries, stakeholders, and rules of engagement before technical work begins. Active testing is never performed without written authorization.

2. Evidence and current-state review

Our team reviews available documentation, policies, configurations, diagrams, asset information, logs, and operating procedures, then interviews the relevant technical and business owners.

3. Technical validation

We validate selected controls through configuration review, architecture analysis, exposure checks, vulnerability assessment, and other authorized testing. Missing evidence and scope limitations are recorded rather than hidden.

4. Risk prioritization

Findings are assessed according to likelihood, impact, control effectiveness, and operational context. The result is a prioritized view of risk, not a flat scanner export where every issue appears equally urgent.

5. Management reporting and roadmap

Leadership receives a clear explanation of the current posture, the most important risks, ownership, recommended actions, quick wins, and a phased improvement roadmap.

6. Remediation and validation, when requested

Assessment and remediation are kept as separate scopes to protect objectivity. Alkabas Global can support implementation after the assessment, and selected findings can be retested to confirm closure.

What the organization receives

Deliverables are agreed during scoping and may include:

- Executive cybersecurity posture summary
- Evidence-based technical findings
- Prioritized cyber risk register
- Governance or compliance gap analysis
- Vulnerability assessment report
- 30/60/90-day remediation priorities
- Longer-term security maturity roadmap
- Management presentation and decision briefing
- Validation or retest report when commissioned

Built for organizations that cannot afford uncertainty

This service is suitable for government entities, banks and financial institutions, oil and gas organizations, telecom operators, healthcare providers, logistics companies, and private organizations that depend on networks, systems, data, or public-facing digital services.

It is especially valuable before a major technology project, after rapid growth, when responsibilities are unclear, when security controls have not been independently reviewed, after a significant incident, or when management needs evidence for risk and compliance decisions.

Why Alkabas Global

Alkabas Global is an engineering-led Libyan technology and cybersecurity partner. We approach assessments from the reality of how organizations operate, not from a product catalogue.

Our work is designed to provide:

- Local operational understanding with internationally recognizable methodology
- Vendor-neutral findings based on evidence and business risk
- Practical recommendations that account for existing systems, budgets, dependencies, and continuity needs
- Clear separation between assessment findings and potential implementation work
- Management-level clarity alongside the technical depth required by IT and security teams

We do not use an assessment to create fear, push unnecessary hardware, or bury management in jargon. We identify what matters, explain why it matters, and define what should happen next.

Frequently asked questions

Is a cybersecurity assessment the same as a penetration test?

No. A penetration test is a focused form of authorized security testing. A cybersecurity assessment can be broader and may cover governance, architecture, identity, vulnerabilities, logging, incident readiness, backup, continuity, cloud, and technical controls. Penetration testing can be included or commissioned separately when appropriate.

Will the assessment disrupt our operations?

The engagement begins with non-intrusive review and evidence collection. Any active testing is agreed in advance, performed within written rules of engagement, and planned around operational risk.

Can you assess an environment with incomplete documentation?

Yes. Incomplete documentation is common and may itself be a control gap. We work with the evidence available, validate what can be confirmed, and clearly disclose missing evidence or limitations.

Does the assessment certify us as compliant with NISSA?

No. Alkabas Global does not claim to certify organizations on behalf of NISSA. Where relevant, the assessment can support NISSA readiness by mapping evidence and findings against applicable controls and identifying gaps that require attention.

Do we have to hire Alkabas Global for remediation?

No. The findings, priorities, and roadmap belong to the client. Remediation can be handled internally, by another provider, or under a separately approved Alkabas Global scope.

How long does an assessment take?

The timeline depends on the number of locations, systems, users, technologies, evidence availability, and testing depth. A clear timeline and required inputs are provided after the scoping discussion.

Move from uncertainty to a clear security plan

Clarity before action

Know what is happening. Know who owns it. Know what to do next.

Request a confidential scoping discussion with Alkabas Global to define the right cybersecurity assessment for your organization.

Request a confidential assessment	Speak to an engineer