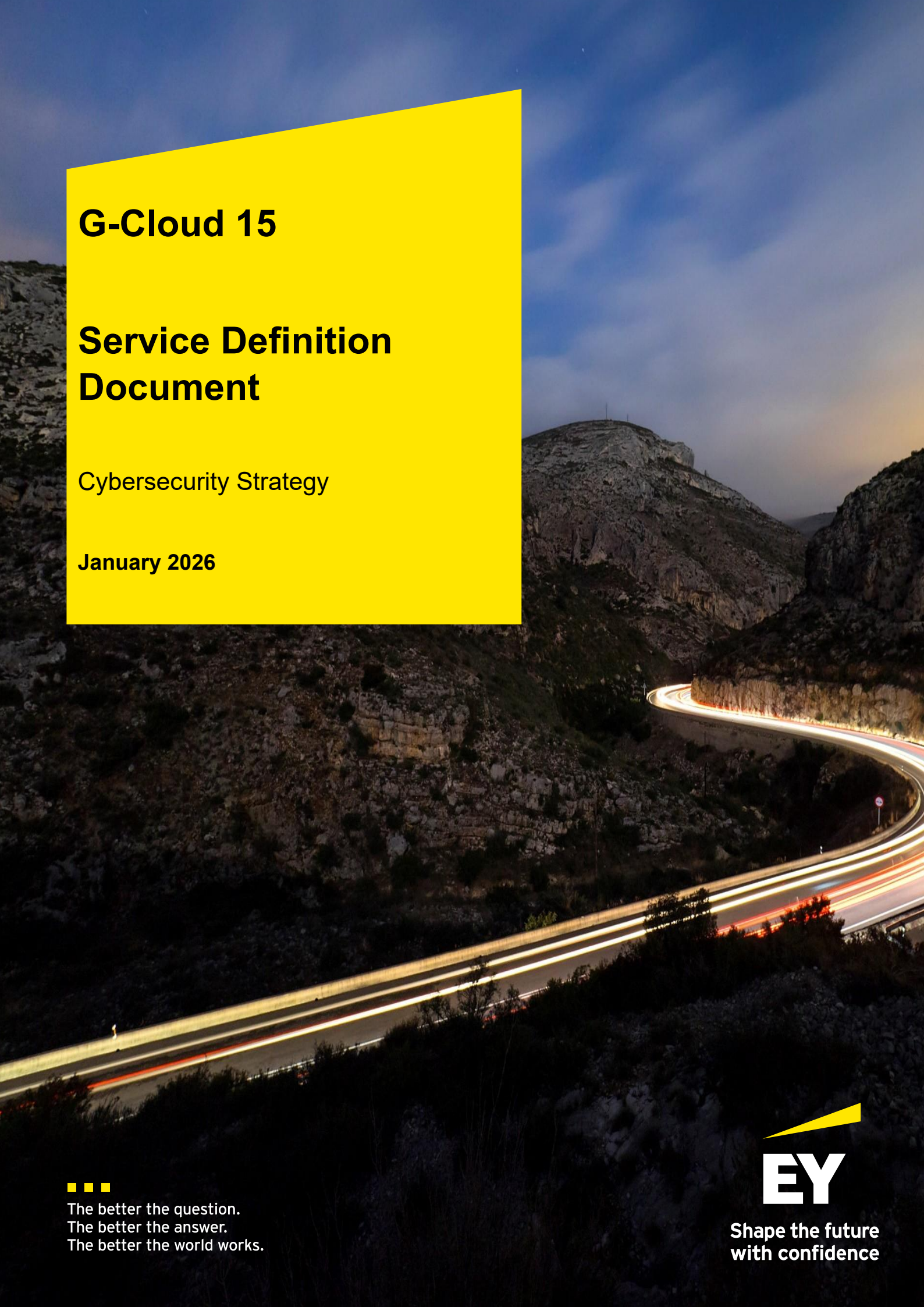




G-Cloud 15

Service Definition Document

Cybersecurity Strategy

January 2026



The better the question.
The better the answer.
The better the world works.



Shape the future
with confidence

Contents

Contents	1
1. Service detail	2
2. Key contacts	5

1. Service detail

Cybersecurity Strategy Service

A cybersecurity strategy is a comprehensive plan that outlines an organisation's approach to ensuring the confidentiality, integrity, and availability of digital assets, networks, and systems. The key goal of a cybersecurity strategy is to protect the organisation against emerging cyber threats and support business continuity even in the face of cyber-attacks.

With an ever-changing cyber threat landscape and increasing compliance requirements, organisations constantly need to improve their cybersecurity posture. A cybersecurity strategy is a critical step in achieving this.

Cybersecurity strategies define the purpose of a cybersecurity program and lay out a strategic plan for enabling the business, reducing risk to the organisation, and optimising cybersecurity operations. They are tools to build trust with executives, stakeholders, and cybersecurity operational teams, by providing a clear vision of how cybersecurity supports a business' agenda and contributes to value creation.

EY's Cybersecurity Strategy Service assists organisations in developing or uplifting their cybersecurity strategy. The service provides a phase-by-phase overview of activities needed to drive the creation of a cybersecurity strategy. These include mobilisation, defining the cybersecurity vision and mission, conducting discovery and review activities, designing the draft strategy document and creating an implementation plan (*as an optional element of cybersecurity strategy projects*). Additionally, the service also provides a view of cybersecurity strategy benchmarking, informed by the EY Benchmark tool.

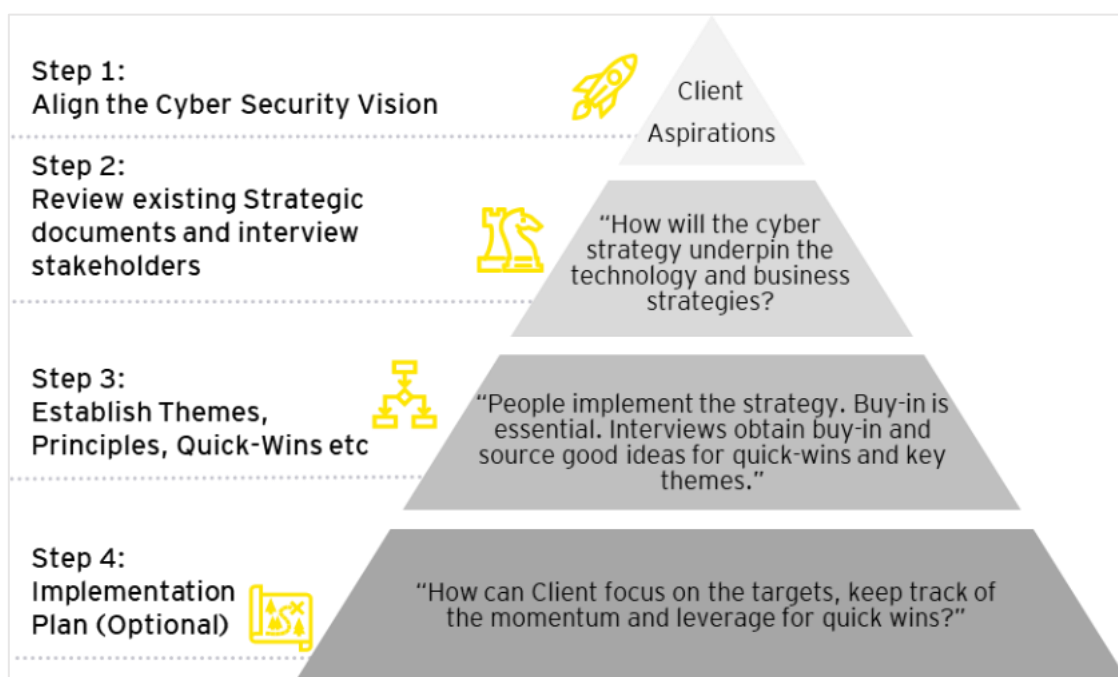


Figure 1 – Cyber Strategy Framework

Key Outcomes:

- **Clear Cybersecurity Vision and Direction:** A clearly articulated cybersecurity vision and mission that aligns with the organisation's values, culture and business objectives, providing a shared sense of direction for leadership and delivery teams
- **Business-Aligned Strategic Priorities:** A defined set of strategic pillars and priority initiatives, aligned to business objectives and key performance indicators, that structure and guide cybersecurity investment and decision-making
- **Risk-Informed Strategic Positioning:** A clear view of the organisation's current and target cybersecurity posture, informed by risk, regulatory expectations, and industry good practice, enabling informed prioritisation and trade-offs
- **Industry and Peer Benchmarking:** Insight into how comparable organisations structure, resource, and focus their cybersecurity strategies, providing context on relative maturity, areas of differentiation, and improvement opportunities
- **Actionable Delivery Roadmap:** A practical, prioritised implementation roadmap setting out initiatives, sequencing, ownership, success measures, and stakeholder engagement, enabling the strategy to be executed and tracked over time

Approach

Our approach helps organisations develop a clear, business-aligned cybersecurity strategy that manages risk and enables business value. It combines strategic direction from senior leadership with practical insight from operational teams, making the strategy credible at the board level and grounded in delivery reality. The strategy can be supported by a prioritised roadmap or implementation plan, enabling organisations to move from ambition to execution.

Our strategic approach leverages both a top-down and bottom-up view.

Top-down engagement focuses on working with senior leaders to understand business priorities, risk appetite, and transformation objectives. This shapes the strategic direction, aligns with wider organisational goals, and supports consistent communication of the strategy across the organisation.

Bottom-up engagement brings insight from operational security and technology teams who manage day-to-day risks and controls. This provides a detailed understanding of current challenges, inefficiencies, and improvement opportunities that may not be visible at senior levels, strengthening the practicality and credibility of the strategy.

Step 1: Mobilisation

- Establish objectives, scope, and stakeholders through engagement with senior leadership and review of existing strategies and plans
- Facilitate initial workshops with security leadership and management teams to identify key themes, principles, and early improvement opportunities

Step 2: Discovery and Review

- Conduct internal discovery through documentation review and stakeholder engagement to identify strengths, pain points, constraints, and key cyber and business risks
- Perform external discovery to assess the threat landscape, regulatory expectations, and relevant market and industry drivers

Step 3: Vision and Mission

- Facilitate workshops with security leadership to define a clear cybersecurity vision and mission aligned to business objectives and performance measures
- Develop concise vision and mission statements that articulate the role of cybersecurity in supporting organisational outcomes

Step 4: Strategy Design

- Use discovery insights, board expectations and compliance requirements to shape the security strategy, identify capability gaps, and define strategic pillars with clear purpose, strengths and ambitions
- Co-create the strategy with key stakeholders to drive alignment, shared ownership, and commitment, including an approach for review and iteration

Step 5: Implementation Design (optional)

- Translate the strategy into a practical implementation roadmap, defining prioritised initiatives, sequencing, ownership, dependencies, and success measures
- Establish governance, reporting, and communication mechanisms to support effective delivery, oversight, and ongoing engagement

2. Key contacts

For further information please get in touch via the email address below.



Rick Hemsley

Consulting Cybersecurity – Government and Infrastructure -
Partner

Email: eytenders@uk.ey.com



Matt Saville

Consulting Cybersecurity – Government and Infrastructure -
Director

Email: eytenders@uk.ey.com

EY | Building a better working world

About EY

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organisation, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organisation, please visit ey.com.

Ernst & Young LLP

The UK firm Ernst & Young LLP is a limited liability partnership registered in England and Wales with registered number OC300001 and is a member firm of Ernst & Young Global Limited.

Ernst & Young LLP, 1 More London Place, London, SE1 2AF.

© 2026 Ernst & Young LLP. Published in the UK.

All Rights Reserved.



In line with EY's commitment to minimise its impact on the environment, this document has been printed on paper with a high recycled content.

Information in this publication is intended to provide only a general outline of the subjects covered. It should neither be regarded as comprehensive nor sufficient for making decisions, nor should it be used in place of professional advice. Ernst & Young LLP accepts no responsibility for any loss arising from any action taken or not taken by anyone using this material.

ey.com/uk