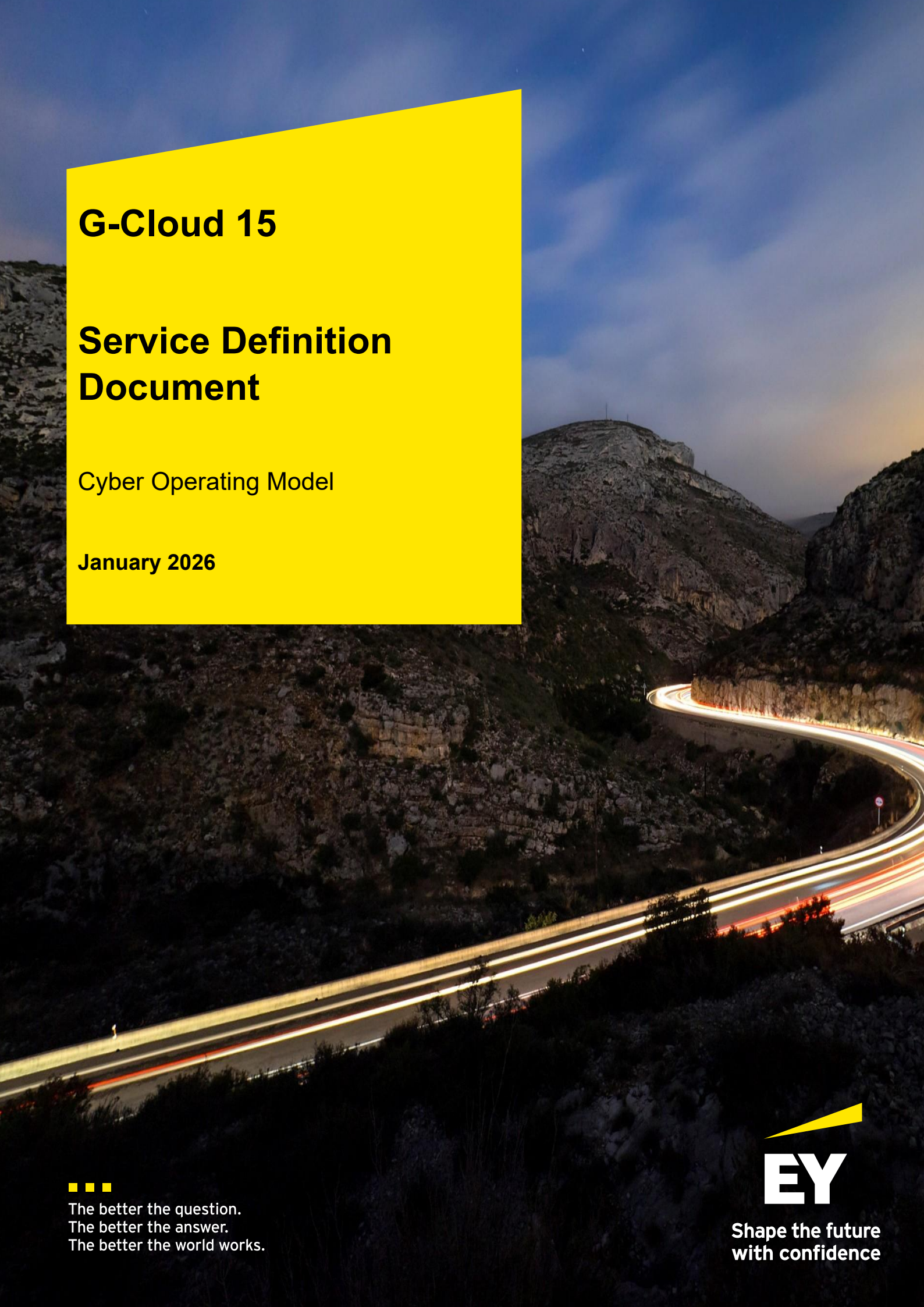

G-Cloud 15

Service Definition Document

Cyber Operating Model

January 2026

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

Shape the future with confidence

Contents

1. Service detail

Cyber Operating Model Service

With the evolving cyber threat landscape, scale of adopting innovative technology (AI) and overlapping regulatory compliance requirements, organisations constantly need to be reviewing and improving their cybersecurity posture. A resilient organisation is dependent on services, systems and structures being underpinned by a robust operating model, which builds a strong foundation for the future, linking risk management, policy and governance to people, skills and culture.

EY's Target Operating Model (TOM) provides a standardised and unified approach to translate your business and cybersecurity strategy into a flexible organisational model that is built on leading practices. The TOM enables you to build governance capabilities to help measure, monitor and track the achievement of security objectives for the cyber function.

Key TOM Outcomes:

- **Increased Visibility:** View on all the elements of how an organisation is structured, operated, and managed together to help the organisation deliver on its security strategy and objectives
- **Improved Governance:** Conceptual model and high-level governance and functional ownership of the processes and divisions of responsibility required to achieve the desired service levels
- **Strengthened Security:** Focussed improvements across skills and talent capabilities, security services/processes and overall technology landscape that enables organisations to combat security threats

Figure 1 – EY's Operating Model Outputs

Our framework for developing cybersecurity TOMs consists of 11 core elements, considering people, processes and technology, that are critical for success. Based on an organisation's demand, we usually propose a two-phase approach, which is intended to future proof an organisation's security capabilities based on the evolving threat landscape in a structured and targeted manner.

We adopt a flexible approach across both phases of the TOM, working with clients to establish priorities and define the scope in a way that is relevant and provides the most value. The two phases are as follows:

Phase One Design:

Strategy, Vision and Brand

- Facilitate leadership workshop to define security objectives for the future, including desired culture outcomes
- Align vision, strategy and brand to organisation's business strategic objectives
- Establish clear direction on the destination and set of outcomes needed to achieve the defined strategy and vision

Case for Change

- Understand the current environment, including challenges faced by the organisation and the main drivers for change
- Define the transformation strategy that sets out ambitions for achieving the vision and strategy
- Identify target outcomes aligned to the transformation strategy
- Develop a transformation roadmap to define steps to achieving the change

Design Principles

- Review Case for Change to understand the vision and strategy for the change
- Hold interviews with leadership and/or identified members of the Security team to understand the desired traits of the future state TOM
- Develop a set of design principles to support the realisation of the future state TOM

Organisational Architecture

- Complete a gap analysis of the current organisational architecture and conduct stakeholder interviews
- Create a functional TOM based on interviews, gap analysis and observations
- Define functional descriptions and characteristics
- Develop RACIs to assign responsibility and accountability across the organisation

Phase Two Implementation:

Geographic Architecture

- Understand the organisation's global footprint and derive a view on critical global business operations
- Identify geography-related enablers of new and existing value streams
- Develop geographic architecture blueprint, roadmap and strategy

Governance Architecture

- Design the governance model structure
- Define governance roles and security hand-offs
- Develop escalation and exception processes

Service Delivery Architecture

- Assess current state through stakeholder interviews
- Develop functional RACI
- Define the interfaces, process flows and hand-offs

Process and Policy Architecture

- Complete policy and process gap analysis
- Define, develop and update policies, and processes
- Define interfaces to integrate with the risk management framework

Technology Architecture

- Identify existing technology innovations and planned future capabilities
- Identify technology enablers of vision, strategy and target outcomes
- Develop technology architecture blueprint and roadmap

People Plans

- Define future cyber competency model
- Create persona-led training and awareness journeys
- Update reward/ performance policy and talent strategy

Performance Architecture

- Define leading metrics with ownership clearly aligned to the RACI
- Develop templates to capture data needed to track, analyse and present results

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.

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.

ey.com/uk