Agent readiness checklist

agent-trust-baseline 0.1.1 (updated 2026-10-18). 31 requirements.
A self-check list. It is not a compliance claim, a certificate or an OWASP certification.
The OWASP MCP column is a DRAFT mapping for owner review, not a finding.

How to use it

1. Run the check on your repository: npx --yes @shield-agent/kya@latest certify
2. For each row, mark Met only when your own evidence shows the requirement.
3. Keep the evidence (report files, policy, owner names) with the checklist.

Data privacy

ID	Requirement	Sev	OWASP	Check kind	Met
DP-01	Every tool call is checked and recorded	high	MCP08	hooks_wired	[ ]
DP-02	No risky writes allowed in hold mode	critical	MCP02	trail_zero	[ ]
DP-03	No shell commands allowed in hold mode	critical	MCP05	trail_zero	[ ]
DP-04	Secrets are never written to disk	high	MCP01	attest	[ ]
DP-05	Old records are deleted on a schedule	medium	MCP08	attest	[ ]

Security

ID	Requirement	Sev	OWASP	Check kind	Met
SEC-01	The gate blocks, it does not just watch	high	MCP07	config_mode	[ ]
SEC-02	Blocking has happened at least once	medium	MCP08	trail_min	[ ]
SEC-03	Human approval has happened at least once	medium	MCP07	trail_min	[ ]
SEC-04	Security check is not red	high	-	orr_category	[ ]
SEC-05	Unknown tools are not allowed in hold mode	high	MCP09	trail_zero	[ ]

Safety

ID	Requirement	Sev	OWASP	Check kind	Met
SAFE-01	Never-list tools are never allowed	critical	MCP02	trail_zero	[ ]
SAFE-02	A sandbox is available for risky work	medium	MCP05	sandbox_inventory	[ ]
SAFE-03	Latest readiness check is not red	high	-	orr_overall	[ ]
SAFE-04	Destructive actions need human approval	critical	MCP02	attest	[ ]
SAFE-05	Blocked actions have a retry limit	medium	-	attest	[ ]
SAFE-06	Sandbox boundary is proven	medium	MCP05	openshell_prover	[ ]

Reliability

ID	Requirement	Sev	OWASP	Check kind	Met
REL-01	Recording is active	high	MCP08	trail_min	[ ]
REL-02	Unknown tools stay rare	medium	MCP09	trail_ratio	[ ]
REL-03	Readiness check is fresh	medium	-	orr_fresh	[ ]
REL-04	Recording restarts after a crash	low	MCP08	attest	[ ]
REL-05	Reports are generated	low	MCP08	receipts_present	[ ]

Accountability

ID	Requirement	Sev	OWASP	Check kind	Met
ACC-01	Every event knows its session	high	MCP10	attest	[ ]
ACC-02	Every event knows its project	medium	MCP10	attest	[ ]
ACC-03	A readiness check exists	medium	-	orr_fresh	[ ]
ACC-04	Cost review is available	low	-	showback_present	[ ]
ACC-05	A named person owns the policy	high	-	attest	[ ]

Society

ID	Requirement	Sev	OWASP	Check kind	Met
SOC-01	Acceptable-use policy	high	-	attest	[ ]
SOC-02	Plan for when the agent misbehaves	high	-	attest	[ ]
SOC-03	Third-party models are disclosed	medium	-	attest	[ ]
SOC-04	Data-processing terms	high	-	attest	[ ]
SOC-05	Human contact for harm	medium	-	attest	[ ]

What this checklist is not

- It does not show that you comply with any law, regulation or standard.
- It is not an audit, an OWASP certification or a certificate from Shield KYA.
- It does not replace your own review, your legal advice or your governance program.
- Shield KYA’s local CLI hook is advisory and fails open. The hosted product is a separate service.

shield-agent.com/readiness-checklist Contact: it@shield-agent.com