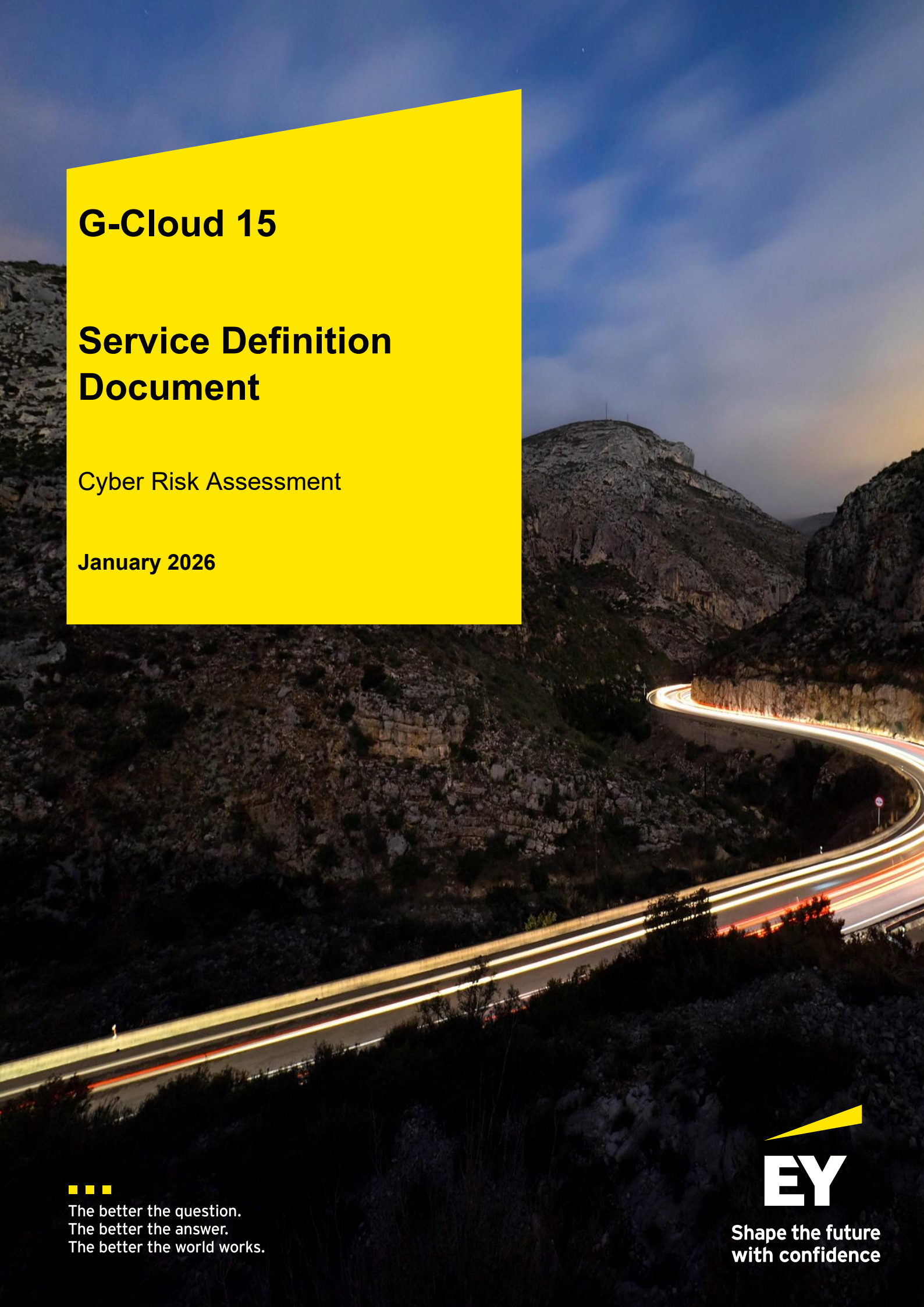

G-Cloud 15

Service Definition Document

Cyber Risk Assessment

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 Risk Assessment Service

According to a 2026 survey conducted by Gartner, only 10% of non-executive directors surveyed have strong confidence in their cybersecurity uplift initiatives and investments. Organisations today are challenged to adapt to an ever-changing ecosystem where new threats and attacks arise daily. At the same time, the attack surface is continuing to expand as organisations increasingly innovate at scale and add new technology, which offers new functionalities and channels greater amounts of data.

EY's Cyber Programme Accelerator (CPA) methodology offers organisations an objective assessment of their cybersecurity programs and structures, provides recommendations on gaps, and helps decide the future state options.

The CPA methodology provides a consistent approach to assessing an organisation's security posture in line within internationally recognised standards and frameworks such as ISO27001, the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and the Information Security Forum Standard of Good Practice (ISF SoGP). We are also able to apply this methodology to UK-specific standards and requirements such as Cyber Essentials, the National Cyber Security Centre's Cyber Assessment Framework (NCSC CAF) and the Cyber Security and Resilience Bill (CSRB).

Our methodology assesses 20 key cybersecurity domains, identifying gaps and weaknesses in an organisation and provides an actionable set of recommendations to drive improvements in the organisation's defences and security posture.

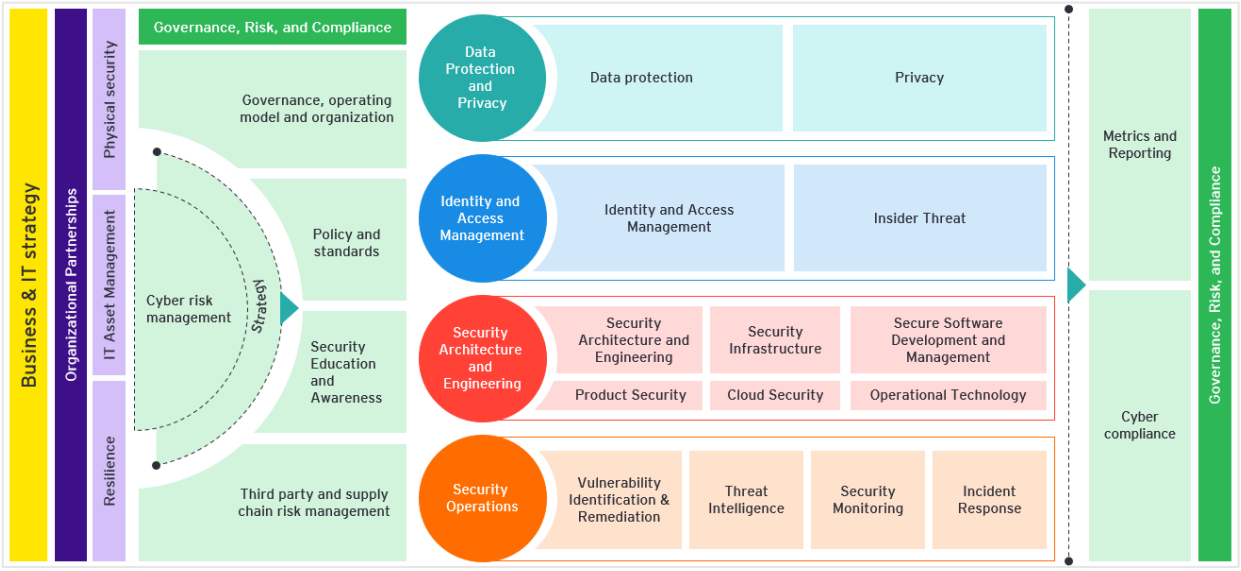

Figure 1 – CPA Domains

The CPA methodology offers different options of assessment levels, ranging from a broad, high-level assessment of maturity, to a deep-dive into a specific information security area/component. CMMI is commonly used to measure cyber maturity on a 1-5 scale in line with our clients' requirements; in addition, we have experience in other scoring methodologies such as NIST Tiers.

The CPA offers an objective assessment of the maturity of an organisation's cybersecurity programs and structures. The CPA reviews the processes, people and technology that an organisation uses to establish, implement, operate, monitor, review, maintain and improve its cybersecurity program. This approach provides organisations with:

- Identification of key business risks related to the maturity of specific cybersecurity domain areas
- Alignment of cybersecurity strategy with a focus on the organisation's strategic priorities and business objectives
- Facilitation of a dialogue between the cybersecurity team and business leaders to articulate the benefits of cybersecurity program investments
- Development of pragmatic recommendations to further improve their cybersecurity programs
- Development of a future state vision and strategic roadmap in support of business objectives
- Improved safeguarding of critical infrastructure and client data

Specifically, our reviews will provide an output that includes:

- A breakdown by domain of the key findings, maturity level and areas of improvement
- Executive reporting that outlines key strengths, areas of improvement, cyber threat landscape, recommendations, and roadmaps
- Roadmap of suggested future cyber improvements linked back to the issues identified

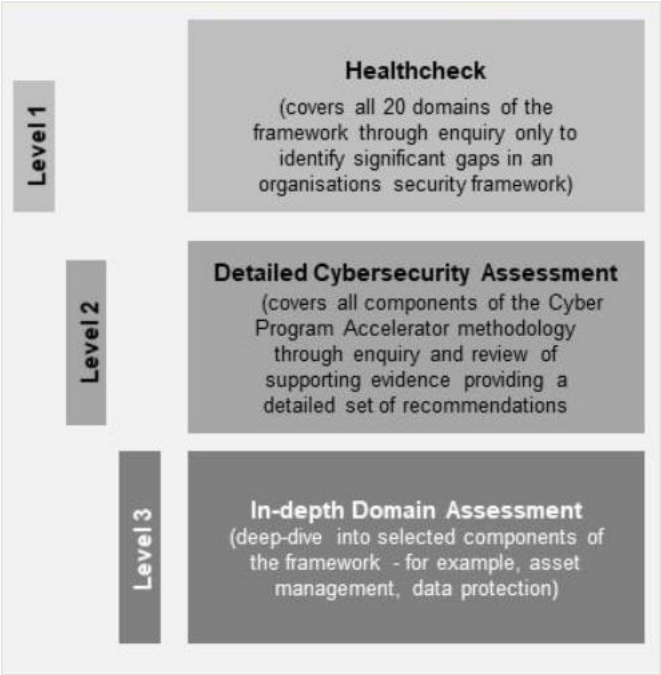

Figure 2 – CPA Assessment Levels

Our assessments can be extended with additional related reviews, such as threat intelligence, physical security (site) reviews, technical vulnerability assessments, cyber risk quantification and benchmarking to provide a comprehensive review of your organisation's maturity.

We have provided cyber maturity assessments across the public and private sector. Often such assessments are used as the initial stage in preparing for a larger transformation journey. Likewise, our assessments can be a useful tool to determine what benefit has been derived after completion of a cyber improvement project or investment in new tools/technology.

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