



THE EXPERTISE YOU NEED. WITHOUT THE FULL INTERNAL OVERHEAD.

UP TO

80%

LOWER DEDICATED
NOC STAFFING COSTS*

Illustrative staffing-cost scenario.
Not a reduction in total IT expenditure.

More expertise.
Less overhead.

Level 3 senior engineers
for major systems,
networks and security.

Expert-led diagnosis.
Action with your approval.



NOC BOX · ILLUSTRATIVE PRODUCT CONCEPT



24/7

Monitoring & response



L3

Senior engineering expertise



Weekly

Reports & service visibility

Ticket → Diagnose → Approve → Fix → Verify → Report

*Actual savings depend on scope, the current operating model and service fees. Supported technologies, coverage and response targets are agreed in the service schedule.

tawajud.net

01 / EXECUTIVE OVERVIEW

A stronger operation. A more focused team.

Tawajud AI brings the customer-side NOC Box, senior engineering and the CloudMS service platform into one coordinated operating model.

01

A local service endpoint

The NOC Box connects approved assets to the service workflow, with local collection and controlled access.

02

A specialist team

A shared NOC owns incidents and brings senior specialists into deeper systems, network and security investigations.

03

A complete service record

Tickets, evidence, approvals and actions stay connected, so your team can see the owner, progress and next decision.

More time for your business.

Move repeatable operations to shared expertise. Keep business priorities, change approval and risk decisions with your organisation.

YOUR GUIDE TO THE SERVICE

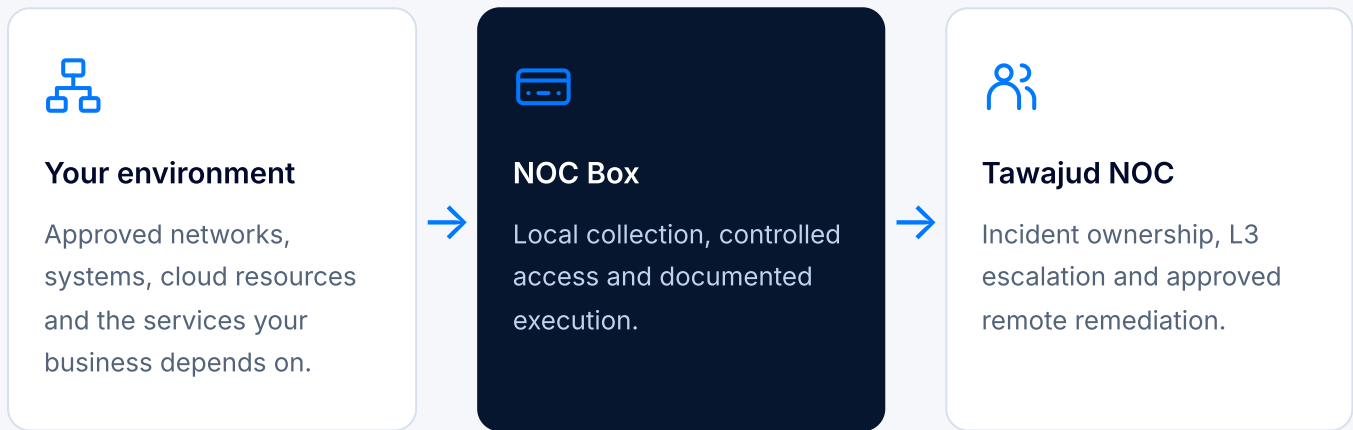
The Box and senior expertise	03-05
Workflow and service levels	06-08
Reports and continuous improvement	09-11
Data protection and business value	12-14
Responsibilities and onboarding	15-18

This is a service offering, not a statement of verified historical performance. The signed service schedule confirms supported platforms, integrations, staffing and coverage.

02 / SERVICE ARCHITECTURE

Local presence. Connected expertise.

The Box provides the local endpoint. The NOC brings the people and process. The platform makes the entire service visible.



CLOUDMS

One workspace. A complete view.

CloudMS connects the ticket, technical evidence, named owner, customer approval, execution and weekly report.

You approve the change

Disruptive or non-standard work requires approval. Routine work may follow a documented, pre-authorised procedure.

You define the data boundary

Agree what stays local, what may be shared and which AI processing routes are allowed. Local-only processing is scoped where required.

Production access starts only after connectivity, identities and data handling have been approved. The Box does not bypass your security controls.

03 / INSIDE THE NOC BOX

A compact device. A broader capability.

A managed service endpoint configured around your approved assets and access policies—not unrestricted remote access.



Monitor

Approved health checks, interface status, events and configuration snapshots where supported.

Control access

Named accounts, restricted management access and separate monitoring and change permissions.

Execute safely

Authorised diagnostics and tested recovery procedures against in-scope assets.

Document the result

Before-and-after checks, timestamps and the action record stay with the ticket.

Deployment needs protected power, an approved management-network connection, an asset list and a local contact. Agree alternative access or a second collector for critical locations.

Physical or approved virtual deployment is available by design. Local AI capacity is sized separately. The Box does not replace firewalls, high availability, backup or physical engineering.

04 / THE ENGINEERS BEHIND THE SERVICE

Senior expertise. An extension of your team.

Our NOC provides Level 3 senior engineering across major systems, network and security technologies, with coverage tailored to your supported environment.

L1

Monitor and coordinate

Receive, validate, communicate and escalate.

L2

Diagnose and restore

Investigate faults and execute approved procedures.

L3

Senior engineers

Lead complex investigations and review recovery plans.

SPECIALISTS ACROSS THE MAJOR TECHNOLOGY DOMAINS

Networks and wireless

Routing, switching, WAN, wireless controllers and access points.

Security platforms

Firewalls, endpoint protection, access control and security-tool health.

Servers and virtualisation

Operating systems, hypervisors, capacity and core services.

Cloud and identity

Approved cloud resources, directories and access services.

Storage and backup

Storage systems, backup jobs, configuration recovery and restore tests.

Data and business services

Supported databases, email and application-related services.

24/7 monitoring and critical response use an agreed duty and escalation rota. L3 engagement, supported products/versions, onsite attendance and vendor escalation are defined in the service schedule. A NOC is not a dedicated SOC or a replacement for vendor support.

05 / HOW WE WORK

One ticket. From first alert to verified recovery.

Prepared information, clear ownership and approved access make action faster without bypassing controls.

01	Detect or receive An approved monitor raises an event, or the customer submits a support ticket.	Time, source and service
02	Prioritise and diagnose The NOC confirms impact, correlates evidence and assigns a named owner. AI may assist the engineer.	Priority, owner and findings
03	Plan and approve Prepare the action, impact, pre-checks and rollback. Record approval or a valid standard-change authority.	Approved scope and plan
04	Execute within scope A qualified engineer or authorised automation performs the approved procedure.	Identity, action and timing
05	Verify service recovery Re-test the affected service. Failed checks trigger rollback or escalation.	Service tests and outcome
06	Close and improve Confirm closure under the agreed policy, preserve the record and assign follow-up actions.	Closure evidence and next actions

Approval is part of the workflow, not an afterthought. Standard work can use documented pre-authorisation; disruptive, exceptional and emergency work follows the customer's agreed authority.



06 / SPEED WITH CONTROL

From approval to action. Minutes, where the work allows.

Prepare access, agree authority and test recovery procedures before the next incident.

ILLUSTRATIVE WORKFLOW · NOT A RECORDED INCIDENT

5–15

Minutes for execution and verification

Proposed target after approval, for validated low-risk procedures, with working remote access and no external dependency.

00:00

Ticket received

An approved monitor detects a recoverable fault.

02:00

NOC owner engaged

The engineer confirms the affected service and impact.

03:00

Procedure selected

Evidence matches a validated low-risk procedure.

05:00

Approval recorded

The authorised approver confirms the plan.

08:00

Remediation complete

The approved steps complete and are recorded.

10:00

Recovery verified

Service checks pass and the outcome is documented.

Fast does not mean uncontrolled. Access, permissions, rollback and service checks are prepared before the change.

This ten-minute example is not a promise to fix every incident in ten minutes. Hardware failures, carrier outages, complex investigations and delayed approvals require separate recovery plans.

07 / SERVICE LEVELS

Fast response. Clear commitments.

Human acknowledgement, technical triage and service recovery are different milestones. Each needs a clear definition and a measurable target.

PROPOSED SERVICE TARGETS · SUBJECT TO AGREEMENT

Priority / impact	Human response	Triage starts	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	Business hours
P4 / Request Routine service request	4 hours	1 business day	Agreed milestones	Business hours

When measurement starts

From the first valid in-scope alert received by the service, or ticket receipt, whichever is earlier. P3/P4 use agreed business time. An automated receipt is not a human response.

How recovery is agreed

Recovery depends on architecture, access and external parties. Approval and supplier wait times are shown separately, while total elapsed time remains visible.

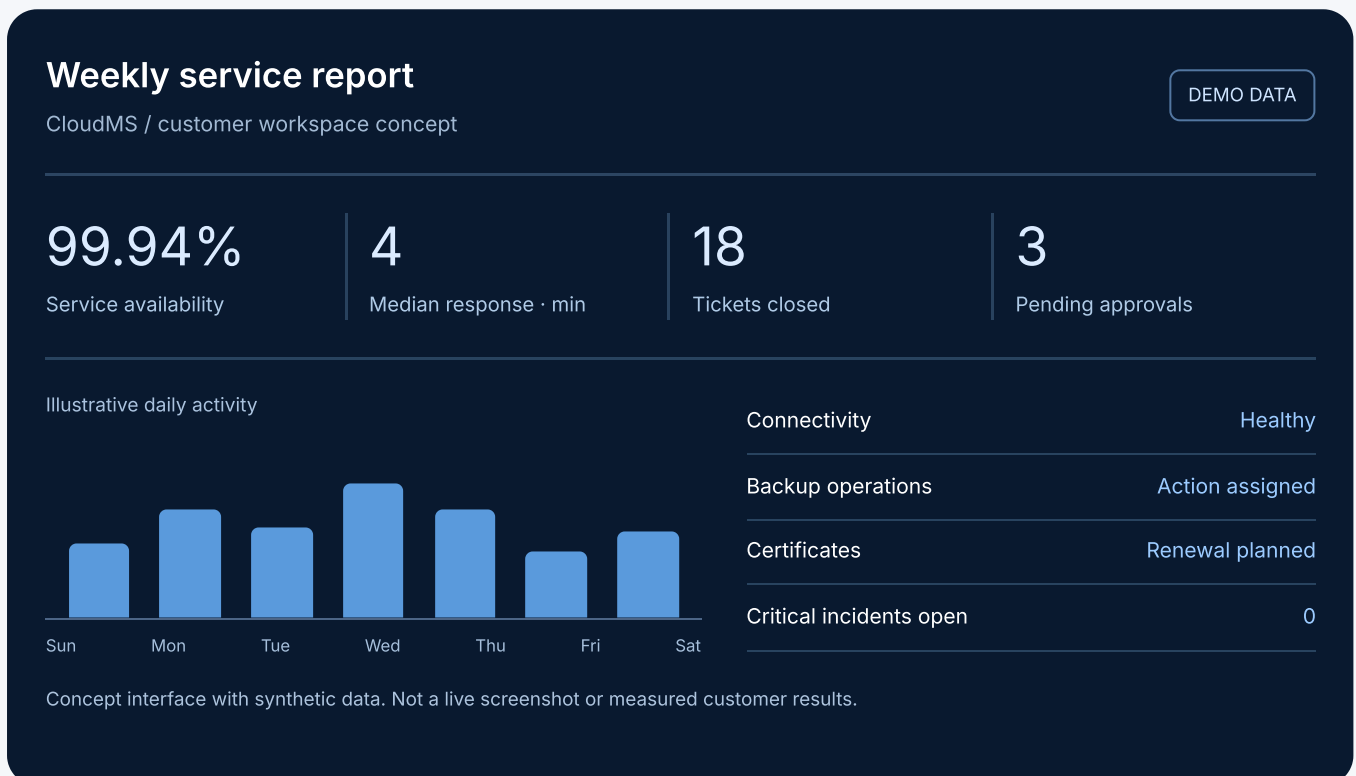
Report monthly attainment by priority, including ticket counts, breaches, response-time distributions and service recovery. A single fast incident is not an SLA success rate.

The signed SLA defines coverage calendars, attainment thresholds, escalation, service-specific recovery targets, exclusions and any credits. These are proposed targets, not achieved results or an infrastructure-uptime guarantee.

08 / WEEKLY PLATFORM REPORTING

See the work. Understand the progress.

A shared customer view connects technical activity to business impact, open actions and the next decision.



Every week: operational clarity

Availability and downtime, ticket status, WAN and wireless health, capacity, configuration backups, approved changes and pending decisions.

Every month: management insight

SLA attainment, recurring causes, ageing tickets, risk and expiry exposure, improvement progress and validated cost or effort saved.

Every metric has a defined period and evidence. Monitoring gaps remain visible; missing data is not counted as a healthy service.

Platform release capabilities, integrations and scheduled reporting are confirmed during onboarding. Each report links actions to a named owner and next review date.

09 / OPERATIONAL PLAYBOOKS

Engineering depth. Repeatable recovery.

Investigate the complete service path, not only the first device that raised an alarm.



Restore connectivity with evidence

Trace the carrier, firewall, routing and core path. Separate local faults from external outages, then apply an approved recovery or failover plan.

Evidence: path tests, traffic checks and the approved change record.



Resolve wireless issues beyond a reboot

Correlate controller, access point, uplink, authentication and addressing information before selecting the correction.

Evidence: successful user access and post-change service checks.



Recover systems and connected services

Check server health, identity, service state, capacity and cloud-side dependencies. Escalate unsupported conditions to the right specialist.

Evidence: health readings, approved actions and service-recovery tests.



Make backups usable for recovery

Investigate failed backup jobs, access and capacity. Restore the schedule and perform the agreed restoration test.

Evidence: successful backup, recoverable version and documented test.

Remote first, not remote at any cost. Physical faults, unsafe changes and unsupported conditions move to the right specialist, supplier or onsite engineer.

Representative service scenarios, not customer case studies or claims of achieved recovery times.

10 / CONTINUOUS IMPROVEMENT

Fix today. Reduce tomorrow's workload.

Closing tickets is only the start. Use operational lessons to reduce repeat work and strengthen the service.

Reduce alert noise

Tune thresholds to real capacity, map related assets, remove invalid monitors and correlate duplicate events before escalation.

Reduce repeat incidents

Link recurring tickets to a problem record, assign root-cause actions and track certificate and licence renewals before deadlines.

PEOPLE + AI + ENGINEERING

Automate the routine. Keep judgement with experts.

AI can summarise evidence, explain unusual signals and suggest next checks. Engineers validate the diagnosis, while customer authority governs execution. Reusable procedures reduce repetition without giving the model independent administrative power.

MEASURE THE IMPROVEMENT

Task efficiency

Manual minutes for equivalent tasks and workloads.

Durable resolution

Repeat incidents, reopened tickets and lasting recovery.

Change quality

Verified success, failed checks and rollback events.

Time returned to your team

Staff effort redeployed, separate from cash savings.

11 / CUSTOMER CONTROL AND DATA

Access for support. Not unrestricted access.

Agree the data boundary, privileged-access model and permitted AI use before collecting production information.

Named and limited access

MFA, least privilege, time-limited administration and separate monitoring and change credentials.

Customer data separation

Separate access, credentials, evidence and reports for each customer. Validate isolation before live activation.

Minimum necessary information

Collect only agreed diagnostic information. Exclude secrets and protect records, logs and backups.

Approved AI processing

Agree processing destinations, retention and no-training/no-secondary-use obligations. Scope local-only operation when required.

OPTIONAL CUSTOMER-SIDE TOKENISATION

Real identifiers remain under your control.

192.168.1.20



IP_A7F2

Keep the mapping inside the approved customer environment. Restore identifiers only for authorised workflows.

Masking is an additional safeguard, not permission to share. Hiding an address does not make a vulnerability or network design safe to disclose.

Deployment controls, applicable requirements, hosting, processor terms and evidence are agreed and verified for each engagement. No certification, blanket compliance or immunity from compromise is implied.

12 / A LEANER STAFFING MODEL

More capability. Less fixed internal overhead.

Use shared specialist capacity while retaining a capable internal owner for priorities, approvals and service oversight.

80%

Lower dedicated staffing spend

An illustrative staffing scenario—not an 80% reduction in total IT cost.

5

Dedicated internal roles

Five full-time-equivalent roles at an assumed fully loaded annual cost of SAR 240,000 each.

1,200,000

SAR per year

1

Retained internal service owner

One full-time-equivalent role retained internally, supported by the shared NOC. Service fees are added on the next page.

240,000

SAR per year

$$(1,200,000 - 240,000) \div 1,200,000 = 80\%$$

SAR 960,000 less dedicated internal payroll in this example. Managed-service fees, enabling costs and onboarding must be added before calculating total savings.

Hypothetical inputs, not salary benchmarks, staffing advice or achieved customer results. Equivalent scope, coverage, workload and risk must be validated. Redeploying employees releases capacity; cash savings require spending to be reduced or avoided.

13 / THE COMPLETE BUSINESS CASE

Start with the full cost. Then calculate the saving.

Staffing is one part of the equation. Add managed-service fees, enabling costs and transition before discussing total savings.

ILLUSTRATIVE INPUTS · SAR · NOT A QUOTATION

Annual cost item	Internal model	Shared model
Dedicated / retained staffing	1,200,000	240,000
Managed NOC service allowance	—	240,000
Tools, connectivity and onsite 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 after the listed recurring costs.

50%

First-year saving

SAR 600,000 after the illustrative onboarding allowance.

Compare equivalent scope, coverage and service levels. Separate cash savings from redeployed staff time and avoided future hiring. Use actual costs to validate the final business case.

All values are planning assumptions, not pricing commitments. Unchanged costs are excluded from both models; a dash means no incremental allowance, not zero actual cost. Add applicable taxes, transition overlap, resilience and extra support. Actual savings depend on scope and cost validation.

14 / RESPONSIBILITIES AND SCOPE

Clear ownership. Better collaboration.

A shared model works when both sides understand their responsibilities, approval rights and the boundaries of the subscription.

Tawajud AI delivers the service

Operate agreed monitoring and tickets, maintain procedures, coordinate senior and vendor escalation, perform approved work, verify recovery and deliver reports.

You retain business authority

Nominate an approver and local contact. Provide access and readiness. Retain ownership, business priorities, risk acceptance and spending decisions.

Box ownership

The loaned Box remains Tawajud AI property unless agreed otherwise. Record its asset identity and condition at handover.

End of service

Revoke service access and handle data under the agreed retention and exit policy. Return the Box within five working days of expiry or termination unless continued use is agreed in writing.

Licences and vendors

Specify included monitoring, security, connectivity and vendor-support entitlements. Identify customer-funded licences and renewals.

Onsite and extra scope

Agree locations, visits, dispatch times and replacement responsibilities. Migrations, new implementations and major projects require separate scope.

End-user helpdesk, a dedicated SOC, threat hunting, digital forensics, application development and major transformation are not automatically included. The signed agreement governs commercial terms, ownership and return obligations.

15 / A CONTROLLED START

Prove the service. Then expand with confidence.

A defined pilot creates a shared baseline and a practical route to operational acceptance.

DAYS

1–5

Discover and agree

Map critical services, assets, related systems, contacts, security needs and current cost and performance.

Acceptance: Approved scope, responsibilities and success measures.

DAYS

6–10

Connect and validate readiness

Deploy the Box, validate restricted access, connect approved monitoring and test alert routing and approvals.

Acceptance: Accepted access controls, test tickets and an initial service map.

DAYS

11–20

Operate and refine

Run the controlled service, validate low-risk procedures, publish weekly reports and review noise and escalation.

Acceptance: Verified workflows, delivered reports and corrective actions.

DAYS

21–30

Review and scale

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

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

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

Illustrative 30-day plan begins after readiness and access approval. Timing depends on integrations, approvals and change windows. Long-term savings and reliability need measurement beyond the pilot.

16 / SERVICE READINESS

Strong capability. A clear working agreement.

Before activation, align the customer, NOC, engineers and service owner around one approved service schedule.

**Supported environment**

Named assets, locations, products and versions, cloud resources, integrations and connected services.

**People and coverage**

Duty team, L3 escalation, approver contacts, on-call arrangements and onsite support.

**Service commitments**

Priority definitions, working calendars, response measurement, recovery objectives, escalation and any credits.

**Control and evidence**

Data boundary, AI routes, privileged access, retention, approvals, rollback and reporting tests.

**Commercial clarity**

Fees, inclusions, licences, ticket and change entitlements, transition support and Box return terms.

Targets, not past results

Response times and rapid-remediation examples are proposed targets. Financial figures use explicit planning assumptions.

Scope, not automatic inclusion

Confirm the platform release, integrations, procedures, staffing, hosting and local support before production activation.

This capability brochure is not the SLA or a quotation. The signed agreement defines the delivered service. TWJ-MS-NOC-2026-09 · Refined edition 3.0.



TAWAJUD AI / MANAGED SERVICES

A more focused team. A stronger operation.

Put senior engineering, accountable response and visible reporting behind your operations—without building every capability internally.



Discover

Your environment and business priorities.

Prove

A controlled pilot and measurable value.

Operate

A service that learns from every outcome.

Build your operations advantage.

Discuss your scope and the right pilot.

tawajud.net ↗

Prepared by Eng. Ibrahim Modhish · Tawajud AI