A Gartner G-Cloud 15 Service Definition for

Cloud Consulting: Cloud Security — Cyber Security for the Board

2026

Gartner G-Cloud 15 Service Definition

Gartner

Service Summary

Gartner will strategically advise clients on industry practices and leadership for cyber security and how to measure, protect and mitigate against security threats and vulnerabilities. Every business has value and cost as levers, and therefore, the value of current cyber security investments requires outcome-driven metrics to measure cyber security risk.

Service Description

The cyber security for the board service will provide support and define strategic activities such as:

- Equipping the Chief Information and Security Officer (CISO) to effectively communicate with the Board by:
  - Creating business-driven cyber security vision and strategies
  - Reporting and communicating the value of cyber security through outcome-driven metrics (ODM), ad hoc dashboards and demonstrating the financial value provided by control investments
  - Understand cyber exposure through financial metrics, combined with security controls maturity and spending analysis
  - Make cyber security effective by allocating resources appropriately to improve return on investment
- Thought leadership and independent assessment:
  - Review and feedback on key plans, scope, methods, approach, outputs and deliverables via assessments, documented reports, workshops and meetings
  - Recommendations for key decisions made during the engagement period to drive excellence in outcomes
  - Outside-in view and challenge to verify or refine approaches, make recommendations and provide supporting evidence
- Industry experience and insight:
  - Active input of key points of view and industry examples for specific workshops and meetings using case studies
  - Facilitate peer exchanges or bring other client examples to assist (with the agreement of the respective Gartner client)
  - Provide expert opinion on key risks, issues and mitigation recommendations

Service Benefits

- Cyber security positioned as a business topic
- Cyber security demystified for the Board
- Empowered CISO leadership
- Optimised cyber security investments and posture
- Manage cyber security budget and prioritise resource allocation
- Visibility in demonstrating value of the cyber security function
- Building leadership credibility through external peer connect/thought leadership

- Building internal capabilty through leading toolkits, methodologies and accelerators
- Accelerates delivery of actionable insights through proven analytical capabilities
- AI-powered analysis that augments Gartner's Insights and SME delivery experience

Service Features

- Weekly cadence of leadership, assurance and oversight
- Accelerate with our unique outcome-driven metrics (ODM) approach
- Operationalise and deliver actionable insights
- Transparent/flexible to address client requirements and emerging challenges
- Regular cadence of governance reporting/planning for the forthcoming period
- Communicate value through ODM/ad-hoc dashboards
- Flexible scope to align with specific areas of the business
- Industry-leading research for cyber security used in analysis/evaluation

Full List of Service Features

Leadership and Reporting

Gartner will be a strategic advisor to organisations to provide thought leadership and best practice input to the management and oversight of IT and operational technology (OT) security practices and to provide effective communication to the board.

- Providing guidance and advisory support toward the execution of optimising security capabilities within the client’s environment
- Establish and oversee effective governance, guiding the development/improvement of governance-related documentation, such as policies, processes, and procedures
- Advice on risk prioritisation to enable focus on what is essential to the client and also address regulatory concerns and requirements
- Provide oversight and strategic input into key initiatives such as regulatory reports.

Strategic Planning

- Gartner will drive the development of a security strategy in response to current as-is and future-state requirements, pulling together client resources to define a cyber security strategy that will work for the client and a roadmap to deliver the defined strategy

Cyber Security Dashboard for the Board

Gartner will help Chief Data and Information Officers (CDIOs) and CISOs communicate security performance and value to the board by selecting the right metrics and target values and accelerating dashboard operationalisation.

- Develop and deliver reporting and dashboarding, establishing KPIs and metrics, reporting framework and capturing appropriate data
- Combine cyber security and its expertise and communication knowledge
- Provide an extensive base of benchmark data on KPIs and ODM
- Accelerate with our unique outcome-driven metrics approach
- Operationalise and deliver actionable insights.

Project Approach

Below is an example where cyber security metrics were customised for an organisation's Board of Directors or senior management.

Phase 1 — Frame and scope dashboarding

Kick-off

- Kick off the project and ensure the proper identification of stakeholders, planning and deliverables
- Define the kick-off meeting agenda, including:
  - Validation of scope, roles and responsibilities
  - Finalisation of the project plan
  - Conduct kick-off meeting

Deliverables

- Kick-off deck

Confirm needs and capture the current state

- Determine target audience(s) (e.g., CEO, CISO, COO, CIO, CFO, domain leaders) for the cyber security and IT dashboards by performing interviews to capture their related concerns, expectations and priorities
- Capture the existing initiatives related to the cyber security dashboarding
- Collect information on existing metrics/Key Risk Indicators (KRIs)/KPIs, the related tools in place, teams/people involved in the data collection and dashboarding
- Collect information on the available data sources
- Assess the data collection capabilities, including the extent and reliability of the existing data sources and data collected
- Evaluate the need and types of KRIs/KPIs and their feasibility based on expectations, priorities, and current data collection and indicator production capabilities

Deliverables

- Summary of the organisation's needs and current state regarding metrics/KPIs/KRIs and cyber security dashboards

Scope dashboards

- Propose sets of candidate metrics/KRIs/KPIs for each dashboard in the scope of the engagement, with the expected level of granularity and the frequency of updating
- Hold a workshop with stakeholders to confirm the sets of metrics/KRIs/KPIs to be included in the dashboards to be delivered by the project

Deliverables

- Set of metrics/KRIs/KPIs to be included in each dashboard to be delivered

Phase 2 — Design dashboard(s) and produce first reports

Design dashboards to be delivered

- Develop a framework for the cyber security department/IT department indicators and dashboards: the general rules, dashboard formats, requirements for the metrics/indicators

- Hold workshops with security and operations stakeholders to determine the way to calculate the suggested metrics/KRIs/KPIs measurements and to define target values and thresholds
- Develop dashboard prototypes in scope, including the list of the indicators/metrics used
- Conduct a workshop per dashboard to present the prototype and collect feedback
- Update the prototypes, feed the dashboards with KRIs/KPIs/metrics test values provided by the organisation and present the results

Deliverables

- Framework for the indicators and dashboards
- Dashboards with test results
- Description of the KPIs/metrics included in the dashboards, target values and thresholds

Deliver the first dashboard report with available data

- Lead organisation to perform collection of real data required for the dashboards
- Calculate the metrics and indicators and populate the dashboards
- Conduct workshop with the stakeholder's project team to present the dashboards and collect feedback
- Collect feedback and update the dashboard to v1.0

Deliverables

- Version 1.0 of dashboards
- Dashboard production process
- Executive briefing presentation sessions

Phase 3 — Build longer-term implementation roadmap

Define prioritised roadmap and initiatives for the realisation of a complete target set of metrics/KRIs/KPIs

- Propose the entire set of the target metrics/KRIs/KPIs to be implemented for the client (including those delivered by the Project) and integrated into the dashboard(s)
- Conduct a workshop to review and finalise the target set dashboard(s), validate gaps to be closed regarding the data sources and existing indicators to be replaced/modified
- Generate a high-level roadmap for dashboard(s) realisation over the next years, indicate potential quick wins and estimate budget for dashboard(s) realisation
- Prepare and deliver a consolidated project report and present executive briefing

Deliverables

- High-level dashboard(s) realisation roadmap
- Consolidated project report and executive briefing presentation
- Communication materials

Project Schedule

The typical outcome-driven metrics/dashboards, maturity or risk assessments are expected to last between 6-12 weeks; however, this is subject to change depending on the organisation's size and the number of domains in scope. Set out below is an example of a typical engagement for outcome-driven metrics/dashboards.

- Phase 1 — Frame and scope dashboarding:
  - 1 Week: Kick-off
  - 2 Weeks: Confirm needs
  - 2 Weeks: Scope dashboards
- Following Phase 1: Phase 2— Design dashboard(s) and produce first reports:
  - 3-4 Weeks: Design the first reports
- Following Phase 2: Phase 3— Build longer-term implementation roadmap board(s):
  - 2 Weeks: Long-term roadmap

Assumptions

Gartner will provide a named individual who agrees with the client as the key point of contact and primary delivery resource for this engagement. Supporting this individual will be the depth of Gartner, including:

- Support of and access to the wider Security and Risk Management practice in Gartner Consulting, including access to specialist resources, intellectual property, use of Gartner research and toolkits
- Access to subject matter expertise within Gartner, whether other consultants or research analysts to contribute to, verify, or validate the work being conducted within this statement of work
- Reporting through the Gartner Consulting Managing Partner as a conduit for access to additional support as required and broader industry insight
- If unforeseen circumstances require the replacement of an associate on an engagement, Gartner will inform the client as soon as reasonably possible and substitute appropriate associates with comparable skills