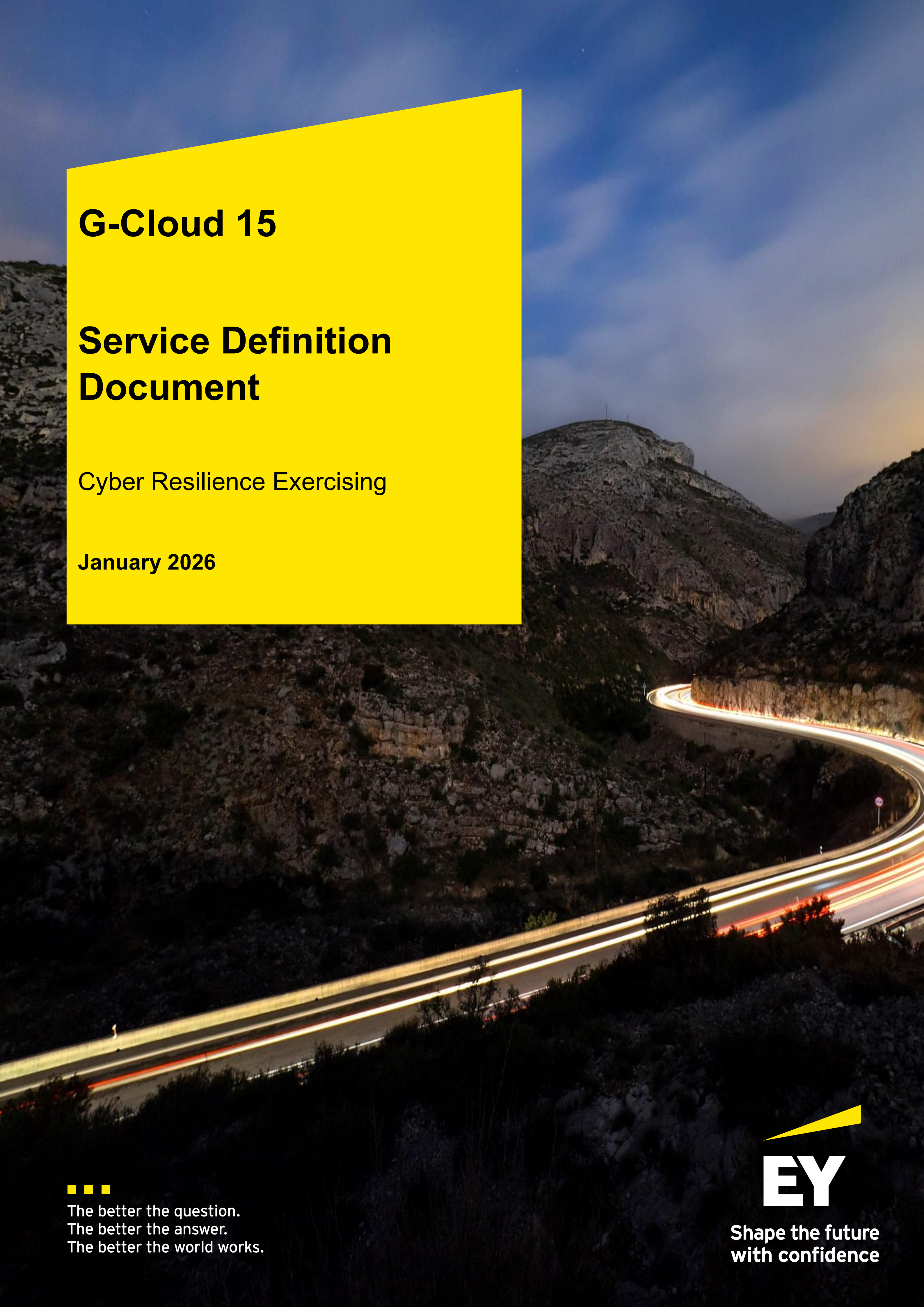

# G-Cloud 15

# Service Definition Document

Cyber Resilience Exercising

**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 Resilience Exercising Service**

Our Cyber Resilience Exercising Service is closely aligned with EY's other cybersecurity offerings. They provide our clients with a comprehensive cybersecurity solution chain. As a National Cyber Security Centre (NCSC) certified incident exerciser, EY delivers cyber exercises that allow clients to validate their crisis response. Effective responses to major cyber crises rely on established processes and a skilled leadership team, both of which are developed and validated over time. Conducting a cyber crisis exercise is a powerful way to assess current capabilities and cyber resilience processes.

We deliver four types of exercises, each of which is tailored to the organisation's maturity level:

1. **Facilitated Discussion:** A group dialogue that guides participants through a realistic attack scenario, enabling them to explore key decisions and define clear action points in a guided environment.
2. **Single-team Simulation:** A table-top validation involving a single team of participants, required to drive activities within the exercise and respond to fully tailored information feeds with facilitation from EY.
3. **Multi-team Simulation:** A table-top validation involving multiple teams (e.g. leadership, technical, functional), required to respond to fully tailored information feeds with facilitation from EY.
4. **Full-scale Live Event or Wargame:** An end-to-end simulation which involves all response and recovery teams, that mirrors real-world crisis conditions. Potentially involving systems and "command post" style working from designated locations.

   The diagram below shows how our cyber exercises are structured and delivered. They translate the exercise types described above into clear deliverables and a simple step-by-step approach.

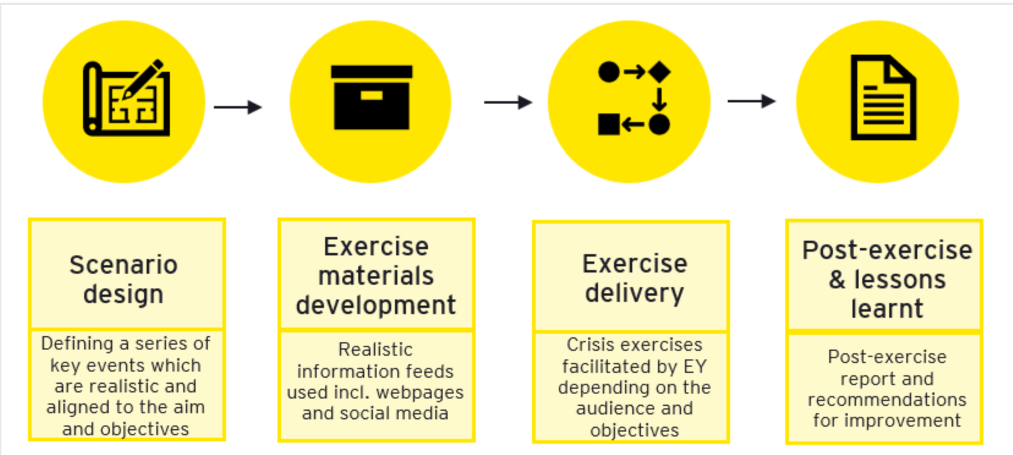


*Figure 1 – Exercise Methodology*

EY's cyber resilience exercising services enable our clients to understand their current capability and maturity through capability understanding, development and validation. EY's services are aligned to the following core standards: Business Continuity ISO 22301, IT

Service Continuity ISO27301, Crisis Management BS11200 and NIST 800-53. Our operational resilience model enables clients to select components that suit their business requirements as seen below.

Cyber crises present unique challenges that make effective response exceptionally complex. The visual below highlights the core issues our exercises are designed to address.

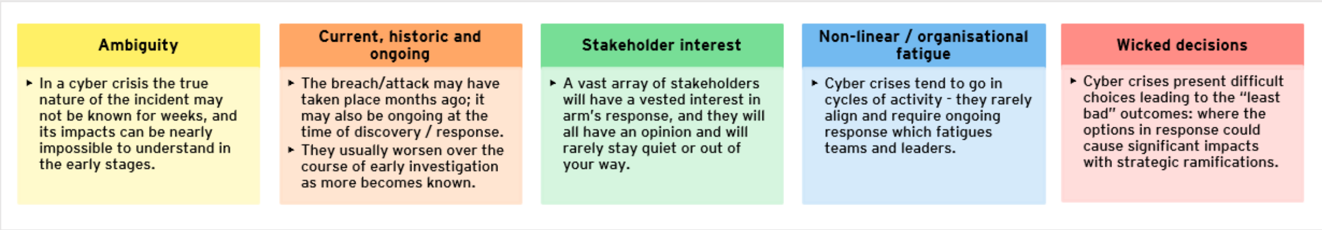


*Figure 2 – What Makes Cyber Different and Difficult*

The features of this service are:

**Capability Understanding**

- Assessing existing processes (including business continuity, crisis management and incident response) against market leading standards and practices such as ISO22301, ISO27361, ISO22316, ISO22398, BS11200, NIST 800-53, NIST 800-61 and others
- Understanding leadership's direction and buy-in in the organisation's resilience posture
- Identifying capability gaps that may limit a timely response and define areas for improvement

**Capability Validation**

- End-to-end testing of an organisation's crisis response, from detection to recovery, including communication and stakeholder management
- Bespoke toolkits for delivering training and exercising
- Tailored recommendations for continuous improvement to achieve desired maturity level

**Capability Development**

- Resilience roadmap development based on identified exercise findings (incl. delivering further exercising as a programme, developing a resilience programme, building business continuity and incident response capabilities etc.)
- Developing a suite of foundational policies, frameworks, plans and playbooks
- Embedding resilience into day-to-day operations

Through this service clients can achieve the following benefits:

- Improved maturity of the organisation’s resilience and incident response capabilities
- Enhanced operational resilience
- Reduced time needed to respond and recover from cyber incidents, minimising operational and financial impact
- Regulatory compliance and alignment with market leading practices

## 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