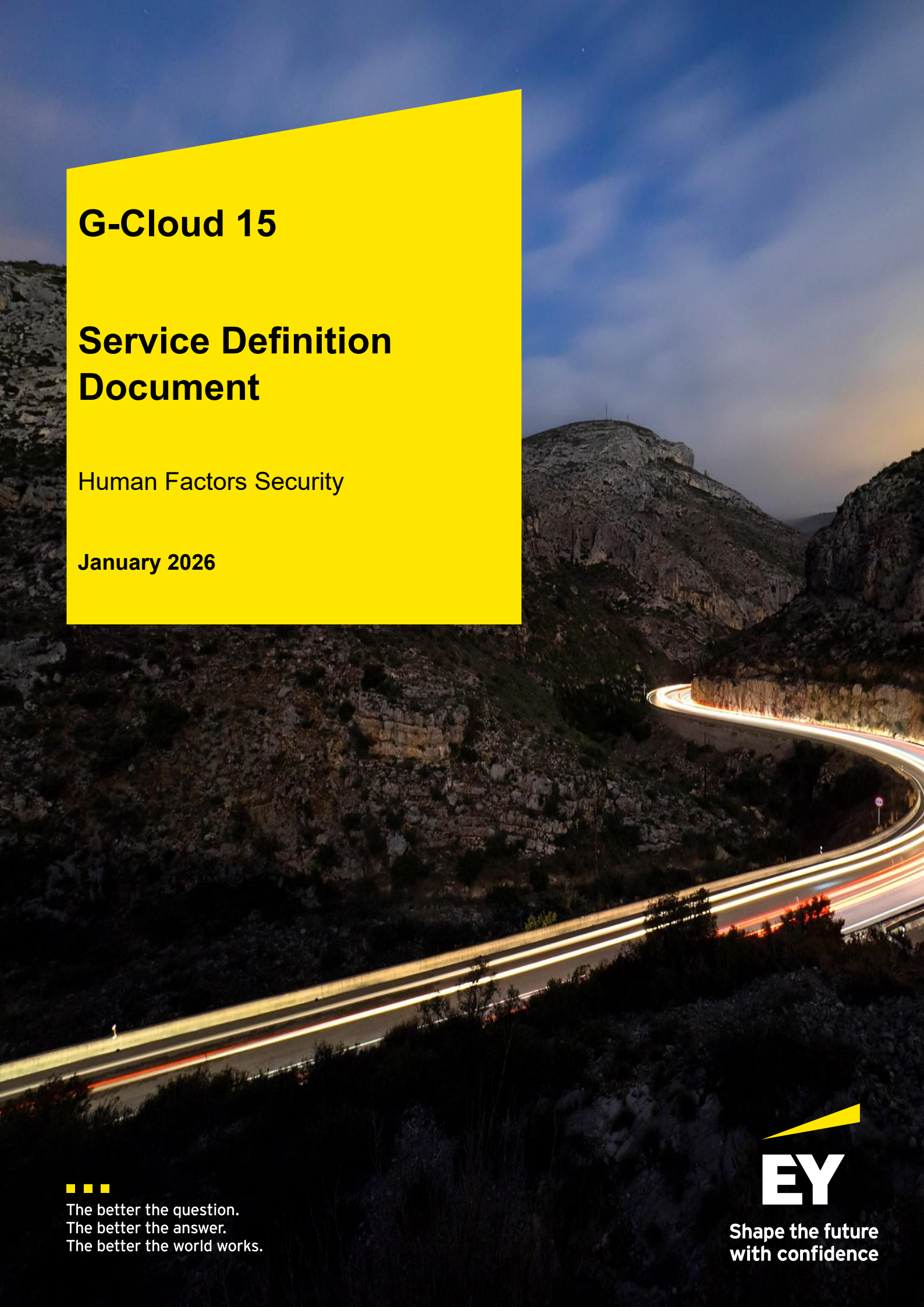

G-Cloud 15

Service Definition Document

Human Factors Security

January 2026

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

Shape the future with confidence

Contents

1. Service detail

Human Factors Security Service

There are seven core components of the EY Human Factors Security Service:

1. **Target Operating Model:** Designing an effective cyber target operating model and supporting organisation design.
2. **Culture and Awareness:** Developing a cyber secure culture, raising awareness, and changing behaviour.
3. **Capabilities and Training:** Developing the right technical and non-technical capabilities at all levels of the organisation.
4. **Organisational Resilience:** Getting the right people in the right place at the right time to build a cyber resilient organisation.
5. **Leadership and Crisis Management:** Developing leadership capability to effectively respond to cyber threats and incidents.
6. **Insider Threat:** Effectively identifying, tackling, and reducing the risk associated with insider threats.
7. **Human-Factor Crisis Communications:** Building capability to communicate effectively internally, externally, and with regulators in times of crisis.

Target Operating Model

- Understand your current cyber operating model and how this aligns with the full organisation operating model
- Identify key areas to strengthen the existing operating model – e.g., strategy and vision, governance, capabilities, processes, structures, etc
- Develop target operating model to strengthen the areas for improvement identified
- Identify dependencies between the different components of the target operating model, such as policies and governance, training, culture and awareness, to ensure its effectiveness
- Develop the implementation roadmap and change management plan to realise the benefits of the target operating model and integrate it with the organisational operating model

Culture and Awareness

- Define current and target culture and levels of awareness
- Utilise the Capability Framework Development (CFD) to identify gaps that need to be addressed and the behaviours that need to change to achieve the target state
- Develop and launch a culture change and awareness programme
- Define metrics needed to measure behaviour change and awareness levels

- Integrate the culture and awareness programme with business as usual - e.g., performance monitoring, governance, programme delivery, etc
- Regularly monitor performance against the target culture and awareness levels using CFD, rewarding positive organisation and individual change

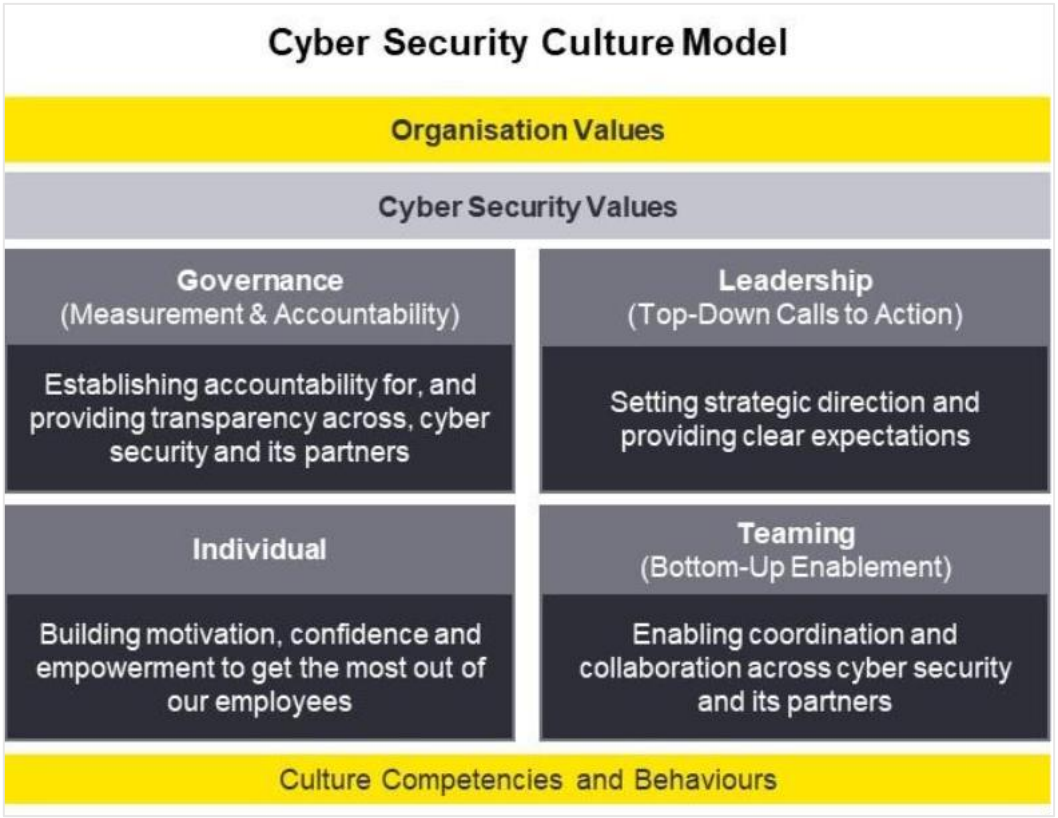

Figure 1 – Cyber Security Culture Model

Capabilities and Training

- Establish current state capability and develop employee personas to inform learning journey development
- Define future capabilities and, using Organisational Capability eXcellence (OCX), establish the gaps to be closed
- Understand the existing learning offer and identify any gaps for uplift
- Design and launch the new learning curriculum in collaboration with our leading cyber training partners, creating learning journeys aligned to employee personas
- Implement a training evaluation process to gather feedback and refine the curriculum post-launch
- Define metrics to measure learning effectiveness

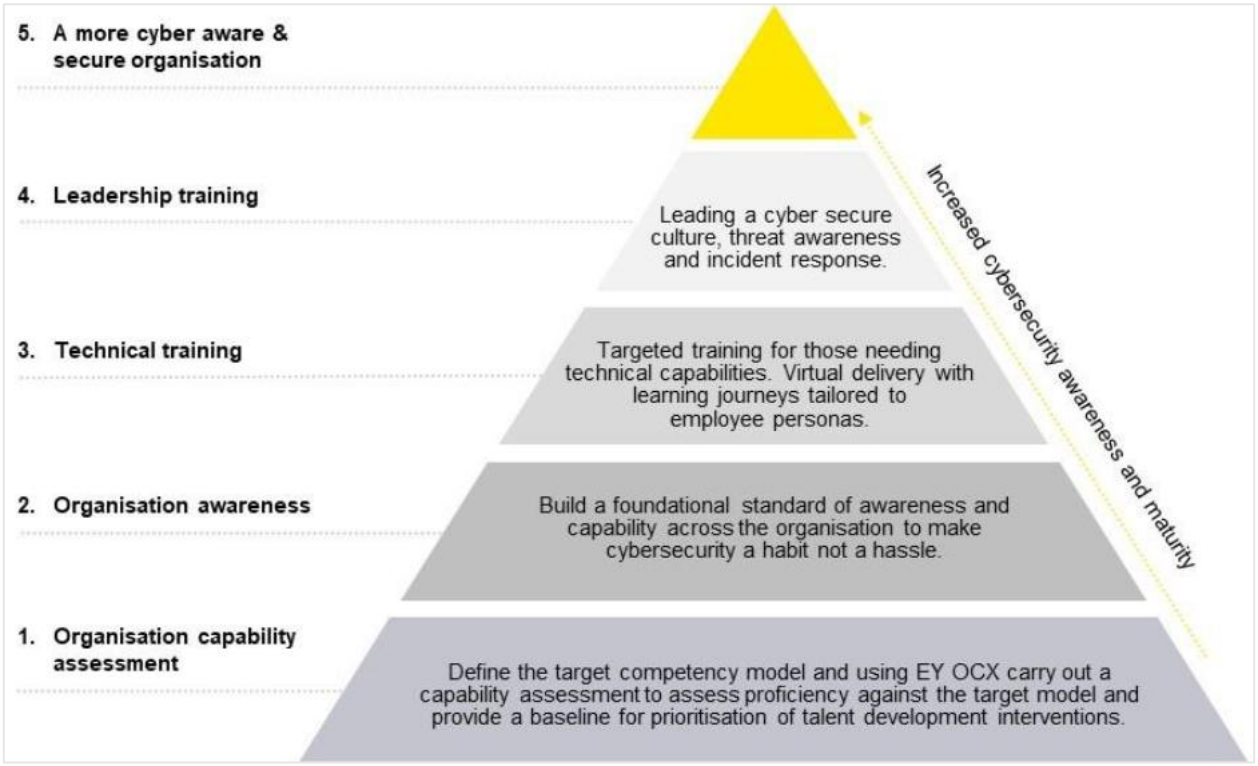

Figure 2 – Cyber Training Pyramid

Organisational Resilience

- Assess the current state of organisational resilience, identifying strengths and weaknesses
- Develop comprehensive plans outlining response strategies for cyber incidents
- Ensure the right people are trained and regularly exercise their roles in crisis scenarios
- Create detailed playbooks for specific incidents, including roles and procedures
- Implement crisis training for teams to enhance decision-making and communication
- Establish protocols for responding to incidents and monitor recovery times
- Leverage technology to support resilience efforts and enhance cybersecurity measures
- Promote a culture of cyber awareness and continuous improvement across the organisation
- Regularly review and adapt strategies based on performance metrics and emerging threats

Leadership and Crisis Management

- Understand the current level of awareness and capability across the leadership population

- Deliver tailored training to give leaders the cyber context and understanding they need
- Run a cyber crisis leadership simulation to test and build leaders' capability to respond
- Define metrics to measure the effectiveness of training interventions and leader response times to simulations
- Evaluate gaps in leadership capability and deliver targeted training interventions to close gaps

Insider Threat

- Understand current policies and practices to identify and manage risks
- Identify gaps and weaknesses in the organisation's approach – e.g., physical security, operating model, culture and awareness, technical capability, etc
- Carry out a risk assessment to identify the most effective ways to close gaps in the insider threat management approach
- Develop a roadmap and specific steps to take in reducing the risk profile
- Carry out periodic review of the risk profile to assess effectiveness in closing the gaps identified

Human-Factor Crisis Communications

- Understand current crisis communications capability and process during human-related cyber incidents
- Define stakeholders who need to be communicated with during a crisis and develop key messages for each group
- Define methods and channels for communication during a crisis, including critical approvals needed
- Review past crisis communications to understand lessons learned
- Develop human factor crisis communications plan so a base template is ready to deploy at short notice
- Run a human factor crisis communications simulation to test capability and deployment readiness
- Evaluate gaps in communications capability, deliver targeted interventions and develop specific communications aids to support more effective future crisis communications

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