ILLUSTRATIVE SAMPLE / FICTIONAL CRM WORKFLOW

Readiness at a glance.

A bounded review of a sales assistant that reads customer records and proposes CRM updates.

ORGANIZATION [redacted]

SYSTEM / IDENTITY [redacted]

Identifiers withheld for demonstration. This is an invented scenario, not a redacted client engagement. Example date: November 1, 2026.

THE DECISION

Resolve the approval gap before enabling write access in this example. Sensitive customer fields, broad CRM writes, and approval that is not enforced together create the first risk path to address.

Permissions	**1 / 3**	■ □ □	Defined
Data Access	**1 / 3**	■ □ □	Defined
Oversight	**1 / 3**	■ □ □	Defined
Evidence	**2 / 3**	■ ■ □	Verified
Response	**0 / 3**	□ □ □	Absent

Levels: 0 confirmed absent; 1 defined; 2 verified; 3 exercised. Unknown = insufficient evidence. Not assessed = out of scope. There is no aggregate pass/fail score or certification.

ILLUSTRATIVE SAMPLE / FICTIONAL CRM WORKFLOW

Connect the risk path.

F-01 / Approval is visible in the interface, but is not bound to the exact action at execution.

PRIORITY **Address before write enablement**

ILLUSTRATIVE PATH

Customer fields available to the agent

CRM tool identity can write broadly

Executor accepts a changed action after approval

WHY THIS MATTERS

In this example, a reviewer approves a harmless update. The execution payload can then change without another authorization check. The combination of reachable data and write access increases the consequence of that gap. This is a fictional observation, not an exploit claim about a real product.

EVIDENCE REGISTER / SIMULATED RECORDS

E-01: tool manifest and permission-policy export.
E-02: data-path map showing customer contact fields.
E-03: synthetic test trace where a changed payload is accepted.
E-04: sample runbook with no named revocation owner.

Limits: no production testing, no client records, and no claim of exhaustive coverage. Real findings link to dated observations, authorized checks, and explicit scope limitations.

ILLUSTRATIVE SAMPLE / FICTIONAL CRM WORKFLOW

Fix. Verify. Keep evidence.

Owners and effort below are illustrative planning entries. Confirm them with the team before implementation.

01 / Restrict the scope

Platform owner | Estimate: small

Use a task-specific identity and expose only required operations. Check an allowed read and an out-of-scope write.

02 / Bind approval to the action

Application owner | Estimate: medium

Bind approval to the identity, operation, target, and payload. Deny missing, expired, replayed, or changed approvals at execution.

03 / Exercise revocation

Security + operations | Estimate: small

Name the responder. In an authorized test environment, revoke access and record denied execution and controlled recovery.

HANDOVER / ACCEPTANCE

Keep the inventory, agreed checks, trace references, observed results, unresolved gaps, and owner sign-off. Reassess after material changes to tools, identity, or data paths. A report is evidence for review, not a guarantee of security or compliance.