Enterprise AI Agent Security Readiness Checklist

Educational self-assessment · Not a certification · November 2026

Organization / system: _____ Environment: _____

Assessor: _____ Date: _____

Mark Yes, No, Unknown or N/A. Record evidence and ownership separately. A Yes is a self-report until independently verified; N/A requires justification. A failed mandatory gate cannot be offset by a maturity score.

Seven-domain screening

Domain	Assessment question	Response
D1 Identity	Verifiable identity, tenant and accountable owner for each agent?	Y / N / ? / N/A
D2 Authorization	Independent authorization for identity, action, resource and parameters?	Y / N / ? / N/A
D2 Authorization	All protected resource paths covered by non-bypassable enforcement?	Y / N / ? / N/A
D3 Delegation	Delegation chain validated for scope, expiry and revocation?	Y / N / ? / N/A
D3 Delegation	Delegated agents independently authorized for protected actions?	Y / N / ? / N/A
D4 Runtime	Credentials, tools, network, quotas and time constrained?	Y / N / ? / N/A
D5 Governance	High-risk actions blocked until approval and reauthorization?	Y / N / ? / N/A
D6 Assurance	Authorization correlated with actual execution and resource state?	Y / N / ? / N/A
D6 Assurance	Evidence integrity protected and gaps monitored?	Y / N / ? / N/A
D7 Recovery	Revocation blocks subsequent actions, including cached grants?	Y / N / ? / N/A
D7 Recovery	Containment, partial effects and privileged recovery tested?	Y / N / ? / N/A

Critical gates for high-impact deployments

[ ] G1 Identity and accountable ownership

[ ] G2 Independent authorization

[ ] G3 Delegation non-amplification

[ ] G4 Independent approval and reauthorization where required

[ ] G5 Non-bypassable execution boundary and runtime limits

[ ] G6 Attributable execution evidence

[ ] G7 Revocation and containment

Disposition: Ready within defined scope / Not ready / Not established

Evidence register / remediation priorities

1. Control / finding: _____ Evidence / owner: _____

2. Control / finding: _____ Evidence / owner: _____

3. Control / finding: _____ Evidence / owner: _____

This checklist is a screening aid, not proof of implementation, certification or compliance with NIST, ISO or the EU AI Act. Formal findings require a defined scope, tests, and review.

Daankwee Group · https://www.daankwee.com