

G-Cloud 15

Service Definition Document

Security Architecture

January 2026



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



**Shape the future
with confidence**

Contents

Contents	1
1. Service detail	2
2. Key contacts	5

1. Service detail

Security Architecture Service

Our Security Architecture Service provides review, design, implementation, engineering and assurance across the key components of your cloud platforms and workload.

We assess governance, build-time security, run-time security and operational readiness, aligning to the National Cyber Security Centre's (NCSC's) 14 Cloud Security Principles and EY's Enterprise Architecture Principles. Our approach applies Zero Trust by design; strengthens identity, data and platform protections and integrates cloud-native detection and response with SIEM/SOAR and incident playbooks.

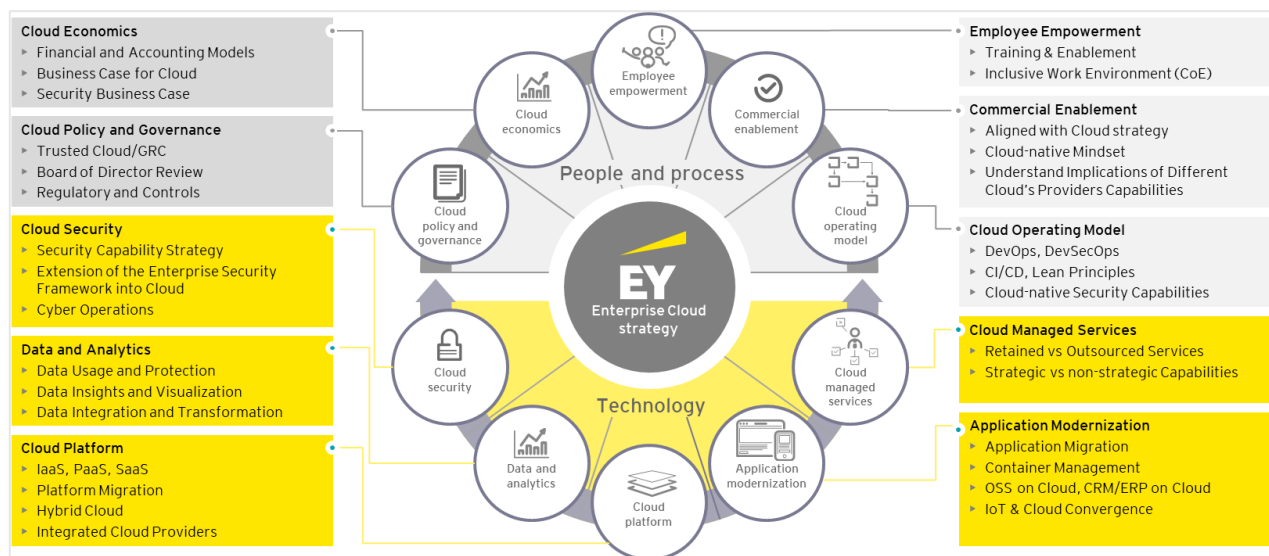


Figure 1 – Enterprise Security Strategy

Our cloud security professionals can advise on a range of topics, and we have delivered projects that cover an array of cloud capabilities. The seven categories below provide a summary of the activities we undertake.

Extension of the Enterprise Security Strategy and Framework into Cloud

- Strategy and vision for secure-by-design cloud adoption
- Accountability and oversight (service ownership, shared-responsibility model, RACI)
- Policy and standards management with policy-as-code and exception handling
- Legal and regulatory management
- AI risk and governance
- Technology risk management
- Security controls mapping to enterprise framework
- Cloud security operating model and alignment with cloud CoE
- Maturity assessment and gap analysis workshops to prioritise improvement remedial work

- Roadmap for post-quantum cryptography

Cloud Security Framework & Controls

- Cloud Security Controls Framework (CSF) tailored to the risk profile
- CSF alignment with enterprise architecture and risk frameworks
- Control-by-control traceability
- Technical reference architecture with options for future expansion
- Security baseline
- AI control set
- Secure configuration practices
- Security guardrails for IaaS, PaaS and SaaS with integration into CI/CD workflows

Cloud Security Assessment

- Diagnostics and root cause analysis of misconfigurations, identity risks and data exposure
- AI/ML security assessment
- Post-quantum readiness assessment
- Comprehensive assessment of risks and vulnerabilities
- Risk-based vulnerability management
- Penetration testing and vulnerability assessment.
- Architectural Risk Assessment (ARA)
- Current state assessment with practical recommendations for secure target state
- Operational readiness and enablement

Architecture and Engineering

- Cybersecurity product augmenting cloud-native controls - vendor selection criteria definition and assessment
- CSPM tools enablement and post-implementation support
- Supply chain integrity and code signing
- Zero Trust design including privileged access control
- Workload protection tool assessment and enablement
- Infrastructure-as-code security

- Identity as new perimeter
- Network, platform and application controls (micro segmentation, application allow listing, secrets management)
- Policy-as-code support with preventative, detective and auto-responsive guardrails

Monitoring and Incident Response

- Specification of cloud security events and use cases
- Threat modelling
- Attack path analysis
- AI in SOC
- SOC integration - cloud detection and response, SIEM/SOAR tuning
- Incident Response (IR) playbooks, Threat and Vulnerability Management (TVM) using cloud-native and third-party tools and services
- Hybrid cloud monitoring and alerting

Platform and Apps Readiness

- 'Path to production' assurance per CSF
- Platform baseline
- Application migration enablement e.g. DevSecOps
- AI deployment readiness
- Change management with released gating
- Environment hardening checklist

Cloud Security Audit

- Internal audit support for cloud security audits and assessments with evidence packs
- Readiness assessment against enterprise standards e.g. ISO27000 family

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