Available on the Marketplace

GETINT

SLA Integration Checklist

A PRACTICAL GUIDE

Introduction

SLA in integrated environments isn't just a timer.
It's a decision system based on status, priority, and timing signals across multiple tools.

When integrations are misaligned, SLA doesn't fail loudly – it silently becomes inaccurate.

→ This checklist helps you ensure your SLA is reliable before going live.

1. Define How SLA Is Interpreted Across Systems

SLA is usually configured separately in each system – but **it depends on the same inputs.**

- [ ] SLA definitions exist in each system where they are needed
- [x] You understand what drives SLA in each tool (status, priority, timestamps)
- [ ] The same real-world event (e.g., status change) leads to consistent SLA behavior
- [ ] Teams agree on how SLA should behave across systems – even if configured separately

Key insight: SLA is not synchronized directly – it is driven by synchronized data

2. Align Status Logic

SLA doesn't run on labels. It runs on **status behavior.**

- [ ] You defined which statuses:
  - run the SLA
  - pause the SLA
  - stop/resolve the SLA
- [ ] Statuses are mapped by meaning, not by name
- [ ] One-to-many mappings are handled intentionally (e.g., Jira → ServiceNow)
- [ ] Edge cases are covered (reopen, waiting, escalated)

Example: "Waiting for customer" should pause SLA — if one system pauses and the other doesn't → SLA becomes wrong

3. Validate Data That Impacts SLA

SLA accuracy depends on more than status.

- [ ] Priority levels are consistent across systems
- [ ] Ticket type / category doesn't change SLA unexpectedly
- [ ] Time-related fields (created, updated) are synchronized correctly
- [ ] No field overwrites SLA-critical data unintentionally
- [ ] **Include custom fields and user mapping** (e.g., Jira usernames vs. ServiceNow IDs) – supported out of the box in Getint.

Note: Getint ensures consistent value mapping (including custom priorities), so SLA calculations remain accurate across systems.

4. Security and SLA Integrity

When systems exchange data, access and control directly impact how SLA behaves.

- [ ] SLA-related data is only accessible to authorized users
- [ ] Permissions don't block or delay SLA-critical updates
- [ ] Integration uses secure authentication (API tokens, OAuth 2.0)
- [ ] Verify compliance: ISO 27001, ISO 27018, SOC 2 Type II, GDPR
- [ ] Service accounts are used instead of personal user accounts

Prepare dedicated service accounts:
Always set up accounts used only for the integration.
If you're connecting with another company, ask them to create one for you.

5. Align Escalation Logic End-to-End

Escalation is where SLA becomes visible — and where inconsistencies hurt the most.

- [ ] Ensure escalation triggers are aligned with SLA conditions across systems
- [ ] Escalation timing (e.g., breach thresholds) is aligned across tools
- [ ] Ownership changes (assignee, team) sync correctly during escalation
- [ ] Notifications and alerts are triggered once — not duplicated or missing
- [ ] Escalation does not depend on fields that are not synchronized

6. Test SLA Behavior (Not Just Sync)

Most teams test if data moves — not if SLA works.

- [ ] You test full SLA scenarios:
  - ticket creation
  - status transitions
  - “waiting” states
  - escalation triggers
  - resolution
- [ ] SLA timers behave consistently across systems
- [ ] You validate time calculations, not just field updates
- [ ] Edge cases are tested (reopen, reassignment, delayed updates)
- [x] Test cases reflect real workflows — not ideal scenarios

Note: Getint helps you verify how SLA-related updates (status, priority, ownership) sync across systems, so you can confirm behavior before going live.

7. Monitor & Detect SLA Risks

SLA performance needs ongoing visibility to remain reliable over time.

- [ ] You can detect sync failures affecting SLA-critical data
- [ ] Alerts exist for delays or errors in synchronization
- [ ] Logs or audit trails are accessible and understandable
- [ ] Leverage Getint’s SLA-backed support – our customers can escalate sync issues directly if needed.

Available on the Marketplace

GETINT

SLA Integration Checklist

A PRACTICAL GUIDE

Why Getint?

SLA performance is only as reliable as the integration behind it.

With Getint, the focus is on keeping **SLA data** accurate, consistent, and trustworthy across systems from day one.

Setup is fast thanks to a **no-code approach**, but when your workflows demand more, **advanced scripting** supports even the most complex SLA logic — including status behavior, field dependencies, and edge cases.

Security is built into the foundation — Getint is **ISO, SOC 2 Type II, and GDPR compliant** — so your SLA data remains protected whether you run in the Cloud, on Data Center, or fully on-premise.

The elements that most often impact SLA accuracy — **status mapping, priority alignment, and custom field synchronization** — are handled out of the box, ensuring that SLA timers reflect real work, not mismatched data.

And when reliability matters most, our dedicated team is there with **SLA-backed support**, helping you maintain stable integrations when your service performance depends on it.