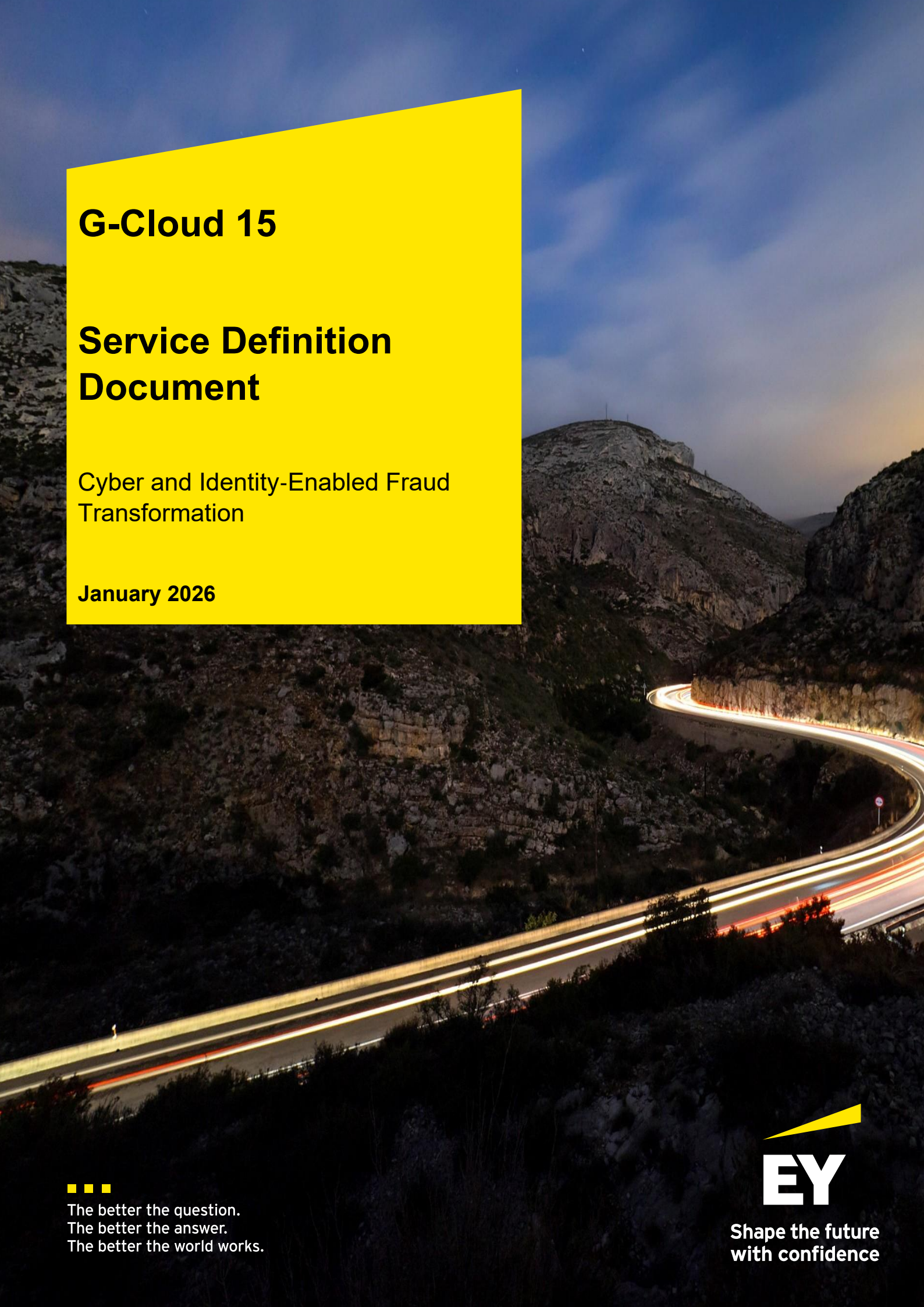


G-Cloud 15

Service Definition Document

Cyber and Identity-Enabled Fraud Transformation

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 and Identity-Enabled Fraud Transformation Service

Identity theft is a key enabler of fraud across digital services, often arising from fragmented identity models, inconsistent controls and misalignment between cyber security, fraud prevention, data and operations.

EY's Cyber and Identity-Enabled Fraud Transformation Service is a consulting service that helps organisations reduce fraud arising from compromised, false or misused identities. The service supports assessment of current arrangements, design of the target state, support for implementation, and embedding of sustainable fraud and identity capabilities. The service takes an identity-first, end-to-end approach, recognising that effective fraud reduction requires coordinated action across strategy, policy, identity, data, technology and operating models. It is modular and scalable, allowing organisations to engage at specific stages of the lifecycle or across the full service as required.

Key Pillars Overview

The delivery framework is applied consistently across a set of core delivery pillars that address the key organisational, technical and operational aspects of identity-enabled fraud:

1. Strategy and Policy: Setting direction, governance and policy frameworks for managing identity-enabled fraud.

2. Data, Risking and Analytics: Improving visibility of identity-enabled fraud risk through data, analytics and risk assessment approaches.

3. Customer Identity and Services: Strengthening how customer identities are defined, represented, delegated and trusted across services and channels.

4. Technology and Architecture: Aligning platforms, integrations and tooling to support effective identity and fraud controls.

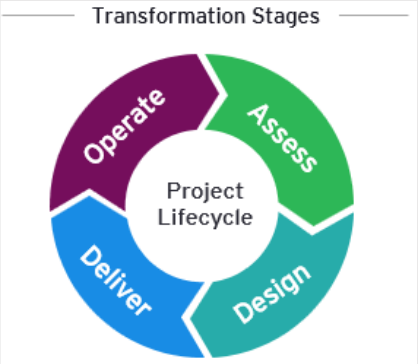
5. Operating Model and Workforce: Transforming roles, responsibilities, skills and ways of working to support sustainable identity fraud management.

Applying the lifecycle consistently across these pillars helps address identity-enabled fraud risks that often arise at the boundaries between strategy, technology and operations.

End-to-End Lifecycle Overview

The service is provided through a comprehensive **Assess, Design, Deliver and Operate** framework, encompassing the entire transformation process from start to finish.

- **Assess:** Understand current identity-enabled fraud risks, controls and capabilities, and identify gaps, constraints and priorities for improvement
- **Design:** Define target approaches, controls, operating models and technical patterns to address identified risks and support effective identity-enabled fraud management
- **Deliver:** Support implementation of agreed changes, including development of artefacts, processes and integrations, and support to procurement and delivery activities where required



- **Operate:** Support embedding, operation and continuous improvement of capabilities, enabling controls, processes and arrangements to remain effective as services, threats and user needs evolve

Delivery and Transformation Approach

Our approach to identity fraud delivery and transformation is based on a framework for delivering measurable outcomes in a fast-moving threat environment. It combines iterative **lifecycle delivery**, an **identity-first and technology agnostic mindset**, **human centred change** to support effectiveness, sustainability, and adaptability of solutions over time.

Iterative, Lifecycle-Based Delivery

The service is delivered using an **Assess, Design, Deliver and Operate** framework applied consistently across all delivery pillars. This framework is intentionally **iterative**, recognising that identity enabled fraud risks, controls and service needs evolve over time. Insights, lessons learned and performance data gathered during **Operate** feed back into **Design**, **Assess** and **Deliver**, enabling continuous refinement of strategies, controls, identity models and operating arrangements rather than one-off change.
The visual below illustrates how each delivery pillar evolves across the lifecycle, and how feedback from live operation informs ongoing improvement.

Lifecycle stages

Delivery pillars

	Assess	Design	Deliver	Operate
Strategy and Policy	Review the organisation's current approach to managing identity-enabled fraud, including strategic objectives, policy frameworks and governance arrangements, and identify gaps, risks and areas for improvement.	Facilitate collaborative design sessions to define a direction for identity-enabled fraud management, including objectives, priorities, success measures and alignment with wider organisational strategies.	Support implementation of the agreed strategy, including development of supporting policy, governance artefacts and a communications approach to enable awareness, adoption and consistent application.	Support ongoing review and iterative improvement of the strategy and associated policies, and enable continued alignment through established governance, assurance and decision-making forums.
Data, Risking and Analytics	Assess identity-enabled fraud risk across platforms and business processes to identify gaps in controls and capabilities, and review alignment with relevant regulatory and risk frameworks.	Design approaches to providing risk visibility, including dashboards and data requirements. Define a repeatable identity fraud risk assessment process incorporating threats and vulnerabilities.	Support implementation of improved data, analytics and risking capabilities, including continuous control monitoring and cyber risk quantification.	Support ongoing operation, optimisation and tuning of data, analytics and risking capabilities, including continuous control monitoring and cyber risk quantification, to maintain effectiveness as risks evolve.
Customer Identity and Services	Assess how customer identity is currently defined, represented and used across services, including identity attributes, authority to act, delegation and federation arrangements. Identify gaps, risks that enable fraud.	Design target customer identity models and patterns, including definitions of identity, representation and authority, approaches to delegation and federation, and how identities are linked and trusted across services and platforms.	Support implementation of the agreed identity models and patterns across services, including integration with existing platforms, and alignment with standards, policies and controls.	Support ongoing operation and evolution of customer identity models, including refinement of delegation and federation arrangements, and assurance that identity services continue to meet fraud, security and user requirements.
Technology and Architecture	Assess the current technology landscape supporting identity-enabled fraud management, including tooling, identity and access controls, system integrations and end-to-end data flows. Identify gaps and risks that limit effectiveness.	Design target functional and technical architectures to support identity-enabled fraud controls, including definition of the functional model, requirements and a roadmap for moving from the current state to the target state.	Provide support through technology procurement and implementation activities, including guidance on requirements, vendor evaluation and integration of agreed solutions.	Support monitoring of tooling and architectural effectiveness over time, including assessment of performance, control coverage and value delivered, and identify opportunities for optimisation and improved return on investment.
Operating Model and Workforce	Assess the current operating model and workforce capabilities supporting identity-enabled fraud management, including roles, responsibilities, skills, capacity and dependencies across teams and services.	Design a target operating model and workforce plan, including role definitions, capability requirements and a roadmap covering recruitment, onboarding and capability development.	Support delivery of the workforce plan, including development of role profiles and job descriptions, and support delivery of training and awareness activities to build capability across relevant teams.	Support ongoing evaluation of workforce capability and operating effectiveness, including skills assessment, coaching, and development of learning and training approaches to sustain and evolve capability over time.

The approach is also designed to work within existing governance and assurance structures and to scale according to organisational need. Clients can engage:

- At a single lifecycle stage (for example, ***Assess*** or ***Design*** only), or
- Across multiple stages to support end-to-end transformation and embedding

This flexibility supports both targeted improvements and broader transformation programmes addressing identity-enabled fraud across services.

Identity-First and Technology-Agnostic

The delivery approach is **identity-first**, focusing on how identities are defined, represented, delegated and trusted across services. This enables organisations to address fraud risks at source rather than treating them only as downstream issues.
The service is **technology-agnostic and vendor-neutral**. It supports informed decision-making and integration with existing platforms, services and teams, enabling organisations to strengthen controls and capabilities without requiring replacement of current solutions.

Human-Centred Transformation

Effective fraud and identity transformation depends on people as well as processes and technology. The service applies **human-centred change principles**, emphasising:

- Clear ownership, roles and accountability
- Engagement of affected teams and stakeholders throughout delivery
- Practical enablement through training, coaching and learning
- Progressive adoption rather than disruptive one-off change

This approach helps facilitate understanding, embedding and sustaining of changes, taking people on a clear journey from current to target ways of working.

Expected Deliverables, Outcomes and Benefits

The Cyber and Identity-Enabled Fraud Transformation Service helps organisations strengthen their ability to prevent, detect and respond to fraud arising from compromised, false or misused identities. It delivers practical improvements across identity, fraud, cyber security and operations, while maintaining a clear focus on value, sustainability and measurable outcomes.

The following are **illustrative examples of deliverables** that may be produced during an engagement. They are indicative only, and not all outputs will be required or delivered in every case. Example deliverables may include:

- Identity-enabled fraud risk assessments
- Identity fraud kill chain development and mapping across services or user journeys
- Current-state capability and control assessments
- Target-state identity and fraud control frameworks
- Identity fraud-focused architecture and design views
- Operating model and governance designs
- Operational processes, playbooks and procedures
- Metrics, dashboards and reporting for identity fraud risk and control effectiveness
- Roadmaps, prioritised backlogs and transition plans

- Business case, benefits and value realisation artefacts
- Training, enablement and knowledge-transfer materials

Typical Outcomes and Benefits

Clients can expect outcomes including:

- Improved understanding and management of identity-enabled fraud risk, with clearer visibility of risks, control gaps and dependencies across services and channels
- Stronger and more consistent identity controls, including clearer definitions of identity, representation and authority, and improved handling of delegation and federated identities
- Better-informed decision making, supported by improved use of data, analytics and risk insights to prioritise actions and investments
- More effective and sustainable delivery, with aligned approaches, operating models, technology and workforce capabilities designed to be embedded and continuously improved
- Reduced delivery and implementation risk through a technology-agnostic, vendor-neutral approach that integrates with existing platforms and services
- Greater engagement and adoption, supported by human-centred change approaches that build skills, ownership and confidence across affected teams

Focus on Value and Measurable Outcomes

Throughout delivery, there is a focus on value realisation, measurable outcomes and evidence-based decision making. The service is designed not only to improve cyber and fraud capabilities, but also to help organisations build credible investment cases, secure funding and **demonstrate return on investment (ROI)** at each stage of the transformation.

From the outset, delivery establishes an evidence-based view of identity-enabled fraud risk, control effectiveness and key cost drivers. Early assessment activities generate outputs such as **quantified identity fraud-risk exposure** and clear articulation of the **financial, operational and reputational impacts** of inaction. These outputs are structured to directly support internal business cases, scorecards and investment submissions, enabling decision-makers to prioritise funding based on risk reduction.

As the service progresses through design and delivery, initiatives are translated into benefit statements that link investment directly to outcomes such as reduction in identity fraud losses. Measures are defined upfront and tracked consistently, providing a clear line of sight **between what is delivered, how it reduces risk, and how it delivers value**.

In addition, rather than relying on large, multi-year transformation programmes, the service supports incremental, prioritised delivery. This enables **early realisation of benefits** from high-impact areas and the ability to refine investment priorities as risk patterns evolve. This approach allows organisations to demonstrate progress and value early, strengthening confidence for subsequent funding rounds.

Once new capabilities are implemented, delivery transitions to ongoing performance and value monitoring, including monitoring of realised versus expected benefits. This enables organisation to demonstrate that **value is not only delivered, but sustained over time**, supporting both operational accountability and future investment decisions.

Overall, clients can expect a transformation approach that delivers measurable outcomes, supports robust investment cases, and provides senior stakeholders with the confidence needed to transform and sustain identity fraud management capabilities.

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