A Gartner G-Cloud 15 Service Definition for

Cloud Consulting: Cloud Security — Supply Chain Security Assessment

2026

Gartner G-Cloud 15 Service Definition

Gartner

Service Summary

Gartner will undertake a tailored supply chain security assessment, covering risks arising from the client's supply chain. It is tailored to the client's operational/risk context and extends across the linked set of resources and processes for their sourcing of products and services through the product and service life cycle.

Service Description

Gartner will independently and objectively assess the security of the products and services within the required scope for assessment of a client's supply chain. The output is tailored to an organisation's objectives for the assessment and can include one or more of the following:

- A security assessment of the product and service security provision, comprising:
  - A description of the current security status of the assessed products and services, matched to an established Gartner set of evaluation criteria
  - A gap analysis comparing current and target states aligned with the organisation's risk appetite
  - An actionable set of recommendations
- A comprehensive security risk assessment covering all or part of an organisation's supply chain. This covers any harm or compromise that may arise from the supply chain. To identify risks and recommend mitigation measures for all in-scope products and services

Where appropriate, the analysis covers the intersection of acquirer and supplier resources and processes.

Service Benefits

- Provides clear view of supply chain risk to organisation/service
- Delivers an actionable plan to mitigate identified risks
- Delivers an unambiguous assessment of the supply chain security status
- Tests the flow-down of security contractual terms and conditions
- Gives evidence-based results based on testing suppliers' claims
- Analysis/results account for coverage of security provisions
- Analysis/results account for coverage of the maturity of controls
- Analysis and results account for the maturity of controls
- Accelerates delivery of actionable insights through proven analytical capabilities
- AI-powered analysis that augments Gartner's Insights and SME delivery experience

Service Features

- Combines evidence from the suppliers, service documentation and interviews
- Workshops validate findings and support in-depth investigation
- Supported by the Gartner cyber security controls assessment tool
- Gartner pre-defined questionnaires underpin the assessment

Gartner®

- Staff experienced in complex supply chain security provision
- Provides a view of end-to-end supply chain security risk
- Delivers an actionable supply chain risk mitigation plan

Full List of Service Features

Gartner combines extensive supply chain security assessment experience with established and tested tools, techniques and reference data to conduct in-depth assessments that probe and test product and service suppliers' claims of security provision. The assessment can look across an enterprise's supply chain or be targeted to a specific domain or subset of operations.

The assessment is closely mapped to the guidance in the NIST Special Publication 161, Cyber Security Supply Chain Risk Management Practices for Systems and Organisations. It also accounts for U.K. regional guidance such as NCSC's Vendor Security Assessment Guidance. Where software product development is involved, secure code verification methods and standards such as the OWASP Application Security Verification Standard (ASVS) are applied.

The assessment is closely tailored to the specific operational and risk context of clients. Results and output are tailored to specific client requirements, ranging from in-depth technical reports to board-level communications materials.

The analysis can cover the full scope of the service delivery life cycle. It accounts for the challenge of the complexity of ICT/OT networks that span supply chain boundaries and the potential depth of supply chains that may involve several levels of subcontracting. These complexities are given appropriate focus through rigorous scoping.

Project Approach

- Week 0: Project mobilisation and kick-off
- Week 1: Validate the scope and develop operational context and risk input
  - Scope of the client's organisation and operations included
  - Specified product and service providers to be assessed
  - Depth of supply chain investigation
  - Identified areas of risk and focus
- Weeks 2 to 4:
  - Issue tailored security questionnaires — by the end of week 2
  - Determine operational and risk context, validating the acquirer's risk appetite across the range of products and services being assessed
  - Review supplied contractual, security, risk and control information
  - Schedule known workshops, supplier interviews and on-site visits
  - Conduct initial acquirer-side interviews
- Weeks 5 — 7:
  - Review questionnaire responses and issue clarification questions
  - Complete interim assessment
  - Schedule remaining workshops, supplier interviews and on-site visits
  - Conduct interviews, workshops and on-site visits

- Weeks 8 — 9:
  - Complete an in-depth assessment
  - Account for contractual, ICT/OT and security control interdependencies and the operational and threat context
  - Gap analysis
- Week 10: Reporting:
  - Development of recommendations
  - Gartner Supply Chain Security Assessment Report
  - Develop any agreed communication materials, such as Board briefing materials

Assumptions

Data Collection:

- Document gathering can commence as soon as the engagement is agreed and the required confidentiality agreements have been signed
- The due diligence (as is) data are reasonably available via interviews and documentation review
- Detailed description of the existing IT landscape and business processes within scope have been documented sufficiently, and no additional analysis needs to be performed by Gartner
- The organisation will provide timely access to all appropriate personnel to be interviewed. These personnel will have the ability to provide data necessary to complete the project, answer questions, provide existing documentation and attend working sessions

Project Schedule

This service description is based on a ten-week engagement.