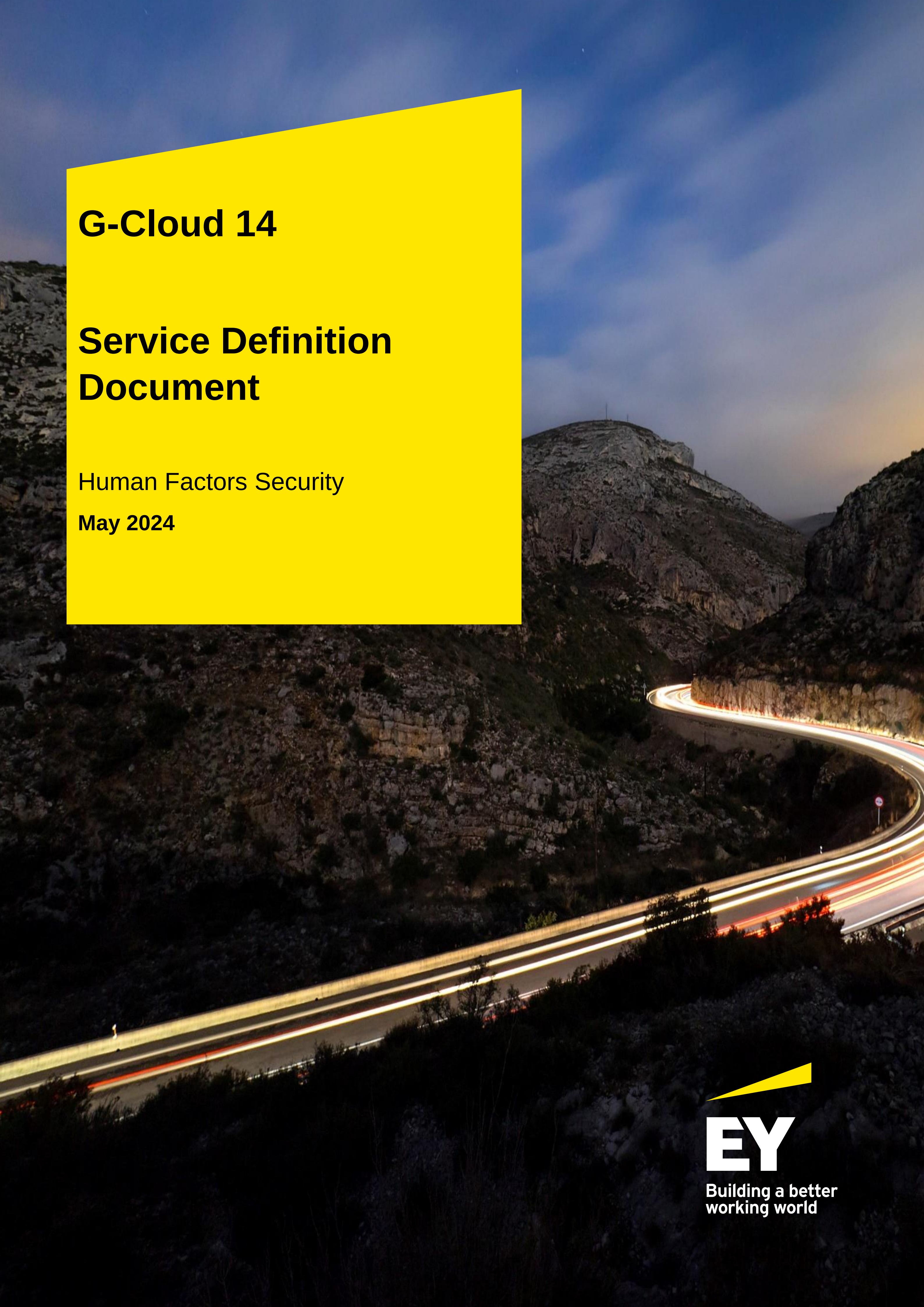


G-Cloud 14

Service Definition Document

Human Factors Security

May 2024

Building a better working world

Contents

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):

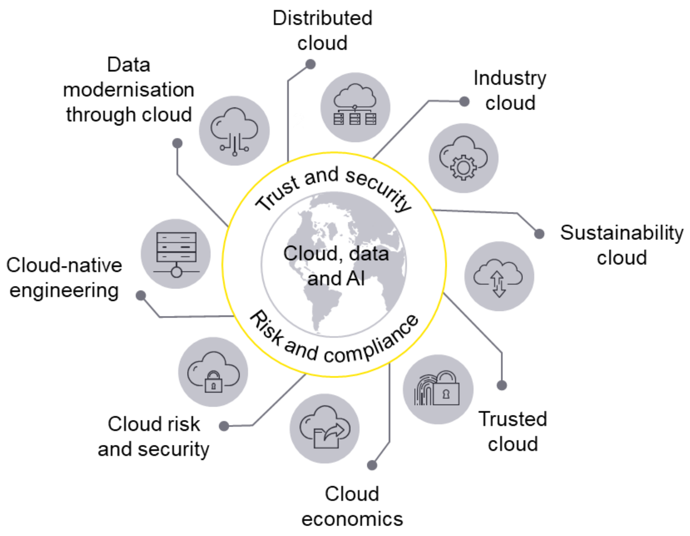


Figure 1 - EY Global Cloud Services

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.

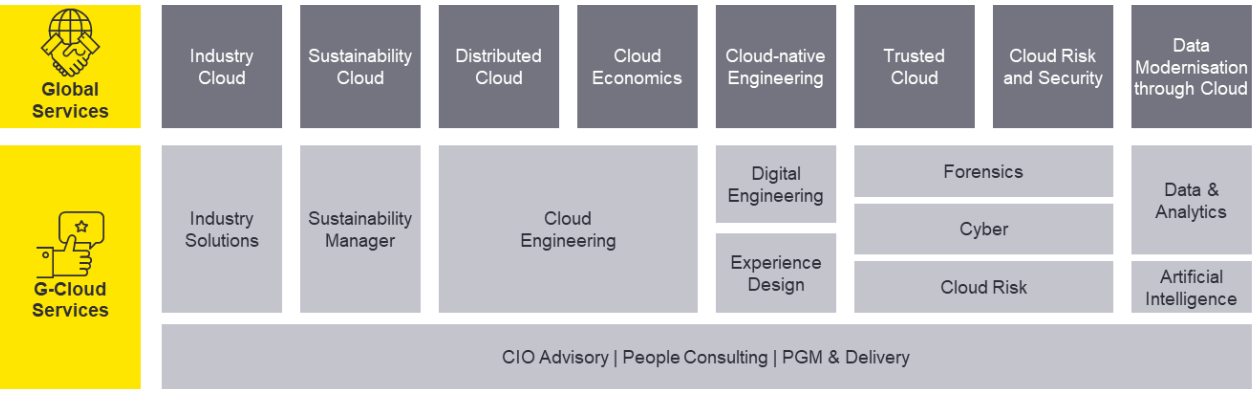
Trusted cloud - Embed strong governance into cloud architecture that helps you comply with rapidly evolving legal and regulatory requirements.

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

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.



Global Services

Industry Cloud

Sustainability Cloud

Distributed Cloud

Cloud Economics

Cloud-native Engineering

Trusted Cloud

Cloud Risk and Security

Data Modernisation through Cloud

G-Cloud Services

Industry Solutions

Sustainability Manager

Cloud Engineering

Digital Engineering

Experience Design

Forensics

Cyber

Cloud Risk

Data & Analytics

Artificial Intelligence

CIO Advisory | People Consulting | PGM & Delivery

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.

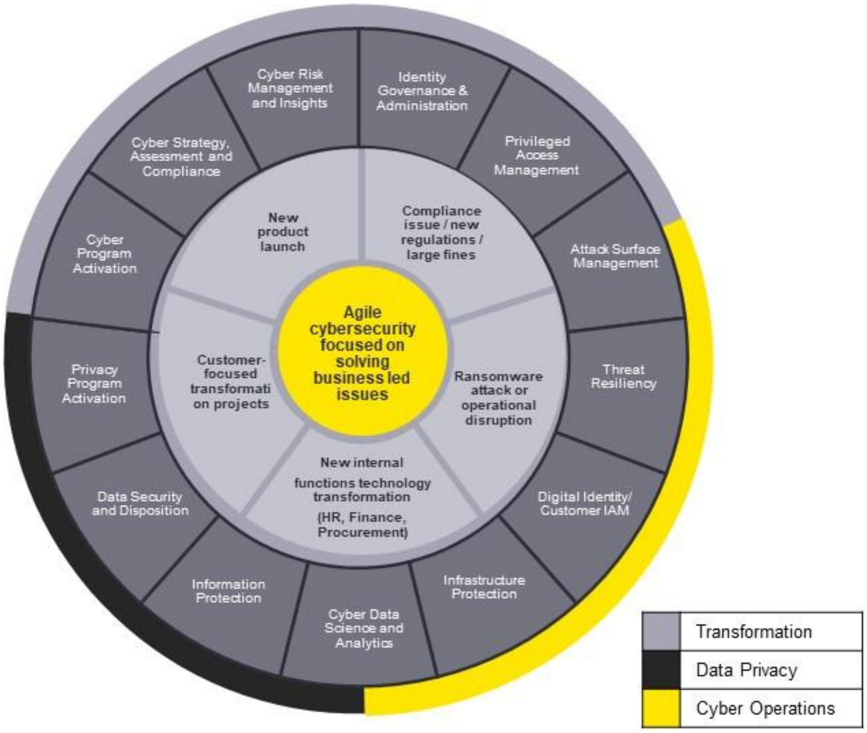

Agile cybersecurity focused on solving business led issues
New product launch
Compliance issue / new regulations / large fines
Ransomware attack or operational disruption
New internal functions technology transformation (HR, Finance, Procurement)
Customer-focused transformati on projects
Cyber Risk Management and Insights
Identity Governance & Administration
Privileged Access Management
Attack Surface Management
Threat Resiliency
Digital Identity/ Customer IAM
Infrastructure Protection
Cyber Data Science and Analytics
Information Protection
Data Security and Disposition
Privacy Program Activation
Cyber Program Activation
Cyber Strategy, Assessment and Compliance
Transformation
Data Privacy
Cyber Operations

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.

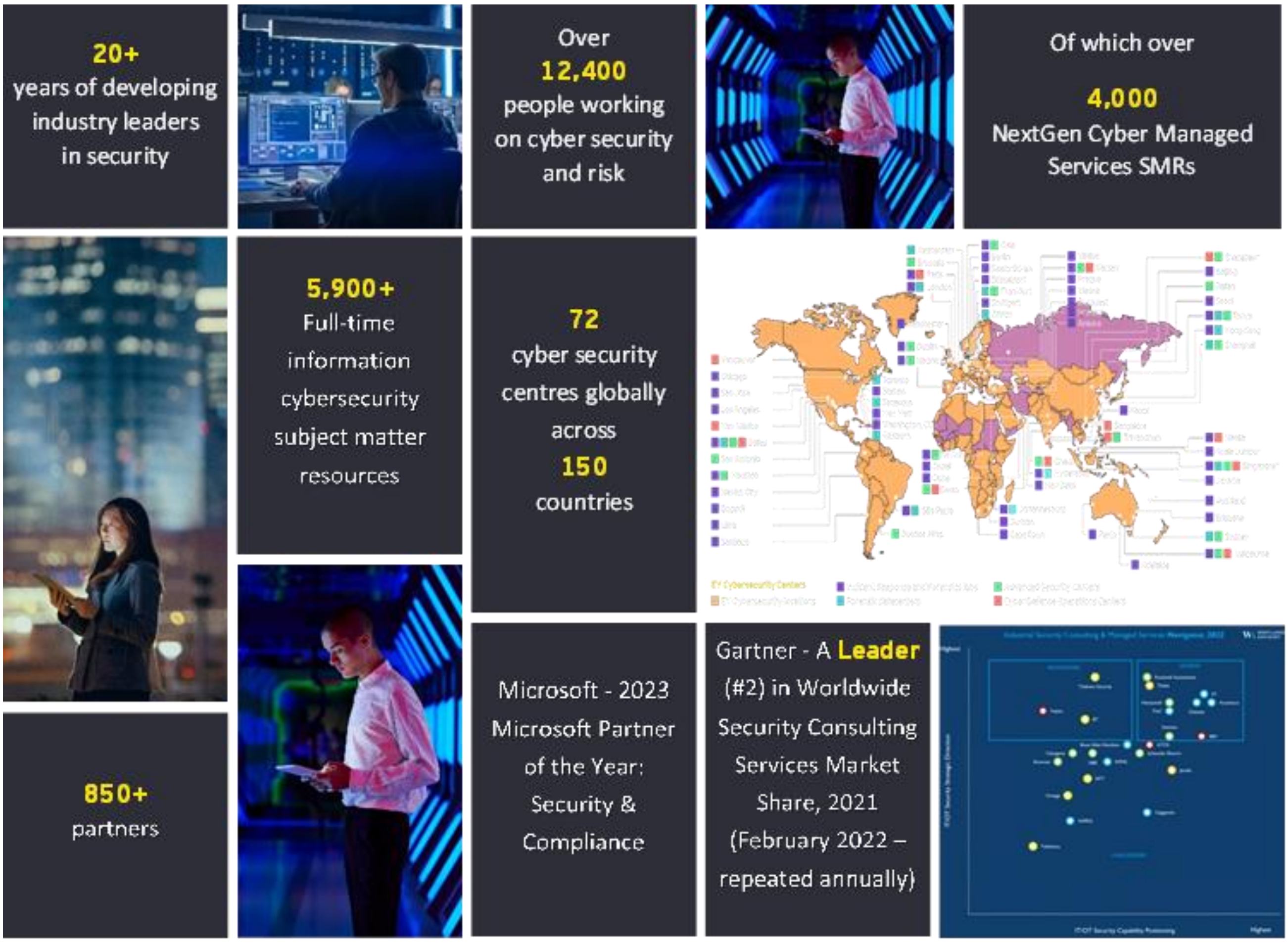

20+
years of developing industry leaders in security
Over
12,400
people working on cyber security and risk
Of which over
4,000
NextGen Cyber Managed Services SMRs
5,900+
Full-time information cybersecurity subject matter resources
72
cyber security centres globally across
150
countries
850+
partners
Microsoft - 2023 Microsoft Partner of the Year: Security & Compliance
Gartner - A Leader (#2) in Worldwide Security Consulting Services Market Share, 2021 (February 2022 – repeated annually)

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.)

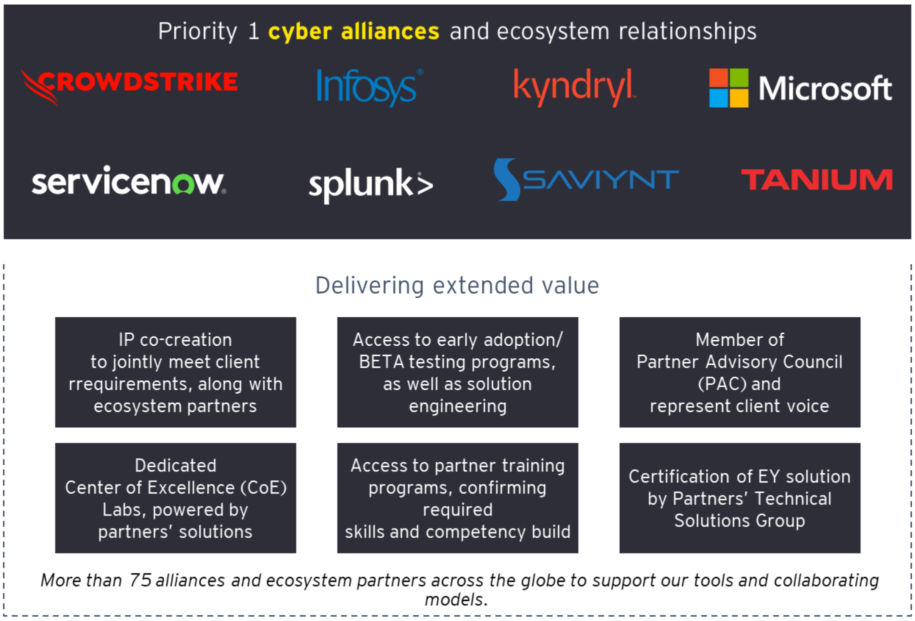
Next Generation Security Operations and Response - EY next generation security operations and response services along with a deep portfolio of advisory, implementation and managed services, can help clients build a transformation strategy and roadmap to implement the next generation of security operations, 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.



Priority 1 **cyber alliances** and ecosystem relationships

Delivering extended value

IP co-creation to jointly meet client rrequirements, along with ecosystem partners

Access to early adoption/ BETA testing programs, as well as solution engineering

Member of Partner Advisory Council (PAC) and represent client voice

Dedicated Center of Excellence (CoE) Labs, powered by partners' solutions

Access to partner training programs, confirming required skills and competency build

Certification of EY solution by Partners' Technical Solutions Group

More than 75 alliances and ecosystem partners across the globe to support our tools and collaborating models.

Figure 5 - EY Cyber Key Alliance Partners

2.2. Service Description

Human Factors

There are **seven** core components of the EY People Security offer:

1. **Target Operating Model:** creating 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. **Academies 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. **Cyber Crisis Comms:** building capability to communicate effectively internally, externally and with regulators in times of crisis

Target Operating Model

- ► Understand current cyber operating model and how this aligns with the full organisation operating model
- ► Identify key areas to strengthen 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 for the target operating model to be effective – e.g., policies and governance, training, culture and awareness, etc
- ► Develop the implementation roadmap to realise target operating model benefits and integrate with the whole organisation operating model

Culture and Awareness

- ► Define current and target culture and levels of awareness
- ► Using CFD articulate the gap that needs to close and the behaviours, from leadership down, that need to change to achieve the target state
- ► Develop and launch a culture change and awareness raising programme
- ► Integrate culture and awareness programme with organisation 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

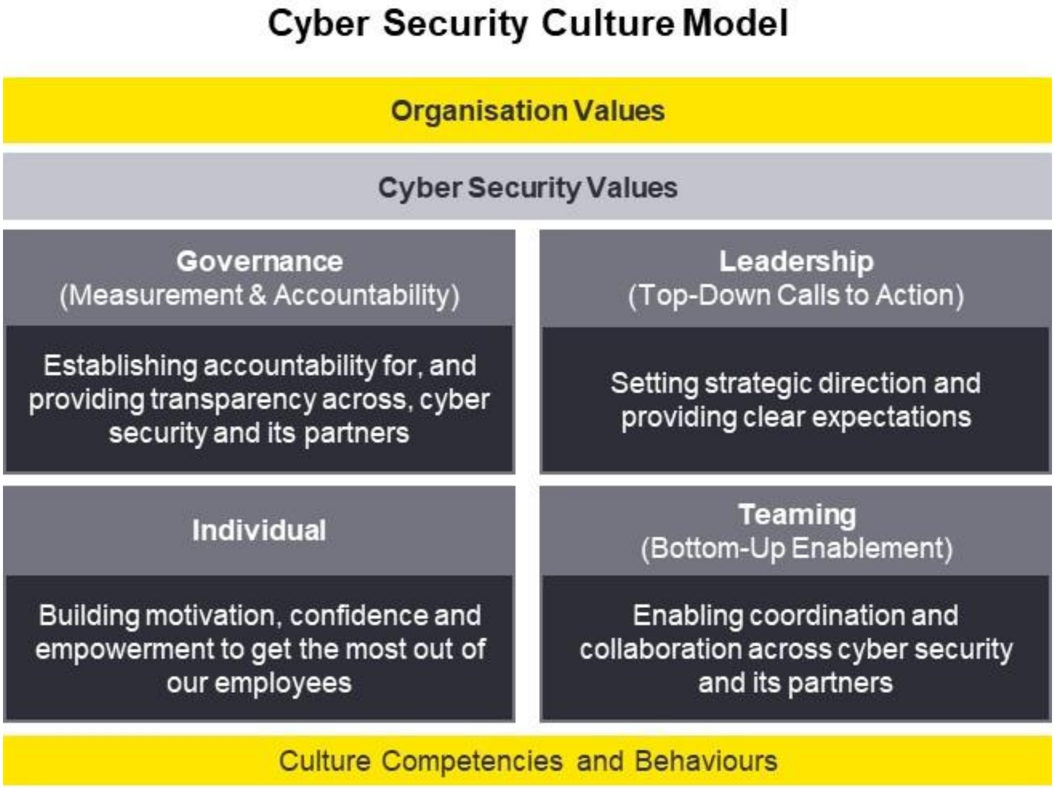

Cyber Security Culture Model
Organisation Values
Cyber Security Values
Governance
(Measurement & Accountability)
Establishing accountability for, and providing transparency across, cyber security and its partners
Leadership
(Top-Down Calls to Action)
Setting strategic direction and providing clear expectations
Individual
Building motivation, confidence and empowerment to get the most out of our employees
Teaming
(Bottom-Up Enablement)
Enabling coordination and collaboration across cyber security and its partners
Culture Competencies and Behaviours

Figure 6 - Cyber Security Culture Model

Organisational Resilience

- Using operating model and capability gap analysis map current capabilities to critical roles across the organisation
- Using the current organisation baseline establish the gap between capability supply and demand
- Develop a future workforce plan, including strengthening existing approaches to talent attraction and retention, to close the gap between supply and demand
- Regularly monitor organisation resilience against the capability assessment and workforce plan

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
- Evaluate gaps in leadership capability and deliver targeted training interventions to close gaps

Academies and Training

- Establish current state capability and develop employee personas to inform learning journey development
- Define future capabilities and using OCX establish the gap to be closed

- Understand the existing learning offer and identify any gaps in provision
- Design and launch the new learning curriculum working with our leading cyber training partners, creating learning journeys aligned to employee personas

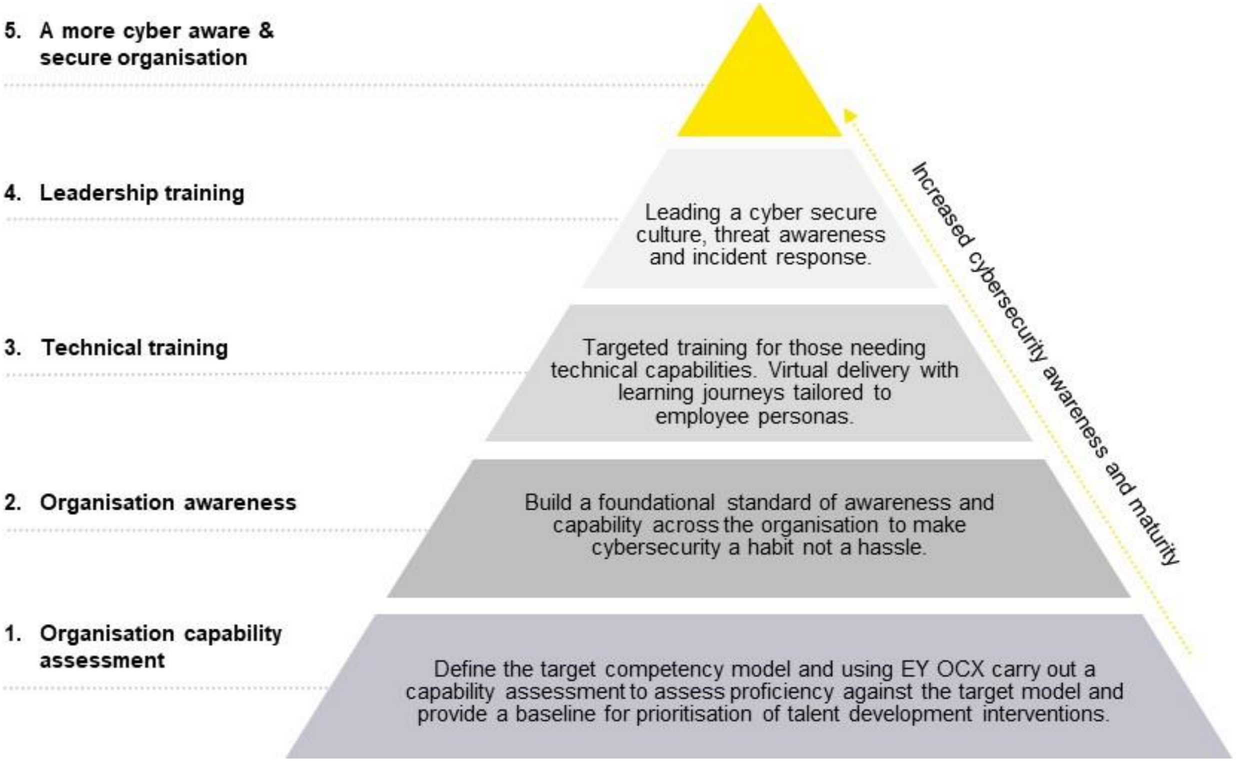

5. A more cyber aware & secure organisation
4. Leadership training
Leading a cyber secure culture, threat awareness and incident response.
3. Technical training
Targeted training for those needing technical capabilities. Virtual delivery with learning journeys tailored to employee personas.
2. Organisation awareness
Build a foundational standard of awareness and capability across the organisation to make cybersecurity a habit not a hassle.
1. Organisation capability assessment
Define the target competency model and using EY OCX carry out a capability assessment to assess proficiency against the target model and provide a baseline for prioritisation of talent development interventions.
Increased cybersecurity awareness and maturity

Figure 7 - Cyber Training Pyramid

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

Cyber Crisis Comms

- Understand current crisis communications capability
- Define stakeholders who need to be communicated with during a crisis, and the different methods and messaging each group needs
- Review past crisis communications to understand lessons learned
- Run a cyber crisis communications simulation to test capability
- Evaluate gaps in communications capability, deliver targeted interventions and develop specific communications aids to support more effective future crisis communications

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.

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