SERVICE SPECIFICATION / MANAGED OPERATIONS

Network operations and monitoring

GHT-SVC-033 • Revision 1.0 • 06 September 2026 • 1 / 3

Covered assets and services connect to health checks, telemetry, thresholds, tickets, escalation, authorized actions, change records, and review.

Intended outcome

A monitored asset and service inventory with tuned alerts, tested ticket and escalation routing, current contacts, exclusions, and an operating runbook.

Service scope

A monitoring platform can observe availability, latency, interface state, capacity, power, temperature, wireless, security, configuration, logs, and application or service checks. Useful monitoring begins with an accurate asset and service map so a device alert can be interpreted in operational context.

Monitoring is not the same as remediation or continuous staffing. Covered hours, telemetry, retention, alert severity, acknowledgement, escalation, response target, remote action, dispatch, third-party coordination, and exclusions must be defined by contract.

How the system fits together

01 Assets and services	Devices, sites, links, power, wireless, dependencies, owners and criticality
02 Telemetry	Health checks, metrics, events, logs, configurations, timestamps and data quality
03 Decision	Baseline, threshold, persistence, correlation, severity, suppression and maintenance mode
04 Action and evidence	Ticket, acknowledgement, escalation, authorized change, dispatch handoff, review and audit

Typical project triggers

- Users report outages before the infrastructure team sees them
- Alerts are noisy, duplicated, stale, or not tied to a service owner
- Device inventory, support status, topology, or escalation contacts are incomplete
- No one reviews recurring incidents, capacity, configuration drift, or unresolved risk

Delivery and acceptance

The final project scope identifies quantities, locations, dependencies, and the evidence required at each delivery stage.

01 Establish monitored truth

Inventory covered assets, services, owners, dependencies, sites, versions, support status, telemetry sources, access, time, contacts, and existing incident history.

Acceptance evidence: Contract-scoped asset and service inventory, dependency map, access record, baseline, coverage window, and contact matrix.

02 Design signal and response

Define checks, collection intervals, thresholds, persistence, suppression, dependencies, severity, ticket routing, acknowledgement, escalation, authorized actions, and retention.

Acceptance evidence: Monitoring and alert catalog, severity and escalation matrix, response targets as contracted, dashboard plan, and exclusion list.

03 Onboard and tune

Configure supported collection, protect credentials, normalize names and time, establish dashboards and tickets, simulate events, and tune noise against observed baselines.

Acceptance evidence: Monitored-asset readback, credential-owner record without secret values, test alerts and tickets, baseline report, and tuned exceptions.

04 Operate and improve

Handle events within the contracted coverage and authority, preserve notes and changes, review false and missed alerts, track recurring conditions, and update the monitored inventory.

Acceptance evidence: Sample alert-to-ticket timeline, acknowledgement and escalation evidence, change record, recurring-issue review, and updated asset coverage report.

Handover deliverables

- Contract-scoped asset, service, owner, and dependency inventory
- Monitoring, alert, severity, escalation, action, and exclusion catalog
- Dashboard, ticket, notification, maintenance, and retention configuration record
- Test alert-to-ticket-to-escalation evidence
- Baseline and recurring-issue reports, coverage readback, and operating runbook

Closeout: GHT and the customer review the agreed evidence, record unresolved exceptions and owners, and confirm acceptance against the signed project scope.

Planning and scope boundaries

Revision 1.0 • 06 September 2026 • 3 / 3

Customer and site inputs

- Covered sites, assets, services, dependencies, criticality, owners, and support state
- Telemetry sources, access method, polling or event intervals, time, retention, and data location
- Baseline, threshold, persistence, severity, maintenance windows, and suppression rules
- Contracted coverage window, channels, response targets, escalation, authority, and exclusions
- Ticketing, remote action, vendor handoff, dispatch boundary, reporting, review, and change process

Constraints and coordination

- Monitoring cannot guarantee availability, detect every fault, or repair a condition outside granted access, authority, support, or service scope
- Coverage windows, response targets, escalation, remote actions, vendor coordination, and dispatch are contract-specific; they must not be implied
- Encrypted, proprietary, legacy, or unsupported systems may expose limited telemetry or control
- Thresholds require tuning, asset inventories require maintenance, and maintenance windows must suppress expected changes without hiding real faults

Commercial scope and responsibilities

This specification describes the service framework. The signed statement of work defines included equipment, quantities, software licenses, integrations, access windows, schedule, pricing, warranty, and support coverage. Additional construction, electrical work, recurring subscriptions, and ongoing support require an explicit line item.

The customer appoints an acceptance owner and provides authorized access, required site information, and decisions. GHT records assumptions, coordinates assigned work, and submits changes for agreement before expanding the scope.

Technical references

National Institute of Standards and Technology — SP 800-137: Information Security Continuous Monitoring | Source review: 2026-08-20

National Institute of Standards and Technology — Cybersecurity Framework 2.0 | Source review: 2026-08-20

Cybersecurity and Infrastructure Security Agency — Cross-Sector Cybersecurity Performance Goals | Source review: 2026-08-20

Service guide and project discussion | Source review: 2026-09-06