

G-Cloud 14

Service Definition Document

Security Architecture

May 2024

Contents

1. Introduction	2
2. Service detail	4
3. Key contacts	9

1. Introduction

EY is delighted to participate in the latest release of the G-Cloud framework. We have been a supplier through G-Cloud since its inception and, in line with digital trends, have evolved our services over this time.

Digitalisation strategies and adoption of cloud technologies are a core enabler in tackling today's challenges such as energy transition and net zero, cyber-security and data loss, workforce skills gap, and ethical and regulatory changes. With enterprise technology evolving at an unprecedented pace, it is critical to work with a partner that can help you navigate these challenges and that brings an in depth understanding of how to leverage the broader technology ecosystem (e.g. ServiceNow, Microsoft, SAP) and emerging technologies (e.g. AI, Augmented Reality) in the context of cloud solutions to do so.

With 135,000 consultants globally, of which 17,000+ are cloud professionals providing services across Azure, AWS, GCP, IBM and Alibaba Cloud, we support all aspects of digital business transformations pivoting around cloud. We deliver end to end services from cloud strategy and migration to solving specific business challenges through building cloud native digital solutions. These technology-driven services are supplemented by our business and people capabilities allowing for holistic transformational change and adoption.

EY offers a range of cloud services that help organisations globally to modernise their business core, build data centricity and connect distributed ecosystems (see Figure 1):

Data modernisation through cloud -

Migrate data to cloud, transform data foundations with intelligent cloud data platforms and infuse AI to accelerate and optimise operations and workflows such as our Advanced Analytics and Data Science service;

Distributed cloud - Develop, deploy and manage distributed architectures across multiple public clouds and edge, building resiliency, security and compliance such as our Cloud Strategy and Architecture service.

Industry cloud - Accelerate speed to market with EY industry clouds, through sector-specific use cases and opportunities to co-create solutions with industry specialists and ecosystem partners such as Microsoft, SAP and ServiceNow.

Sustainability cloud - Design cloud solutions that reduce carbon emissions and embed energy-efficient architecture and methods into cloud-based solutions such as our Microsoft Sustainability Manager solution.

Trusted cloud - Embed strong governance into cloud architecture that helps you comply with rapidly evolving legal and regulatory requirements.

Cloud economics - Create transparency on your cloud consumption and strengthen governance of costs and controls, enabling data-driven decisions and optimisations.

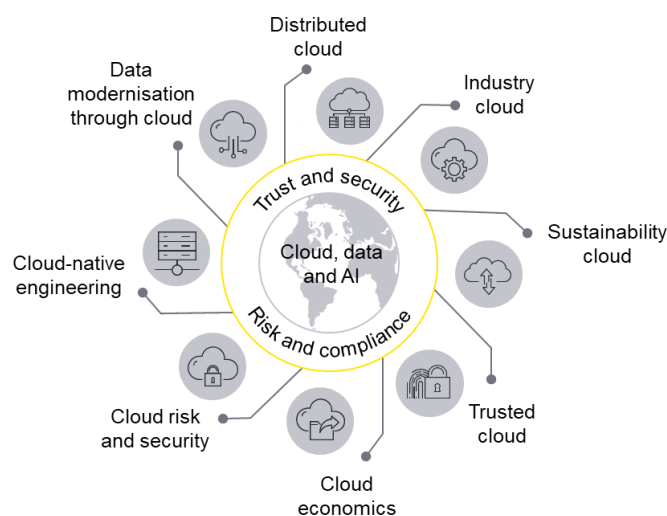


Figure 1 - EY Global Cloud Services

Cloud risk and security - Secure trust in critical business applications and data platforms hosted in multi-cloud environments from the onset, enabling innovation and transformational change.

Cloud-native engineering - Develop and deploy data and insights-driven microservices and composable architectures, enabled by industrialised DevOps.

For G-Cloud 14, we have curated a range of services grouped into themes (see Figure 2) which align to our Global Cloud Services and that can be procured separately or together to meet your specific requirements.

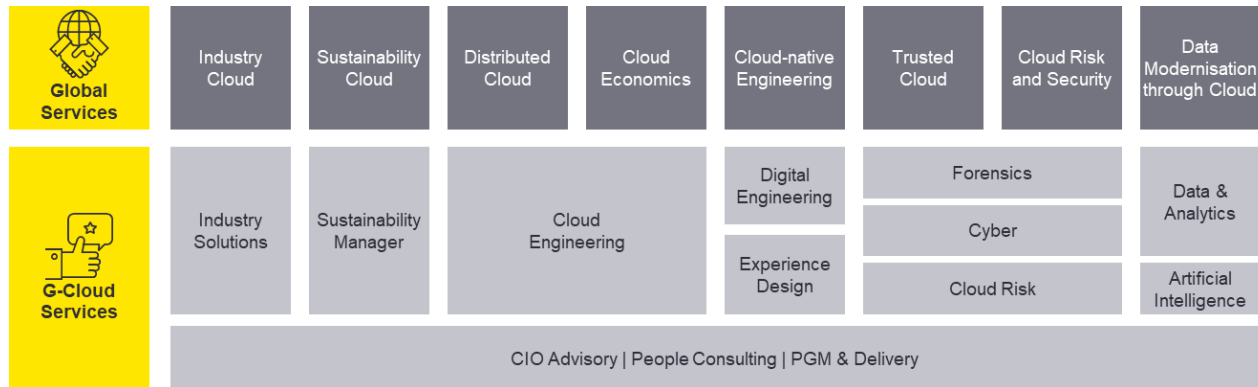


Figure 2 - EY G-Cloud 14 Service Themes

EY has been recognised as a:

- ✓ Leader in the Gartner Magic Quadrant for completeness of vision and ability to execute and have scored highest in Strategy and Consulting, Data Management and Governance Use Cases.
- ✓ Leader in Cloud Security and Microsoft Implementation Services by IDC MarketScape
- ✓ Top cloud professional services provider, based on an analysis of our capabilities and strategies by IDC MarketScape
- ✓ Leader in the 2023 Cloud Services in Insurance PEAK Matrix by Everest Group

2. Service detail

2.1. Introduction to the Service

EY enables secure cloud transformation journeys by orchestrating cloud and technology providers as well as providing the required security services for compliant and resilient cloud business models. We deliver positive security transformation to the business through the design or review of cloud service architecture ensuring it meets business need and requirements for security, risks mitigation and conforms to the relevant policies and regulations, while balancing information and business risk against cost of controls.

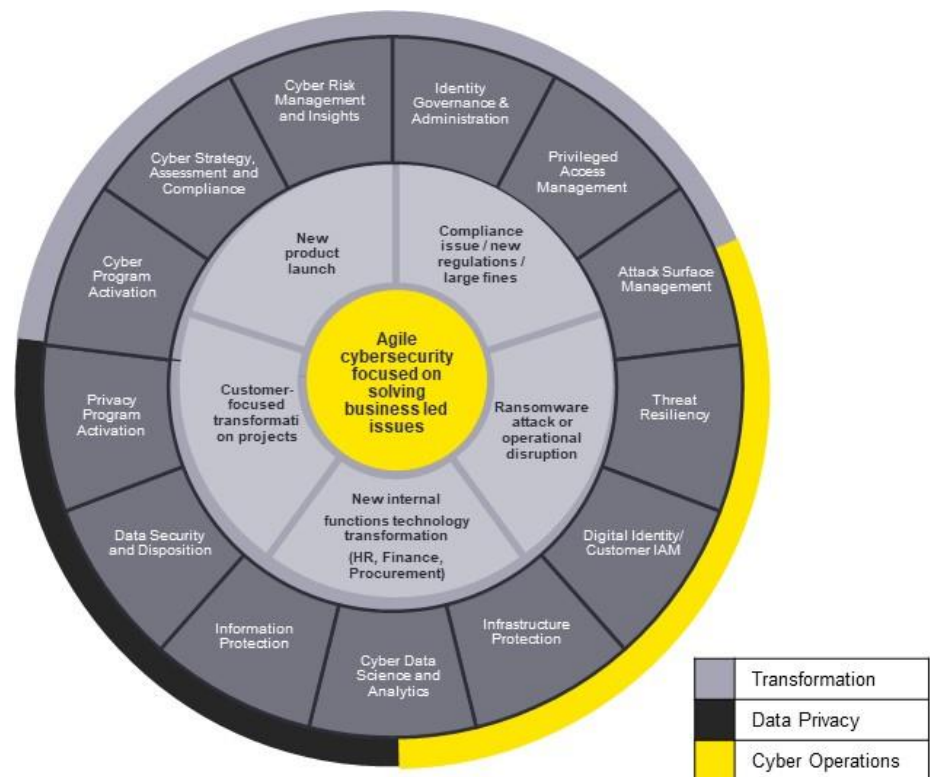


Figure 3 - EY Cyber Services

The components of this service are:

- ▶ Cloud Security Governance
- ▶ Security Capability and Cyber Strategy
- ▶ Extension of the Enterprise Security Framework into Cloud
- ▶ Cyber Operations
- ▶ Cloud Security Assessment
- ▶ Architecture and Engineering
- ▶ Cyber Resilience
- ▶ Platform and Apps Readiness
- ▶ Human Factors Security
- ▶ Cyber Board Advisory
- ▶ Cloud Security Audit

Through this service clients can achieve the following benefits:

- ▶ Compliance to industry and government cloud security standards
- ▶ Security architecture assessment and maturity review of the cloud services
- ▶ Consistent process across cloud providers and business units
- ▶ Effective cloud governance
- ▶ Regulatory compliance integrated to design and review
- ▶ Information security risk assessment and assurance
- ▶ Resilient cloud infrastructure design and review
- ▶ Alignment of cloud security strategy with the core information security strategy
- ▶ Defined cloud security patterns based on standards and leading practices

EY Cybersecurity supports trust in systems, design and data, so organisations can take more risk, make transformational change and enable innovation with confidence. EY teams accomplish the mission by developing solutions that can be used to assure security and resilience of key business transformation initiatives and/or business functions. These solutions are built using talent, experience and capability resident within the 5 competencies.

Security Strategy, Risk, Compliance and Resilience - This set of solutions helps organisations evaluate the effectiveness and efficiencies of their cybersecurity and resiliency programs in context of the business growth and operations strategies. The solutions apply consistently regardless of where they are applied (IT, IoT, OT, Cloud), provide clear measurement of risk and capture current risks to the organisation and demonstrate how cyber risks will be managed going forward. Each service can be combined to form a larger program or transformation effort.

Data Protection and Privacy - EY data protection and privacy services and solutions are designed to help organisations protect their information over the full data lifecycle – from acquisition to disposal. EY service offering helps organisations stay up to date with data security and data privacy good practices, as well as compliancy with regulation, in a constantly evolving threat environment and regulatory landscape. In the event of misuse or breach of personal information, the services can help companies forensically identify the scope and nature of the misuse or breach, and take steps to remediate and report on the event.

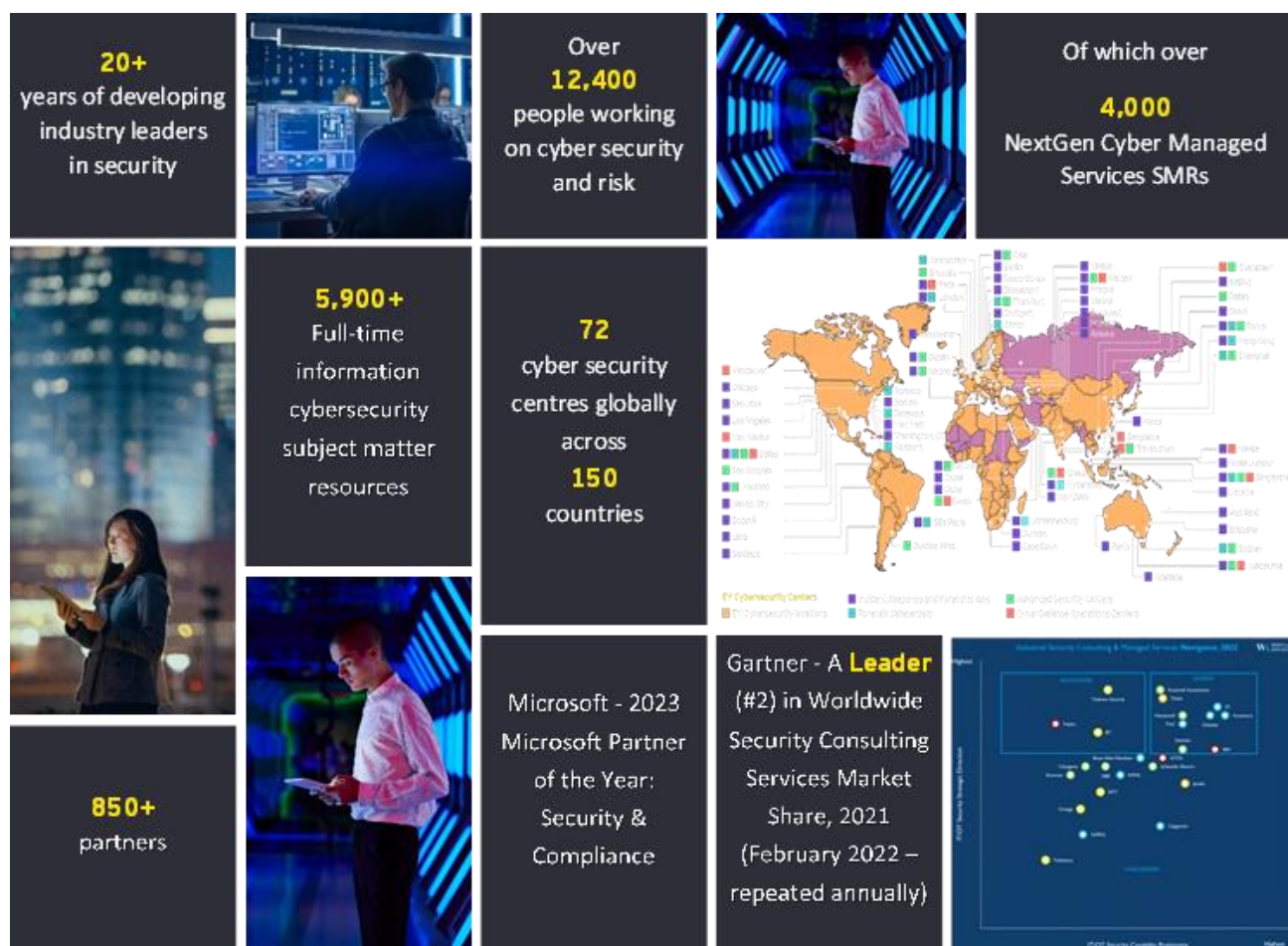


Figure 4 - EY UKI Cyber Key Metrics

Identity and Access Management (IAM) - This set of solutions helps support organisations with their definition of access management strategy, governance, access transformation

and ongoing operations. IAM includes the processes and technologies collectively used to manage the lifecycle of digital identities (profiles) for people, systems, services and users, and is a crucial part of keeping a client's data and key resources protected from cyber attacks and limited to only those who should have access.

Security Architecture, Security Engineering, and Emerging Technologies - EY security architecture, security engineering, and emerging technologies services and solutions are designed to help companies protect their organisations from adversaries that would seek to exploit weaknesses in the design, implementation, and operation of their technical security controls, including disruptive technologies in the marketplace (e.g., cloud computing, blockchain, internet of things (IoT)/industrial control systems (ICS) devices, connected automotive, robotic process automation (RPA), etc.)

Next Generation Security Operations and Response - EY next generation security operations and response services along with a deep portfolio of advisory, implementation and managed services, can help clients build a transformation strategy and roadmap to implement the next generation of security operations, and provide the right amount of support to help you manage leading class security operations in a programmatic way.

Alliances

At EY, we deliver long-term value to our clients and society with our Alliance & Ecosystem Relationships by enabling secure transformations through integrated delivery of cybersecurity with other capabilities.

In today's complex cyber risk landscape, our clients need and value comprehensive reliable cybersecurity strategies and operations. EY stands out for its ability to create value for clients through future-proofed technology, that enable business outcomes, via our alliance ecosystem orchestration.

EY cyber professionals work closely with our alliance partners to combine transformational consulting experience with leading technologies. Together, we help businesses create dependable capable safeguards and strategies to detect, respond to and prevent, potential cyber attacks.

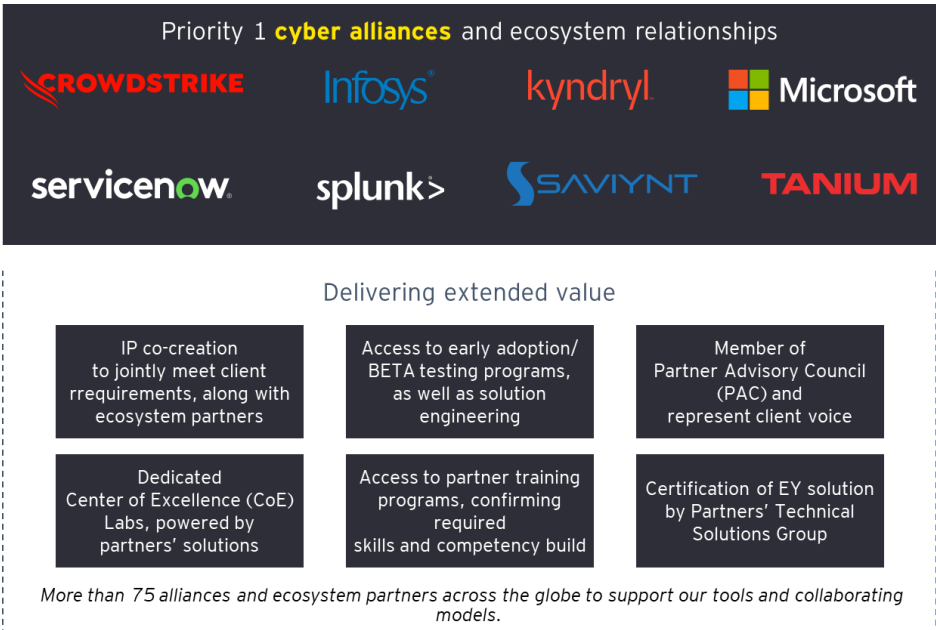


Figure 5 - EY Cyber Key Alliance Partners

2.2. Service Description

Security Architecture

Our security architecture services provide review, design, implementation and assurance across the key components of your cloud systems. Broadly, our reviews will consider the governance, build time security, runtime security and operational readiness of the cloud systems. Our security architecture services are aligned to wider EY enterprise architecture principles.



Figure 6 - Enterprise Cloud 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 have been asked to undertake.

Extension of the Enterprise Security Strategy and Framework into Cloud

- ▶ Strategy and Vision
- ▶ Accountability and Oversight
- ▶ Policy Management
- ▶ Legal and Regulatory Management
- ▶ Technology Risk Management
- ▶ Cloud Security Operating Model and Alignment with Cloud CoE
- ▶ Workshop for maturity and gaps mapping

Cloud Security Framework & Controls

- ▶ Cloud Security Controls Framework (CSF)
- ▶ CSF alignment with enterprise architecture and risk frameworks
- ▶ Reference Architecture
- ▶ Security Baseline
- ▶ Patterns
- ▶ Security Guardrails for IaaS, PaaS and SaaS

Cloud Security Assessment

- ▶ Diagnostics and root cause analysis
- ▶ Comprehensive assessment of risks and vulnerabilities

- ▶ Pen testing and Dark Web Search
- ▶ Architectural Risk Assessment (ARA)
- ▶ Operational Readiness and Enablement

Architecture and Engineering

- ▶ Cybersecurity product augmenting cloud-native controls – vendor selection and rollout
- ▶ CSPM tools enablement and post-implementation support
- ▶ Workload protection tool enablement
- ▶ Infrastructure-as-code security
- ▶ Identity as new perimeter
- ▶ Network, platform and application controls
- ▶ Policy-as-code support
- ▶ Preventative, detective and auto-responsive guardrails

Monitoring and Incident Response

- ▶ Specification of Cloud security events and use cases
- ▶ Threat Modelling
- ▶ SOC Integration
- ▶ Incident Response (IR), 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
- ▶ Application migration enablement

Cloud Security Audit

- ▶ Internal Audit support for Cloud Security audits and assessments

3. 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.

© 2024 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