

# Agent Permission Readiness Scorecard

Kompakte Checkliste fuer Tool-Rechte, Approval Policy, Audit und Rollback vor produktiven AI-Agenten.

Tirion Agent Permission Model

Score max: 36

Updated: 2026-07-01

AUSWERTUNG

30 bis 36 Punkte

Production-ready fuer definierten Scope.

23 bis 29 Punkte

Pilot-ready mit kontrollierten Aktionen.

16 bis 22 Punkte

Nur Demo oder Read-only.

0 bis 15 Punkte

Nicht einsetzen.

BEWERTUNGSDIMENSIONEN

| Dimension                | Leitfrage                                                         | Score |
|--------------------------|-------------------------------------------------------------------|-------|
| Purpose Bound            | Ist der Agentenzweck eindeutig und eng genug?                     | 0-3   |
| Identity                 | Ist klar, welche User-, Service- und Business-Identitaet handelt? | 0-3   |
| Tool Inventory           | Sind alle Tools mit Owner, Zweck und Side Effects dokumentiert?   | 0-3   |
| Scope Minimality         | Sind API-/Graph-/OAuth-Scopes minimal und begruendet?             | 0-3   |
| Data Boundary            | Sind Datenklassen, Mandantengrenzen und Sensitivitaet definiert?  | 0-3   |
| Action Tiering           | Ist jede Aktion P0 bis P5 zugeordnet?                             | 0-3   |
| Human Approval           | Passt die Freigabe zur Wirkung der Aktion?                        | 0-3   |
| Prompt Injection Defense | Werden untrusted Inhalte von Instruktionen getrennt?              | 0-3   |
| Tool Guardrails          | Gibt es Validierung vor und nach Tool-Ausfuehrung?                | 0-3   |

|                     |                                                                    |            |
|---------------------|--------------------------------------------------------------------|------------|
| <b>Auditability</b> | Sind Tool Calls, Argumente, Freigaben und Outputs nachvollziehbar? | <b>0-3</b> |
| <b>Rollback</b>     | Gibt es Korrektur- oder Ruecknahmeprozesse fuer Schreibaktionen?   | <b>0-3</b> |
| <b>Kill Switch</b>  | Kann Agent oder Tool sofort deaktiviert werden?                    | <b>0-3</b> |

#### HARTE STOP-KRITERIEN

- Schreibrechte ohne Tool- und Approval-Policy.
- Globale Admin-, Mailbox-, Drive- oder Graph-Rechte ohne Begrueendung.
- Untrusted content plus Tool-Ausfuehrung ohne Isolation.
- Kein Audit fuer externe oder mutierende Aktionen.
- Kein verantwortlicher Owner.

#### KURZ-CHECKLIST

- Agentenidentitaet und Owner definiert.
- Tool-Liste und Tool-Manifeste vorhanden.
- Scopes minimal und getrennt nach Aufgabe.
- P0-P5-Aktionstier je Tool festgelegt.
- Human Approval vor P4/P5-Aktionen eingerichtet.
- Traces, Rollback und Kill Switch vorhanden.

Tirion nutzt diese Scorecard als kompaktes Arbeitsdokument. Das vollstaendige Framework steht als HTML-Seite auf der Tirion Website.