moring

AGENT READINESS CHECKLIST / 36 CHECKS / ONE DEPLOYMENT

Is this agent ready for production?

Pick one agent in one environment. Work through the 36 checks and mark what you can show today, with the record that shows it.

Agent / environment: _____ Owner: _____ Date: _____

What the agent can change (systems, data, money): _____

How to mark each check. Verified: you ran the test and kept the record. Partial: in place but incomplete, untested, or only on some agents. Unknown: no one can show it yet. Each check lists a test you can run and the record to keep. The scoring guide is on the last page.

01 Identity and access

ID-1 **Each agent has its own workload identity**
Test: List identities in the identity provider or secret store. None are shared between agents. **Keep:** Identity inventory export
☐ Verified ☐ Partial ☐ Unknown
Owner: _____ Record / date: _____

ID-2 **Agents use no shared or human service accounts**
Test: Search tool-call logs for human or shared accounts. **Keep:** Log query and result
☐ Verified ☐ Partial ☐ Unknown
Owner: _____ Record / date: _____

ID-3 **Credentials are short-lived**
Test: Check token lifetime and rotation settings. **Keep:** Token policy or config
☐ Verified ☐ Partial ☐ Unknown
Owner: _____ Record / date: _____

ID-4 **Each action records the person the agent acted for**
Test: Pick 5 actions. Each names the agent and the on-behalf-of user. **Keep:** 5 sample records
☐ Verified ☐ Partial ☐ Unknown
Owner: _____ Record / date: _____

ID-5 **Tokens are scoped per tool and accepted by one service only**
Test: Decode a token and check its audience and scopes. The caller's token is never passed through. **Keep:** Decoded token, redacted
☐ Verified ☐ Partial ☐ Unknown
Owner: _____ Record / date: _____

ID-6 **Human approvers are named and authorized for what they approve**
Test: Check the mapping of approvers to roles. **Keep:** Approver role table
☐ Verified ☐ Partial ☐ Unknown
Owner: _____ Record / date: _____

02 Policy and controls

PL-1 **Policy is written as code in version control**
Test: Find the repository and its last 5 changes. **Keep:** Repository link and history
☐ Verified ☐ Partial ☐ Unknown
Owner: _____ Record / date: _____

PL-2 **Anything without a matching rule is denied**
Test: Call a tool that no rule covers. **Keep:** Test run output
☐ Verified ☐ Partial ☐ Unknown
Owner: _____ Record / date: _____

PL-3 **Every tool call is checked against policy before it runs**
Test: Trace one call end to end. The policy decision comes before execution. **Keep:** Trace with timestamps
☐ Verified ☐ Partial ☐ Unknown
Owner: _____ Record / date: _____

PL-4 **Policy has automated tests that gate merges**
Test: Run the test suite and confirm it blocks a failing merge. **Keep:** CI run
☐ Verified ☐ Partial ☐ Unknown
Owner: _____ Record / date: _____

PL-5 **New policy runs in observe-only (shadow) mode before it enforces**
Test: Check the last policy rollout for an observe-only period. **Keep:** Shadow-mode log
☐ Verified ☐ Partial ☐ Unknown
Owner: _____ Record / date: _____

PL-6 **Policy changes are reviewed and logged**
Test: Check the approval and audit entry for the last change. **Keep:** Change record
☐ Verified ☐ Partial ☐ Unknown
Owner: _____ Record / date: _____

03 Data and egress

EG-1	**Outbound destinations are on an allowlist** **Test:** Try a call to a host that is not listed. **Keep:** Blocked-call log	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____
EG-2	**Calls to unknown hosts are blocked and raise an alert** **Test:** Check that an alert fired for that attempt. **Keep:** Alert record	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____
EG-3	**Sensitive data, such as personal data, is labeled and checked before it leaves** **Test:** Send a labeled record to a tool that is not approved for it. **Keep:** Block or escalation record	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____
EG-4	**Code runs in a sandbox with no standing credentials** **Test:** Inspect the sandbox configuration. **Keep:** Sandbox config	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____
EG-5	**Secrets never appear in prompts or context** **Test:** Scan prompts and traces for secret patterns. **Keep:** Scan report	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____
EG-6	**Outputs are checked before they reach external systems** **Test:** Find the output filter or review step. **Keep:** Config and a sample	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____

04 Evidence and audit

TR-1	**Each action has one linked record: prompt, identity, tool call and result** **Test:** Pick an action and fetch all four with one trace ID. **Keep:** Trace export	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____
TR-2	**Records are append-only and tamper-evident** **Test:** Check for signing or hash chaining. **Keep:** Verification output	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____
TR-3	**Denied actions are logged as fully as allowed ones** **Test:** Find a denied action in the log. **Keep:** Denied record	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____
TR-4	**Approvals and the approver's identity are in the record** **Test:** Pick an approved action. **Keep:** Approved record	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____
TR-5	**Retention matches the longest rule that applies to you** **Test:** Compare the retention setting with your list of rules. **Keep:** Retention setting and rule list	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____
TR-6	**One query can replay an incident** **Test:** Time a replay of a decision from last week. **Keep:** Query and minutes taken	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____

05 Cost and limits

CP-1	**Each agent has a spend budget with an alert** **Test:** Check the budget and the alert threshold. **Keep:** Budget config	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____
CP-2	**Each tool has a rate limit** **Test:** Exceed the limit in a test. **Keep:** Throttle log	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____
CP-3	**Each task has a maximum number of steps or loops** **Test:** Trigger a loop in a test. **Keep:** Stop record	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____
CP-4	**Each action has a size limit (records touched or amount moved)** **Test:** Try an action above the limit. **Keep:** Block or escalation record	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____
CP-5	**Each agent has a limit on parallel calls** **Test:** Run more parallel calls than the limit allows. **Keep:** Throttle log	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____
CP-6	**Cost is attributed to team, agent and task** **Test:** Pull a cost report by agent. **Keep:** Cost report	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____

06 Stop and recover

KS-1	**Any single agent can be switched off in minutes** **Test:** Time a shutdown in a test. **Keep:** Timed drill record	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____
KS-2	**All agents can be switched off at once** **Test:** Run a global stop in a test. **Keep:** Drill record	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____
KS-3	**Credentials can be revoked quickly** **Test:** Revoke them and confirm calls fail. **Keep:** Revocation test	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____
KS-4	**If the policy engine is down, tool calls are blocked** **Test:** Stop the policy engine, then call a tool. **Keep:** Test output	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____
KS-5	**Each agent has a named owner on call** **Test:** Check the owner list and on-call schedule. **Keep:** Owner table	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____
KS-6	**The stop procedure is drilled on a schedule** **Test:** Check the date of the last drill. **Keep:** Drill log	☐ Verified ☐ Partial ☐ Unknown Owner: _____ Record / date: _____

Scoring guide

Count your marks in each area. Read each area on its own: a strong result in one area does not make up for a gap in another.

Area	Verified	Partial	Unknown	Ready?
01 Identity and access				
02 Policy and controls				
03 Data and egress				
04 Evidence and audit				
05 Cost and limits				
06 Stop and recover				

An area is ready when all six checks are Verified. Count Unknown as a gap: if no one can show it, plan as if it is missing. Partial marks are your shortest list of fixes, because something is already in place.

Next action: _____ Owner / date: _____

Verified is your documented conclusion, not a certification. A yes without a record is not evidence. Keep the record reference, deployed version, date and owner for each check. Online version: moring.ai/resources/agent-readiness-checklist