

Alert priority and customer onboarding

Proposed discussion aid | As of 2026-10-02 | Not a signed service schedule

All targets are proposed for discussion. No live response coverage is established here. A target applies only after selection in a signed service schedule, validated staffing and commissioned routing.

Critical / P1

PROPOSED TARGET: 15 elapsed minutes

Trigger:	An agreed critical service is unavailable, or an authorized security owner identifies an active incident with immediate material impact.
Clock:	Only inside the explicitly contracted staffed coverage window; 24/7 requires commissioned staffing.
First action:	Human acknowledgment, impact check and initial triage; emergency changes only under explicit authority.
Escalation:	Primary operator and customer incident authority immediately; backup owner at the missed-target threshold.

High / P2

PROPOSED TARGET: 60 elapsed minutes

Trigger:	A major degradation affects an important service or multiple users, with limited workaround; a security finding needs urgent owner review.
Clock:	Inside the contracted staffed coverage window.
First action:	Acknowledge, confirm the affected boundary and agree the next action.
Escalation:	Assigned operator and service owner; backup owner if the acknowledgment target is missed.

Proposed alert priorities | P3-P5

Use agreed impact, urgency, service criticality and staffed calendars to assign the operational priority.

A vulnerability severity or scan label does not by itself assign an operational alert priority. Define promotion and downgrade authority in the signed schedule.

Medium / P3

PROPOSED TARGET: 4 business hours

Trigger:	Limited service degradation, a bounded control gap or a user-impacting issue with a viable workaround.
Clock:	Published business-hours calendar and customer time zone.
First action:	Acknowledge, classify, assign an owner and schedule investigation.
Escalation:	Assigned queue; service owner if impact grows or the target is missed.

Low / P4

PROPOSED TARGET: 1 business day

Trigger:	Minor defect, nonurgent maintenance request or improvement with minimal present business impact.
Clock:	Published business-hours calendar; holiday rules defined in the schedule.
First action:	Acknowledge and agree an owner, priority and planned work date.
Escalation:	Assigned queue; include missed or aging work in the operating review.

Informational / P5

PROPOSED TARGET: Review within 5 business days

Trigger:	Expected event or advisory with no current required incident action; retain it for context, trends or evidence.
Clock:	Scheduled review cadence; no incident-response promise.
First action:	Retain or summarize according to policy; do not create an unowned incident for every event.
Escalation:	Escalate only when correlated context changes impact or the agreed rule requires it.

Clock definitions and operating guardrails

Proposed process language for review and service-schedule selection.

Vulnerability severity and CVSS are assessment evidence; operational alert priority also considers business impact, urgency and service criticality. A scan finding is not automatically a Critical incident.

Acknowledgment is a human ownership and initial triage step. It is not restoration or resolution. Emergency changes require explicit authority.

Proposed policy rules

- All targets are proposed for discussion. The signed service schedule selects the priority rules, supported assets, calendar, authorized actions and validated capacity.
- Acknowledgment means a human records ownership and begins the agreed impact/triage check. An automated alert receipt or ticket creation does not count. Acknowledgment is not restoration or resolution.
- Clock starts when a qualifying alert/ticket reaches the designated monitored queue during coverage. Measure detection and ingestion delay separately; retain event, ingestion, queue, acknowledgment and action timestamps.
- For elapsed targets outside coverage, route according to the agreed out-of-hours procedure; no staffed response is implied. Business-hour targets accumulate only within the agreed time-zone and holiday calendar.
- Do not pause an acknowledgment clock because work is awaiting the customer. Track customer/supplier wait separately for investigation and resolution. Priority reassignment requires reason, approver and original timestamp.
- Define update frequency, escalation channels and backup responders per severity in the signed schedule. Do not invent a universal restoration target without dependencies, authority and recovery evidence.
- Maintenance suppression requires an owner, assets, reason, start and expiry. Preserve suppressed-event evidence where required; test expiry and exceptions. Deduplication links related events to one accountable incident.
- Test clock boundaries, duplicate alerts, disconnected collectors, holiday/weekend arrival, primary-owner absence, escalation and unresolved shift handoff before coverage starts.

Customer onboarding and commissioning

Eight-step proposed path from scoping through steady operation and exit.

1. Select the service and assign owners

Customer names sponsor, technical owner and backup; completes Core plus the relevant worksheets using approved private records.

2. Reconcile inventory and unknowns

L8DT compares counts with the approved inventory, logs unresolved scope and identifies evidence needed. Unknown requirements cannot silently become zero-cost assumptions.

3. Confirm authorization and data handling

Validate owner/third-party permission, methods, support personnel and data boundary. Active testing and restricted access need their actual approvals.

4. Produce the scoped assessment or proposal

Define objectives, sampled assets, methods, outputs, operating units, full price lines, exclusions, priority clocks, capacity and acceptance. Owner approves the final scope.

Customer onboarding and commissioning

Eight-step proposed path from scoping through steady operation and exit.

5. Provision through the approved route

Customer or authorized operator creates only the agreed access; record role, expiry, custody and removal. Worksheets never request passwords or private keys.

6. Pilot and rehearse

Exercise the selected workflow, negative cases, collector failure, routing, primary/backup escalation, recovery and rollback within the authorized window.

7. Accept the service and start coverage

Customer approves commissioning evidence and unresolved exceptions. Confirm actual staffing and contact reachability before any target clock or 24/7 coverage starts.

8. Operate, review and exit predictably

Run the agreed review cadence, record incidents/changes/evidence and adjust scope with approval. Handoff/export and revoke access through the termination checklist.

Coverage starts only after customer acceptance of commissioning evidence and confirmation of actual staffing and contact reachability. No 24/7 capacity or target is implied by this worksheet.