A STRONGER WAY TO RUN IT

Always present. Ready to act.

Managed Services NOC Box

A local service presence. Shared specialist expertise.
AI-assisted operations with people in control.

Illustrative appliance concept. Final hardware is scope-dependent.

24/7 service model • Approval-led action • Weekly assurance

01 / EXECUTIVE OVERVIEW

More operational strength. *Less internal burden.*

Tawajud AI combines an on-site NOC Box, a remote Network Operations Centre and a shared service platform to move from fragmented support to a coordinated operating model.

24/7

Continuous oversight

Monitoring and critical response in the proposed flagship service.

5 min

Priority-one response

Proposed qualified-human acknowledgement target, not a fix guarantee.

Weekly

Visible service value

Health, incidents, changes, risks and next actions in one report.

Keep the expertise. Reduce the dependency.

Give a lean team access to broader engineering capability. The NOC handles agreed operations while your people retain priorities, approvals and ownership.

Make speed visible. Make control explicit.

Every issue follows a traceable path: ticket, owner, diagnosis, approval, action and verification. Management sees what changed and improved.

THE VALUE EQUATION

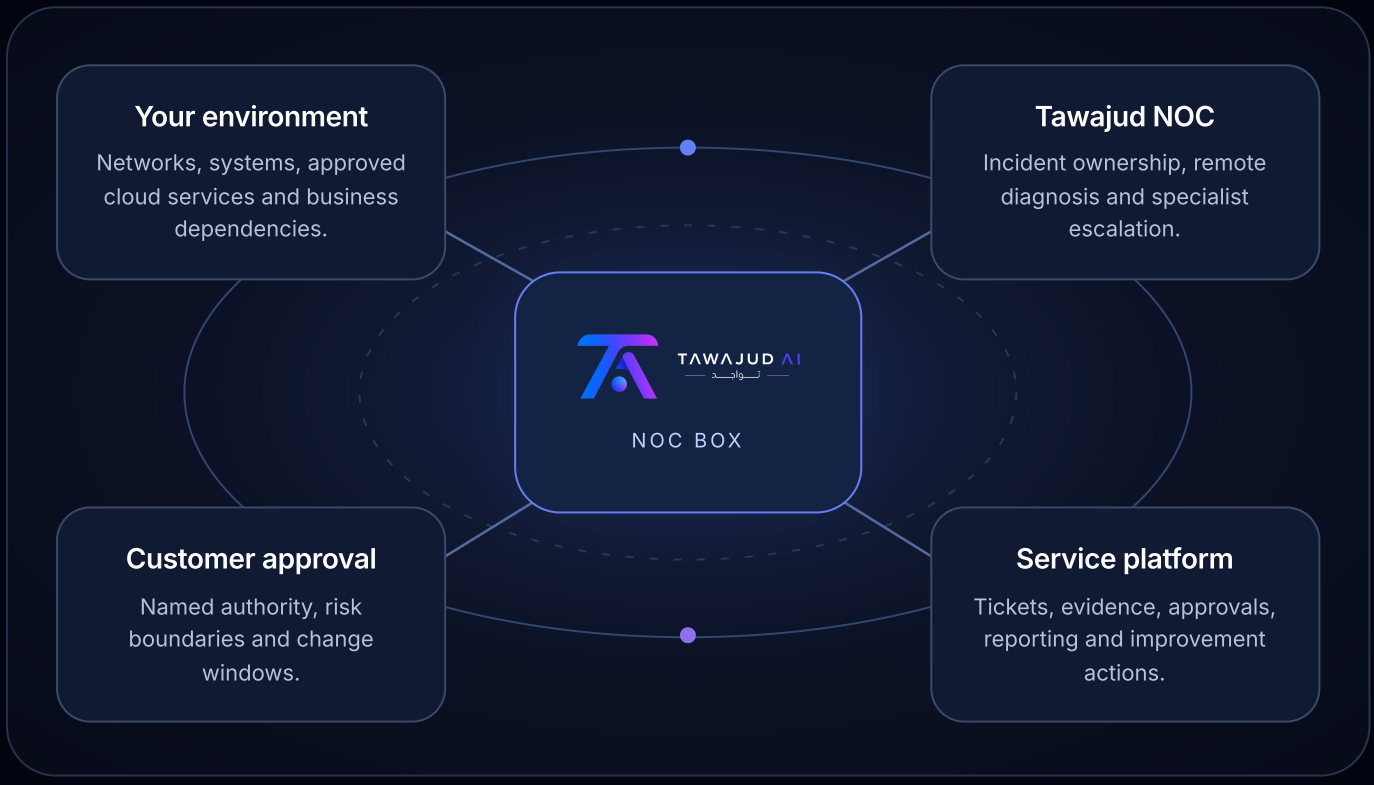
A stronger service for the customer. A repeatable delivery model for Tawajud.

This brochure presents a service offering and proposed targets. Scope, integrations, staffing, service hours and commitments are confirmed through onboarding and the signed service schedule.

02 / THE SERVICE ARCHITECTURE

Local presence. *Connected expertise.*

The Box is the customer-side service endpoint. The NOC brings people and process. The platform brings a shared view of the work.



Observe locally

Collect approved health and diagnostic evidence close to the systems it describes.

Act deliberately

Use authorised access and a reviewed plan rather than uncontrolled remote intervention.

Prove the outcome

Verify service recovery and preserve the work record for the customer.

One service record, not repeated handovers. The same ticket carries the technical context from the first alert to the weekly management report.

03 / INSIDE THE NOC BOX

Small footprint. *Wide operational reach.*

A managed local access and collection point, configured around the customer's approved assets and security boundaries.

Local visibility

Approved health checks, event collection, interface status, service tests and configuration snapshots where supported.

Controlled access

Restricted management connectivity, named identities and separate permissions for observation and authorised changes.

Guided execution

A customer-approved path to run tested diagnostic and remediation procedures against in-scope assets.

Evidence capture

Before-and-after checks, action transcripts and time records connected to the incident or change.

Customer readiness	Protected power, management-network access, approved connectivity, current inventory and a named service owner.
Resilient access	Monitor the Box heartbeat. Size a second collector, alternate connection or on-site fallback where service criticality requires it.
Right-sized deployment	Select the physical appliance or approved virtual deployment during design. Local AI processing is scoped separately; it is not assumed to run on every Box.

The Box is not a bypass. It operates within the customer's agreed access controls. It does not replace firewalls, high availability, backup or physical engineering.

04 / HOW WE WORK

One ticket. *A complete chain of action.*

Speed comes from having the context, ownership and permission ready—not from skipping controls.

01 **Detect or receive**
An approved monitor raises an event, or a customer submits a ticket through the agreed channel.

RECEIPT
Time, source, service

02 **Triage and diagnose**
The NOC validates impact, removes duplicate noise and assigns a named owner. AI may assist with evidence review.

OWNERSHIP
Severity, analyst, checks

03 **Plan and approve**
Prepare the action, impact, pre-checks and rollback. Obtain named approval or reference an existing standard-change authorisation.

CONTROL
Approved plan and scope

04 **Execute safely**
A qualified engineer or approved automation runs the authorised procedure within the agreed limits.

ACTION
Who, what, when

05 **Verify recovery**
Re-test the affected service. Failed checks trigger rollback or escalation; a successful command alone is not closure.

VALIDATION
Service checks and status

06 **Close and improve**
Record the outcome, confirm closure under the agreed policy and update recurring-problem actions and reporting.

ASSURANCE
Evidence, cause, follow-up

Customer in control: risky or out-of-scope changes stop at the approval gate. The model may suggest an action; it does not grant authority.

05 / SPEED WITH CONTROL

From approval to action. *In minutes, where eligible.*

Prepared access, clear authority and tested procedures can make routine recovery a short, controlled operation.

ILLUSTRATIVE WORKFLOW · NOT A RECORDED INCIDENT

00:00 — Ticket captured
A monitored service reports a recoverable fault.

02:00 — NOC owner engaged
The analyst confirms the affected service and business impact.

03:00 — Safe procedure selected
Evidence matches an approved, low-risk recovery runbook.

05:00 — Approval recorded
The authorised customer approver confirms the action.

08:00 — Remediation executed
The permitted procedure completes; the transcript is retained.

10:00 — Recovery verified
Health checks pass and the ticket moves to verified resolution.

5–15 min

Proposed execution + verification target
After approval, for validated low-risk runbooks with working remote access and no external dependency.

The ten-minute sequence is an example, not a universal restoration promise. Complex faults, security investigations, failed hardware, carrier outages and delayed approvals follow separate response and recovery plans.

06 / 24/7 OPERATING MODEL

Always-on oversight. *Expert-led response.*

The service design combines continuous monitoring, an accountable duty team and specialist escalation—not dependence on one individual.

NOC monitoring & first response

24/7 PROPOSED COVERAGE

Validate alerts, create and own incidents, run initial diagnostics, communicate impact and escalate unresolved or unacknowledged critical events.

Network, systems & cloud specialists

ESCALATION BY SCOPE

Investigate deeper faults, prepare changes, coordinate vendors and execute authorised recovery work. On-call availability is defined in the service schedule.

Service delivery management

CONTINUITY OF OWNERSHIP

Review SLA results, recurring incidents, aged tickets and improvement actions. Maintain the customer communication and governance rhythm.

Customer service owner & approver

RETAINED AUTHORITY

Set business priorities, accept risk, approve controlled changes and provide the access or local assistance needed to restore service.

When an incident is major

Assign an incident lead, open the agreed communication bridge, protect the timeline and coordinate restoration across all parties. Capture follow-up actions after recovery. [3]

When hands are needed on site

Dispatch the agreed local resource for power, cabling, replacement or physical inspection. Locations, response windows and charges are contracted separately.

Coverage follows page 9 and starts after staffing and readiness acceptance.

07 / WHAT THE SERVICE CAN COVER

One operating view. *Across the critical estate.*

Build the service around business dependencies and supported integrations. Select the domains, assets and activities that matter to your organisation.

Networks & connectivity

WAN, firewall and switch health; link errors and capacity; configuration control; provider coordination.

Wireless & site services

Controller, access-point and authentication health; user-impact diagnosis; approved wireless changes.

Systems & virtualisation

Server and hypervisor health; capacity; operating services; patch coordination; controlled maintenance.

Cloud & identity

Approved cloud resources, access and directory services; sign-in dependencies; service health; expiry tracking.

Backup & recoverability

Backup-job monitoring, failure investigation and configuration backups; restoration testing and recovery evidence.

Security operations support

Security-tool health, policy work and certificate expiry; remediation coordination and customer security-team escalation.

Scope is explicit. End-user helpdesk, application development, a dedicated SOC, threat hunting, digital forensics and major transformation projects are optional or separately contracted—not implied by a NOC subscription.

08 / SLA & PERFORMANCE FRAMEWORK

A fast response. *A clearly defined commitment.*

Proposed flagship targets for qualification and contract agreement. A human acknowledgement, technical triage and service restoration are different milestones. [2]

PRIORITY & IMPACT	HUMAN RESPONSE	TRIAGE STARTS	PROGRESS UPDATES	COVERAGE
P1 **Critical** Major service outage.	**5 min**	**15 min**	Every 30 min	24/7
P2 **High** Degraded service.	**15 min**	**30 min**	Every 60 min	24/7
P3 **Normal** Limited impact.	**1 hour**	**4 hours**	Each business day	Agreed business hours
P4 **Request** Routine request.	**4 hours**	**1 day**	Agreed milestones	Agreed business hours

How the clock works

Response and triage targets run from the first valid in-scope alert received by the service or ticket receipt, whichever is earlier. P3/P4 hours and days mean agreed business time. An automated receipt is not a human response.

How restoration is agreed

Set service-specific recovery objectives after baselining access, architecture and dependencies. Display approval and third-party wait time separately; keep total elapsed time and customer updates visible.

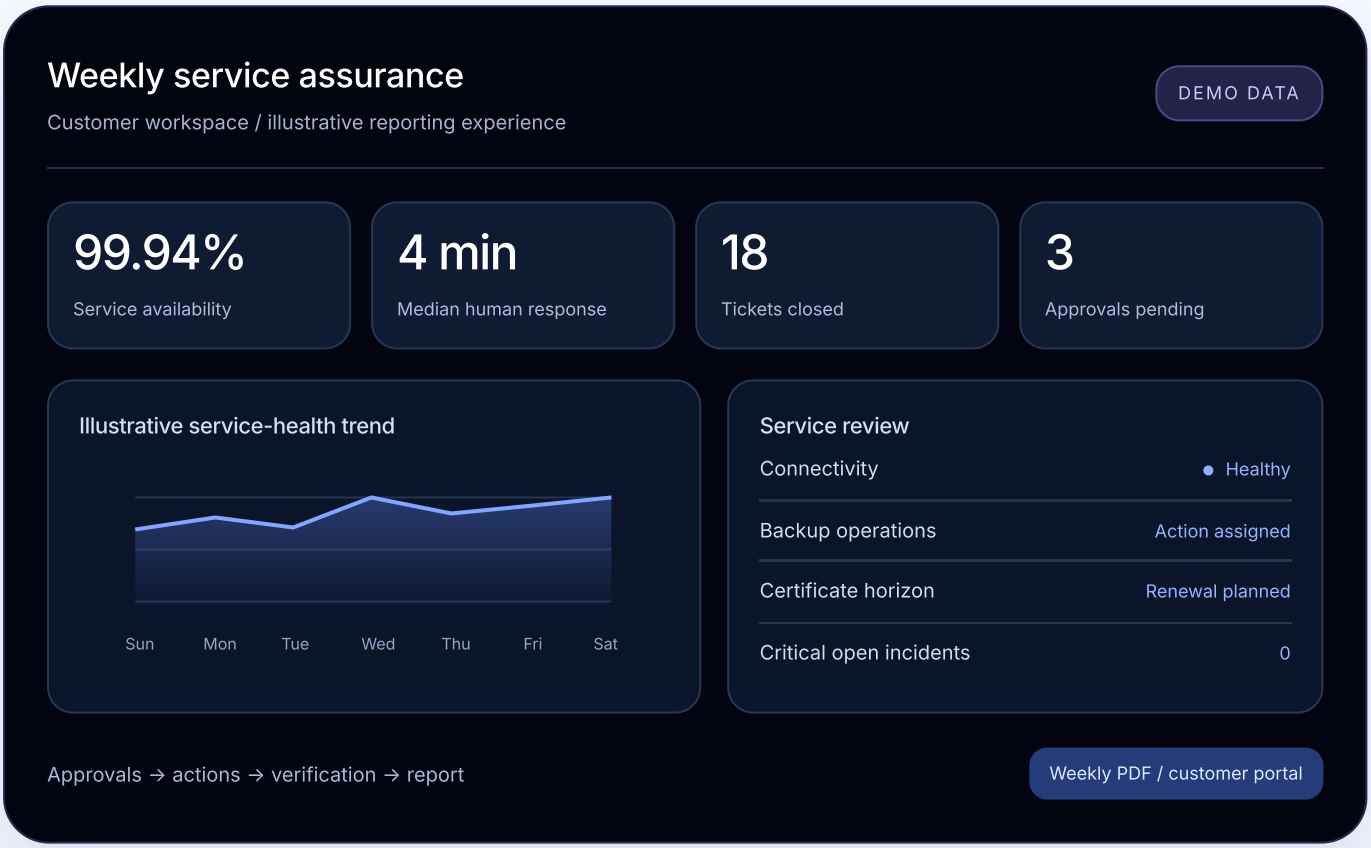
Measured monthly: report attainment and breaches by priority, with ticket counts, response and restoration distributions, and agreed exclusions. An isolated fast incident does not establish an SLA success rate.

Final coverage calendars, attainment thresholds, escalation rules, restoration objectives, exclusions and any service credits belong in the signed SLA. These are proposed targets, not published historical results or an infrastructure-uptime guarantee.

09 / THE CUSTOMER EXPERIENCE

See the work. *See what improves.*

A weekly service report connects operational activity to business impact, emerging risk and the next decisions needed from the customer.



Concept interface with synthetic values, not a live screenshot or a statement of achieved performance. Final platform capabilities and integrations are confirmed at onboarding.

Weekly operational view

Availability and downtime; open and closed tickets; WAN and wireless health; capacity and error trends; configuration backups; changes; pending approvals and named next actions.

Monthly management review

SLA attainment; repeated incidents and root causes; backlog ageing; risk and expiry exposure; improvement progress; actual service cost and measured effort released.

Not just a polished dashboard. Every metric carries a period, definition and evidence. Show median and tail response times, and flag monitoring gaps rather than counting missing data as healthy. [2]

10 / HOW ISSUES ARE HANDLED

Practical engineering. *Repeatable methods.*

Representative service scenarios show the approach—not customer case studies, identified environments or claims of measured results.

Restore connectivity with evidence

Check the business path from carrier to edge, routing and core. Separate a local configuration fault from an upstream outage. Execute only an approved recovery or failover plan.

> Proof: path tests, traffic verification, change record and carrier reference where applicable.

Resolve wireless issues beyond a reboot

Correlate controller, access point, uplink, authentication and addressing evidence. Confirm the affected user journey before selecting the authorised correction.

> Proof: successful client access, service reachability and post-change health checks.

Turn backups into recovery readiness

Investigate failed jobs, credentials, capacity and changed configurations. Restore the scheduled job and validate the required recovery test under the approved scope.

> Proof: successful job record, recoverable version and witnessed restoration-test outcome.

Reduce alert noise and prevent repeats

Tune thresholds against real capacity, map dependencies and investigate recurring failures. Track certificate or licence expiries and assign actions before deadlines.

> Proof: alert-test results, reviewed event trends and dated improvement actions.

Remote first, not remote at any cost. Physical faults, unsafe changes and unsupported conditions escalate to the right specialist or on-site resource.

11 / SECURITY BY SERVICE DESIGN

Access to support. *Not unrestricted access.*

Agree the data boundary, privileged-access model and permitted AI use before collecting production information. Zero-trust principles require explicit authorisation—not trust based only on location. [4]

01 / IDENTITY

Named, limited access

MFA, least privilege, time-bounded administration and customer-controlled approval. Separate monitoring credentials from change permissions.

02 / ISOLATION

Customer boundaries

Scope access, credentials, evidence and reports to the correct customer. Validate isolation before live service activation.

03 / DATA HANDLING

Minimum necessary data

Collect only agreed evidence. Where approved, tokenise identifiers locally and retain the mapping inside the customer boundary.

04 / AI GOVERNANCE

Approved processing only

Define permitted AI destinations, retention and no-training obligations in the service and processor agreements. Scope local-only processing where required.

A controlled action leaves a controlled record.

Record the requester, approver, approved plan, executing identity, timestamps, output and verification. Make privileged activity reviewable and retain records under the customer-approved policy.

Customer-aligned assurance

Map the applicable Saudi requirements, including NCA controls where in scope, to the deployment and evidence pack. Regulatory applicability and customer approval are assessed per engagement. [5]

Clear security boundaries

Masking reduces exposure; it does not make every finding safe to share. No blanket sovereignty, certification, zero-risk or “impossible to breach” claim is made by this brochure.

12 / A LEANER OPERATING MODEL

More capability. *Less fixed staffing cost.*

Shift repeatable operational work to shared specialists and approved automation, while retaining a capable internal owner. Reducing manual, repetitive work is a core reliability-engineering principle. [1]

80%

Lower dedicated staffing spend in the illustrative scenario below.

ILLUSTRATIVE STARTING MODEL

5 FTE

Dedicated internal roles

SAR 1.20m / year

Five full-time-equivalent roles at an assumed fully loaded SAR 240,000 per role annually.

→

ILLUSTRATIVE SHARED MODEL

1 FTE

Retained internal owner

SAR 240k / year

One equivalent role retained internally. Tawajud NOC capacity and other costs are added on the next page.

SAR 960k less dedicated payroll = (SAR 1.20m − SAR 240k) ÷ SAR 1.20m = 80%. This is a modelled staffing-cost difference—not an 80% reduction in total IT cost.

Assumptions are illustrative, not salary benchmarks, a staffing prescription or an achieved customer result. Feasibility depends on workload, service scope, risk, local support and equivalent coverage. Redeploying employees releases capacity; it creates cash savings only when expenditure is actually avoided or reduced.

13 / THE COMPLETE BUSINESS CASE

Show the full cost. *Then measure the value.*

The staffing example is only one part of the decision. Add the managed service, enabling costs and transition before discussing total savings.

ILLUSTRATIVE ANNUAL SCOPE / SAR	INTERNAL MODEL	SHARED MODEL
Dedicated / retained staffing	1,200,000	240,000
Managed NOC service allowance	—	240,000
Incremental tools, connectivity & on-site reserve	—	60,000
Recurring annual operating cost	**1,200,000**	**540,000**
One-time onboarding allowance	—	60,000
First-year cost	1,200,000	600,000

55%

Recurring annual saving

SAR 660,000 per year in this model after the listed recurring costs.

50%

First-year saving

SAR 600,000 after the illustrative onboarding allowance.

Measure operational efficiency

Track repeat-incident rate, manual minutes per comparable task, remote-resolution rate and change success. Use matched scope, volume and periods; do not count reopened tickets as durable success.

Validate commercial savings

Compare equivalent coverage and service levels. Separate released staff capacity from cash saved and avoided future hiring. Use actual invoices and approved staffing costs.

All amounts are hypothetical inputs, not a quotation. Unchanged costs are excluded from both models; dashes mean no incremental allowance, not zero actual cost. Add applicable taxes, transition overlap, redundancy and extra support. Savings depend on validated scope and actual costs.

14 / A CLEAR WORKING AGREEMENT

Keep responsibility clear. *Keep the service moving.*

A successful shared-service model needs both sides to know what they own, what they approve and what remains outside the subscription.

TAWAJUD AI

Own the delivery process

Operate the agreed monitoring and incident workflow. Maintain runbooks, manage specialist escalation, perform authorised remote work, verify outcomes and deliver scheduled service reporting.

THE CUSTOMER

Own business decisions

Nominate an approver and local contact. Provide access and readiness. Retain business priorities, risk acceptance, system ownership and decisions on expenditure or disruptive change.

Box ownership	The loaned NOC Box remains Tawajud AI property unless a signed agreement states otherwise. Record its asset identity and condition at handover.
End of service	Revoke service access, return or remove customer data under the agreed retention policy and return the Box within five working days of expiry or termination, unless continued retention is agreed in writing.
Licences & suppliers	Confirm which monitoring, security, connectivity and vendor-support entitlements are included. Customer-funded licences and renewals remain explicit rather than assumed.
On-site & extra scope	Define site locations, included visits, dispatch windows, consumables and replacement hardware. Migrations, redesigns, new implementations and substantial project work require separate scope.

Transparent commercial terms: agree included assets, locations, ticket and change entitlements, approved automation, support hours, reporting, retention, fees and exit support before service activation.

15 / START WITH A CONTROLLED PILOT

Prove the service. *Then expand with confidence.*

An illustrative 30-day onboarding and pilot plan, starting after customer readiness and access approval.

DAYS 1–5

Discover & agree

Map critical services, assets, dependencies, contacts, security requirements and the current cost and performance baseline.

Exit evidence: Approved scope, responsibility matrix and success measures.

DAYS 6–10

Connect & prove readiness

Install or provision the Box, validate restricted access, connect approved monitoring and test alert routing and customer approvals.

Exit evidence: Accepted access controls, test tickets and initial service map.

DAYS 11–20

Operate & refine

Run a controlled service period, validate selected low-risk runbooks and publish the first weekly reports. Review noise, gaps and escalation.

Exit evidence: Verified workflows, report delivery and documented corrective actions.

DAYS 21–30

Review & scale deliberately

Compare measured service performance and workload with the baseline. Confirm commercial scope, specialist capacity and the production SLA.

Exit evidence: Customer go-live decision and a prioritised improvement plan.

Go-live is an acceptance decision.

Require a witnessed alert-to-ticket test, a recorded approval, an authorised action with rollback readiness, successful verification, delivered reporting and a confirmed escalation rota.

Timing depends on access, integrations, approvals and change windows. Validate longer-term savings and reliability beyond the pilot.

16 / ASSURANCE & INTERPRETATION

Strong promises. *Clear boundaries.*

This capability brochure is a service-design and commercial discussion document. The signed agreement defines the delivered service.

Targets, not past results

All response and rapid-remediation times are proposed targets or labelled examples. Savings use stated planning assumptions; no audited customer result is claimed.

Scope, not automatic inclusion

Confirm platform release, integrations, runbooks, hosting, staffing, access and local support at onboarding. An illustration does not establish production availability.

No implied certification or endorsement. The references below inform the approach. They do not certify Tawajud AI, endorse this offering or substantiate its timing or cost assumptions.

SELECTED PRIMARY REFERENCES · REVIEWED 9 SEPTEMBER 2026

[1] **Google SRE · Eliminating Toil ↗**
Principle: reduce repetitive manual operations and invest in reusable engineering.

[2] **Google SRE · Service Level Objectives ↗**
Principle: distinguish metrics, performance objectives and contractual service levels.

[3] **NIST SP 800-61 Rev. 3 · April 2025 ↗**
Reference for incident preparation, response, recovery and continual improvement.

[4] **NIST SP 800-207 · Zero Trust Architecture ↗**
Reference for explicit authentication, authorisation and resource-focused access.

[5] **NCA · Essential Cybersecurity Controls 2:2024 ↗**
Saudi control reference for deployment-specific applicability and assurance mapping.

Definitions: NOC: Network Operations Centre. FTE: full-time equivalent. SLA: service-level agreement. MFA: multi-factor authentication. RCA: root-cause analysis.

Publication: TWJ-MS-NOC-2026-09
English capability edition · Version 1.0
Prepared by Eng. Ibrahim Modhish · Tawajud AI

MANAGED SERVICES / TAWAJUD AI

A leaner team. A stronger service. *A faster business.*

Keep your people focused on the business.
Give your operations a coordinated service behind them.

A local Box.
An accountable NOC.
Human-approved action.
Evidence you can see.

DISCOVER PROVE OPERATE IMPROVE

Eng. Ibrahim Modhish
Tawajud AI · Managed Services

Explore Tawajud AI ↗