A Gartner G-Cloud 15 Service Definition for

Cloud Consulting: Cloud Security — AI Security & Risk Assessment

2026

Gartner G-Cloud 15 Service Definition

Gartner

Service Summary

Gartner's AI Security & Risk Assessment service enables organisations to identify, evaluate, and mitigate security and risk concerns associated with AI usage and deployments. Gartner provides independent assessments, best practice recommendations, and tailored strategies to enable AI solutions that are trustworthy, secure, and compliant with regulatory requirements.

Service Description

Gartner's AI Security & Risk Assessment service provides an objective and comprehensive evaluation of the client's AI systems, focusing on risk management, security controls, and trustworthiness. Gartner begins by engaging with stakeholders to understand the organisation's AI landscape, use cases, and business objectives. Through structured workshops and data collection, Gartner assesses existing AI governance, security frameworks, and risk exposure across critical AI assets and processes.

Gartner applies its AI Trust, Risk, and Security Management (TRiSM) methodology to benchmark the maturity of AI security controls, identify gaps, and prioritise remediation activities. The assessment covers data integrity, model robustness, privacy, ethical risks, and compliance with relevant standards. Gartner works collaboratively with clients to develop a tailored improvement roadmap, including tactical and strategic recommendations for strengthening AI security posture and managing risks throughout the AI lifecycle.

Throughout the engagement, Gartner leverages industry-leading research, toolkits, and frameworks to deliver actionable insights and support operationalisation. Upskilling and awareness programmes are provided to enable teams, so they are equipped to maintain secure, trustworthy, and compliant AI systems, enabling clients to harness the full potential of AI while minimising risk.

Service Benefits

- Reduces corporate risk of AI-related security incidents and breaches
- Compliance with AI regulations and ethical standards
- Improves visibility of AI assets and risk exposure
- Strengthens governance and control over AI deployments
- Enables rapid identification and remediation of vulnerabilities
- Supports responsible and trustworthy AI development
- Enhances resilience against adversarial attacks and data poisoning
- Provides actionable recommendations for risk mitigation
- Provides targeted upskilling and awareness for AI security
- Facilitates stakeholder alignment, confidence building and informed decision-making

Service Features

- Comprehensive assessment of AI security and risk controls
- Stakeholder workshops and data collection sessions
- Benchmarking using Gartner's TRiSM methodology
- Gap analysis and prioritised remediation planning

Gartner®

- Review of AI governance and compliance frameworks
- Evaluation of data integrity and model robustness
- Accelerates delivery of actionable insights through proven analytical capabilities
- Development of tailored improvement roadmap
- Development of upskilling and awareness programmes for staff
- AI-powered analysis that augments Gartner's Insights and SME delivery experience

Full List of Service Features

- Project Plan — Following project initiation, Gartner will propose a detailed plan outlining roles, responsibilities, stakeholders, and key milestones for the AI security and risk assessment.
- Stakeholder Workshops — Gartner will facilitate sessions to understand the client's AI landscape, business objectives, and risk appetite, ensuring all relevant perspectives are considered.
- Data Collection — Gartner will assist the client in gathering documentation on AI assets, processes, governance structures, and security controls.
- TRiSM Benchmarking — Gartner will apply its Trust, Risk, and Security Management methodology to objectively assess the maturity of AI security controls and risk management practices.
- Gap Analysis — Gartner will identify gaps in AI security, privacy, and compliance, prioritising remediation activities based on risk exposure and business impact.
- Improvement Roadmap — Gartner will develop a tailored roadmap with tactical and strategic recommendations for strengthening AI security and managing risk across the AI lifecycle.
- Upskilling and Awareness — Gartner will deliver targeted training sessions and awareness programmes to equip staff with the knowledge required to maintain secure and trustworthy AI systems.
- Ongoing Support — Gartner will provide ongoing support for operationalising recommendations and monitoring AI security posture.

Project Approach

- Week 0: Project Initiation and stakeholder alignment. Gartner will engage with key client representatives to clarify objectives, define roles, and agree on project milestones and deliverables.
- Weeks 1-4: Stakeholder Workshops & Data Collection. Gartner will facilitate sessions to understand the AI landscape, gather documentation, and identify critical assets and processes.
- Weeks 1-6: TRiSM Benchmarking & Gap Analysis. Gartner will assess AI security controls and risk management maturity, identifying gaps and prioritising remediation activities.
- Weeks 1-6: Governance & Compliance Review. Gartner will evaluate AI governance frameworks, privacy controls, and ethical risk management practices.
- Weeks 1-8: Roadmap Development. Gartner will collaborate with clients to create a strategic and tactical plan for strengthening AI security and risk management.

- Weeks 1-8: Upskilling & Awareness Programmes. Gartner will deliver targeted training sessions and awareness programmes for staff involved in AI development and deployment.
- Weeks 1-12+: Operationalisation & Ongoing Support. Gartner will support the implementation of recommendations and provide guidance for monitoring and maintaining AI security posture.

Project Schedule

Gartner anticipates that the AI Security & Risk Assessment engagement will require approximately 6-8 weeks depending on the activities within scope. The precise timeline will be tailored to the scope and specific requirements of each client and may be adjusted to accommodate organisational complexity, stakeholder or regulatory needs.