A Gartner G-Cloud 15 Service Definition for

Cloud Consulting: Cloud Security — Cyber Security Controls Maturity Assessment

2026

Gartner G-Cloud 15 Service Definition

Gartner

Service Summary

Gartner provides a trusted independent assessment of cyber security capability and maturity across enterprise digital technologies, covering IT and Operational Technology (OT) for cloud, on-premises and hybrid services. The maturity assessment is benchmarked against sector peers. It is closely aligned with NCSC and NIST standards and mapped to ISO 27001.

Service Description

The Gartner Cyber Security Maturity Assessment provides a trusted, independent assessment of cyber security maturity based on a widely adopted framework that is aligned to the U.S. National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) control categories and underpinned by an industry-aligned reference database for the Gartner Cyber security Controls Assessment service.

The assessment follows a structured analysis of each of NIST's control domains. There is a qualitative and quantitative dimension to the assessment. Weighted criteria are adjusted to match specific client context and cover:

- The scope of business and digital service coverage of the capability in place for the assessed control categories
- Efficacy of the control, both technical and procedural
- Maturity of the control provision

The assessment delivers:

- Detailed findings across the assessed organisation and services in the form of an appraisal for each control category and an integrated view of composite security maturity
- A quantified score that can be compared with a range of benchmark data, such as comparison with sector peers
- Recommendations for improvement

This assessment is particularly useful for organisations who want an independent view of their cyber security maturity and key areas on which to focus improvement and who may wish to compare this with peers in their sector.

Service Benefits

- Supports stakeholder understanding of organisational cyber security maturity
- An approach fully aligned with NCSC and NIST standards
- Comparison with peers/average sector levels of cyber security maturity
- Defined and prioritised recommendations to improve risk posture
- Specific guidance for planning necessary remediation
- Support for cyber security improvement programme definition
- Materials suitable for Board and executive stakeholder presentation
- Accelerates delivery of actionable insights through proven analytical capabilities
- AI-powered analysis that augments Gartner's Insights and SME delivery experience

Gartner®

Service Features

- Structured assessment based on extensive, maintained Gartner reference data
- Strong consultative engagement to investigate your current status
- Output structured to support cyber security improvement programme/initiative planning
- Investigation and analysis undertaken by experienced and certified practitioners
- Graphical analysis and comparison of results with benchmark data

Full List of Service Features

The scope of the Gartner Cyber Security Controls Maturity Assessment is tailored as follows:

- The full set or a subset of the 23 NIST Cyber Security Framework (CSF) controls are selected for assessment
- The operational scope of the assessment, including business and digital technology coverage

Operational and risk context assessment drives the establishment of target cyber security control maturity levels. The current maturity state of the in-scope controls and the targeted scope of business operations is investigated, informed by:

- Relevant documentation
- Key stakeholders with insight and knowledge of control implementation and operation
- Plans for maintenance, upgrade or improvements

A qualitative and quantitative assessment of the in-scope controls is undertaken. Graphical analysis of the quantified results is presented along with required benchmark statistics to enable peer group and industry sector comparison.

A gap analysis between the current and target control maturity states is undertaken. This informs:

- Detailed findings across the assessed organisation and services in the form of an appraisal for each control category and an integrated view of composite security maturity
- A quantified score that can be compared with a range of benchmark data, such as comparison with sector peers
- Recommendations for improvement

Project Approach

- Week 0: Project mobilisation and kick-off
  - Preparatory activities to define the scope of the assessment, prepare information and set up initial interviews with stakeholders
- Week 1 to 3: Determine operational and risk context, review supplied control information, and conduct initial interviews
  - Investigate, determine and validate operation context, risk appetite and resultant target maturity levels for the in-scope controls
  - Conduct interviews with stakeholders, review appropriate control documentation and capture findings

- Week 4: Interim maturity assessment to inform review and validation of target maturity control levels
  - Complete an interim assessment of cyber security control maturity
  - Validate or adjust the target maturity levels for the in-scope controls
- Weeks 5 and 6: Complete a detailed assessment of the current cyber security controls maturity
  - Complete an in-depth assessment covering the selected NIST-CSF control functions
  - Account for control interdependencies and the operational and threat context
- Week 7: Gap analysis and development of recommendations
- Week 8: Compile the final report and any tailored communication materials
  - Gartner Cyber Security Controls Maturity 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.