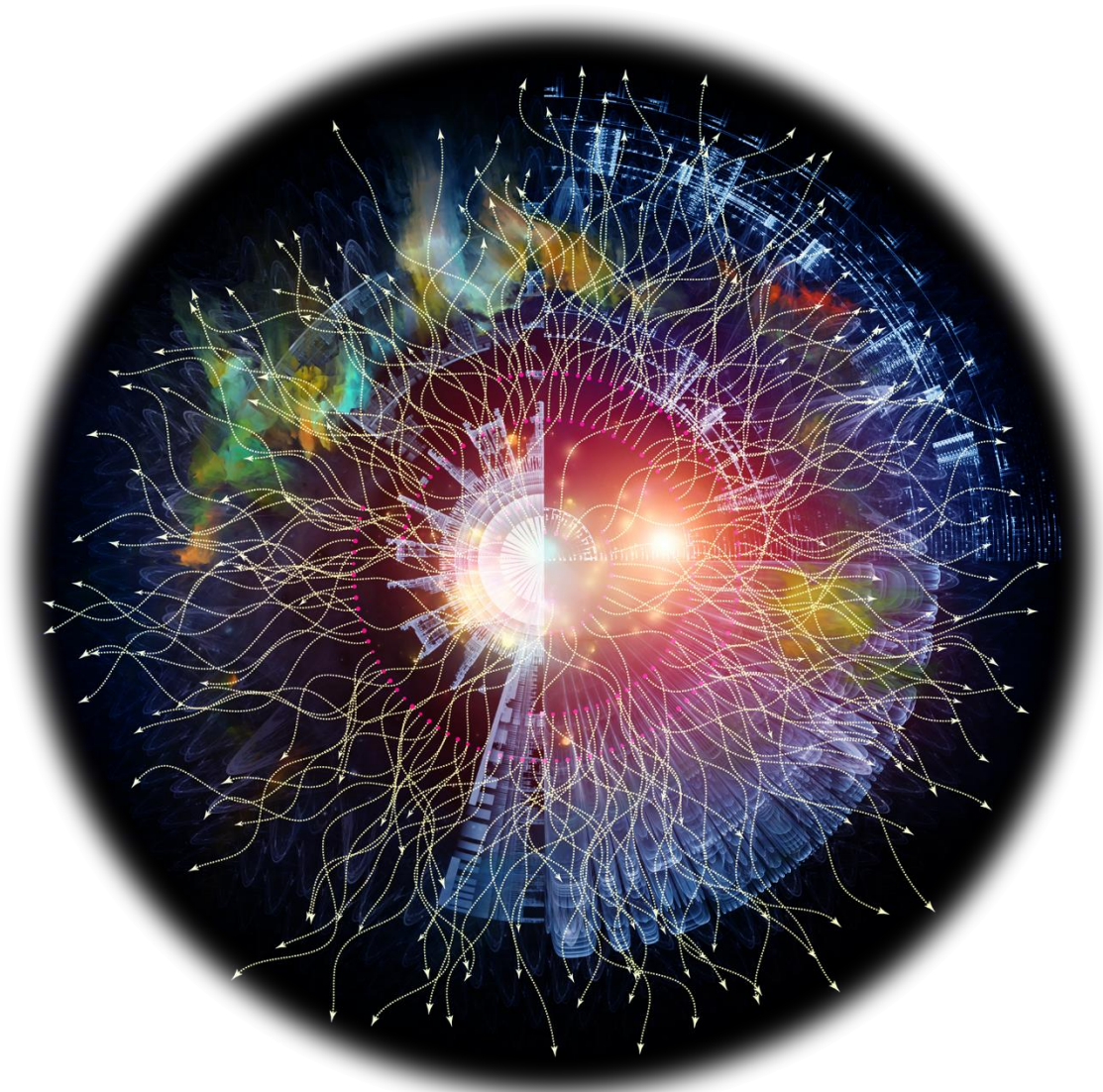




Zero-Trust and Network Segmentation

G-Cloud 15 Service Definition Document

January 2026

Contents

1	Deloitte Overview	1
2	Service Overview	3
3	Detailed Service Description	1
4	Contact Details	5

1 Deloitte Overview

As a leader in professional services, Deloitte LLP is committed to making an impact to our clients, our people and for society. We have over 27,000 staff based across the UK providing audit, risk advisory, tax, consulting, financial advisory and legal services to public and private clients across multiple industries. We work together to build trust, support inclusive growth, and build capability, enabled by our **breadth and depth of expertise across advisory, delivery, engineering and managed services.**

Our **public sector practice** serves Central Government, Government Agencies, Local & Regional Government, Defence, Security and Justice, Health and Social Care, Transport, Education and Housing. We also provide services to the Northern Ireland Office, Scottish Government, Welsh Government and Crown Dependencies.

Our Cloud Capability

At Deloitte, we help our clients **Imagine, Deliver and Run** the businesses of the future through the power of **Cloud**. We have deep Cloud architecture, engineering, operational, commercial, and business transformation expertise delivered by a team of more than 26,000 Cloud Practitioners globally. We have delivered over 2,000 cloud implementations over the past 5 years and have 60+ cloud centres of excellence supporting the delivery of cloud services to our clients.

In the UK, we have a team of over 100 Cloud managed service specialists plus the following certifications across AWS, Microsoft Azure, Google Cloud and Oracle Cloud Infrastructure (OCI):



We help our clients with all aspects of their journey-to-cloud and optimisation of their cloud and cloud-services investments. Our Cloud practice can support you to optimise your client investments, and to navigate your organisations cloud journey, providing specialist cloud architecture, engineering, and operational skills at all stages, with a large proportion of our team holding the clearances required to meet your specific security requirements.

Our AI Capability

Deloitte stands at the forefront of AI transformation and was recognised as a Leader in the 2025 IDC MarketScape for Artificial Intelligence (AI) services for the fourth consecutive time. Supported by a £3 billion investment in AI, Data, Automation, Cloud, and Cyber, we seamlessly integrate our deep AI expertise with our extensive cloud capabilities. Our UK team is part of 339K AI-fluent practitioners globally, and includes over 1,300 AI specialists and engineers, many of whom hold the necessary security clearances for public sector delivery.

Through the Deloitte AI Institute, our hub for cutting-edge research and innovation, and strategic alliances with leading hyperscalers, we empower public sector clients to optimise costs, streamline processes, and navigate their AI journey. We achieve this by leveraging our ReadyAI™ models, which provide end-to-end support for AI solution implementation, and our Trustworthy AI™ framework, ensuring responsible and ethical deployment.

Our alliances & ecosystems

To bring full value to our clients, Deloitte is a premier consulting partner with all the leading hyper-scale cloud vendors in the market including AWS, Google, Microsoft¹ and SAP. A selection of our partners and alliances are presented below:



What the analysts say

Don't just take our word for it. Deloitte is recognised by the analyst community as being **leaders in cloud transformation services**. This reflects the wealth of experience we have in delivering cloud services across the public sector and wider private sector combined with our out-of-the-box templates, tools and assets.

Gartner

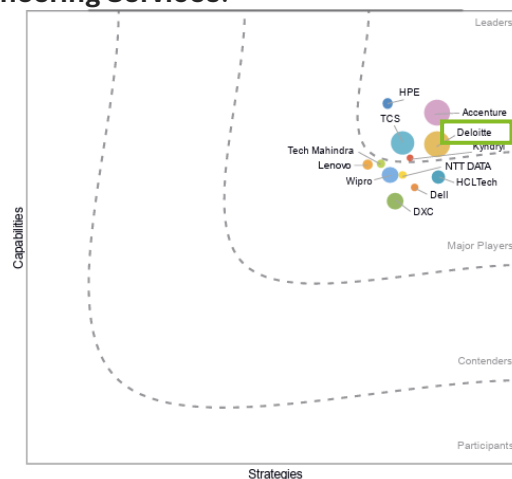
Deloitte was also positioned as a Leader in the **Gartner Magic Quadrant for Public Cloud Infrastructure Professional and Managed Services, Worldwide** for each year from 2019 through 2025.



Gartner: Magic Quadrant for Public Cloud IT Transformation Services. © Gartner inc. 2025

IDC

Deloitte was again awarded Leader status in the **IDC MarketScape: Worldwide Hybrid IT Consulting and Integration Services 2025** Vendor Assessment. This follows our 2024 success. We were also recognised as Leaders in **Hybrid IT Consulting & Integration Services** and **Software Engineering Services**.



IDC MarketScape: Worldwide Hybrid IT Consulting and Integration Services 2025 Vendor Assessment © IDC inc. 2025

Deloitte scored highest in 4 of 5 Use Cases in **Gartner® Critical Capabilities for Public Cloud IT Transformation Services 2025** report: *"Deloitte approaches all aspects of cloud adoption, including migration, with transformation as an objective."*

Cloud Transformation

Transform Faster, Transform Smarter

Deloitte's Cloud Transformation can fast-forward your journey to the Cloud, unlocking innovation, efficiency, and growth.

[Find out more here](#)

¹ As Microsoft's Independent Auditor, Deloitte cannot have a direct or material indirect business relationship with Microsoft, such as having an alliance or being a registered partner. Nonetheless, Deloitte can provide Microsoft-related technology services and invests heavily across its global business building technical skills and capabilities to develop world-class consulting and solution delivery capabilities.

2 Service Overview

Deloitte assists clients defining and implementing their organisation's **Zero-Trust & Network Segmentation** strategy in line with their cloud and digital agenda. Zero Trust is a framework for looking at Cyber Security in a new way. Based on the fundamental principle of “never trust, always verify” or least privilege access, Zero Trust moves away from the traditional perimeter-based concept of managing security, to one where trust is established between individual resources and consumers, as and when needed.

The Deloitte's Zero Trust framework helps organisations bring focus on their specific challenges and aspirations, develop a plan of action, and deliver the end-to-end capabilities aligned to the business drivers. We recognise that many clients have started what is a multi-year journey and that there is no single product solution, it requires a well-defined approach architected around multiple **identity and security components** which draw upon many supporting concepts including (among many others) **network macro and micro-segmentation, software defined perimeter and Secure Access Service Edge (SASE)**.

In a broad and rapidly evolving marketplace, Deloitte brings an understanding of the common integrations with broader ecosystem partners and technologies including offerings from cloud-centric vendors (e.g. Zscaler, Illumio, Akamai, Cloudflare) as well as traditional network perimeter vendors with evolving offerings (e.g. Cisco, Palo Alto Networks, Checkpoint, Microsoft, F5).

Features

- **Identification:** Capture business drivers, challenges, and priorities
- **Assessment:** Perform assessment and provide as-is capability review, maturity assessment, benchmarking and gap analysis
- **Definition:** Build a tailored and pragmatic Zero Trust strategy and roadmap aligned to business needs and aspirations by prioritising the most relevant initiatives and optimising existing investments
- **Implementation:** support organisations through the journey of implementing the Zero Trust and network segmentation strategy anticipating and addressing challenges to achieve the target state.
- **Transition:** Incremental service enablement, validation, and operational transition.

Benefits

- **Modern workplace enablement:** Supporting the ‘new normal’ of remote working patterns and enabling employee productivity, by reducing friction and providing secure and flexible access
- **Enhanced support for digital products and services:** Using Zero Trust principles to securely develop digital products and services and meet evolving user demand.
- **Improved risk management:** Enhancing the ability to detect and respond to threats in real time and reducing attack surface by restricting lateral movement
- **Consistent security framework:** Enabling a consistent security architecture across cloud and on-premises environments and integrating legacy services.
- **Sustainable cost management:** Manage security costs by minimising IT complexity through automating, simplifying, and standardising the way security is provided.

- **Enhanced organisation agility:** Enabling faster and secure innovation, greater agility, and easier and more efficient integration with partners and third parties

Technology we typically work with:

Attack Prevention and Response	Reducing the Attack Surface	Network Security Operations
CASB	SASE	SIEM / XDR integration
DLP / IPS / IDS	SSE	SOAR
DDoS / BOT Management / OWASP	WAAP	SDP
Vulnerability mgmt. / ASM	ZTNA	

3 Detailed Service Description

Business Context

Public sector bodies are increasingly under pressure to deliver on an aggressive digital agenda for both services and operations to meet rising citizen expectations while at the same time facing an ever-evolving cyber threat landscape.

This, as well as a broader set of business drivers and demands, are pushing Zero Trust onto the agenda and highlighting the need for greater speed and adaptability in how organisations approach cyber security, as they seek to survive and thrive in an increasingly digital world. Some of the main drivers we see our clients experiencing are:

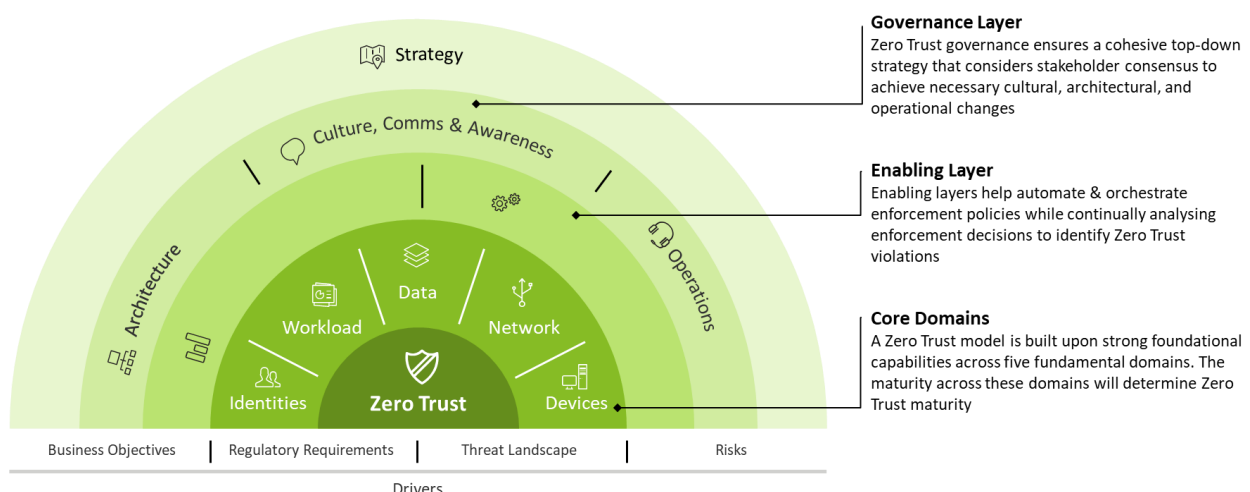
- The rapid pace of digitalisation is increasing **IT complexity** and driving up **cost**
- **Adversaries** are becoming more **sophisticated** and are outmatching current cyber defences
- The development of **digital products and services** is being **constrained** by rigid cyber security controls
- The **shift to the Cloud** is demanding a new approach to securing critical business data
- An **increasingly mobile workforce** now expects to be able to work from anywhere, on any device
- The demand for **better and easier business collaboration** requires a more agile approach to security
- The **cost of compliance** is rising due to overlapping and rigid controls, and more strenuous requirements
- The **proliferation of Shadow IT** is increasingly hard to contain without damaging business agility
- Increasingly **complex** vendor landscapes and **supply chains** require a more efficient approach to security

However, public sector organisations typically operate at huge scale and complexity. Adjusting the approach to cyber security towards **Zero Trust and further network segmentation** often impacts the wider operating model and results in significant transformation and implementation challenges.

Our experience is that delivering a **comprehensive cyber security strategy based on Zero Trust** cannot just be about complementing the current security architecture with point products to continue delivering existing services. This results in questions about the overall ‘enterprise-wide’ operations and can mean starting from first principles in design terms and clean up application access privileges and policies.

While Zero Trust can help unlock a range of benefits, to truly realise its potential organisations need to approach it methodically, with a clear line of sight to how Zero Trust will deliver these benefits for them.

Key Concepts



Zero Trust is a new way of thinking about security based on the principles of “never trust, always verify” –aligning the way you do security to the way you do business. It is much more than just a technology. It is a framework that **integrates** a range of **adaptive** and next generation capabilities. It is also **transformative**, re-imagining how organisations manage cyber and unleashing it, to **better align** to the way you work.

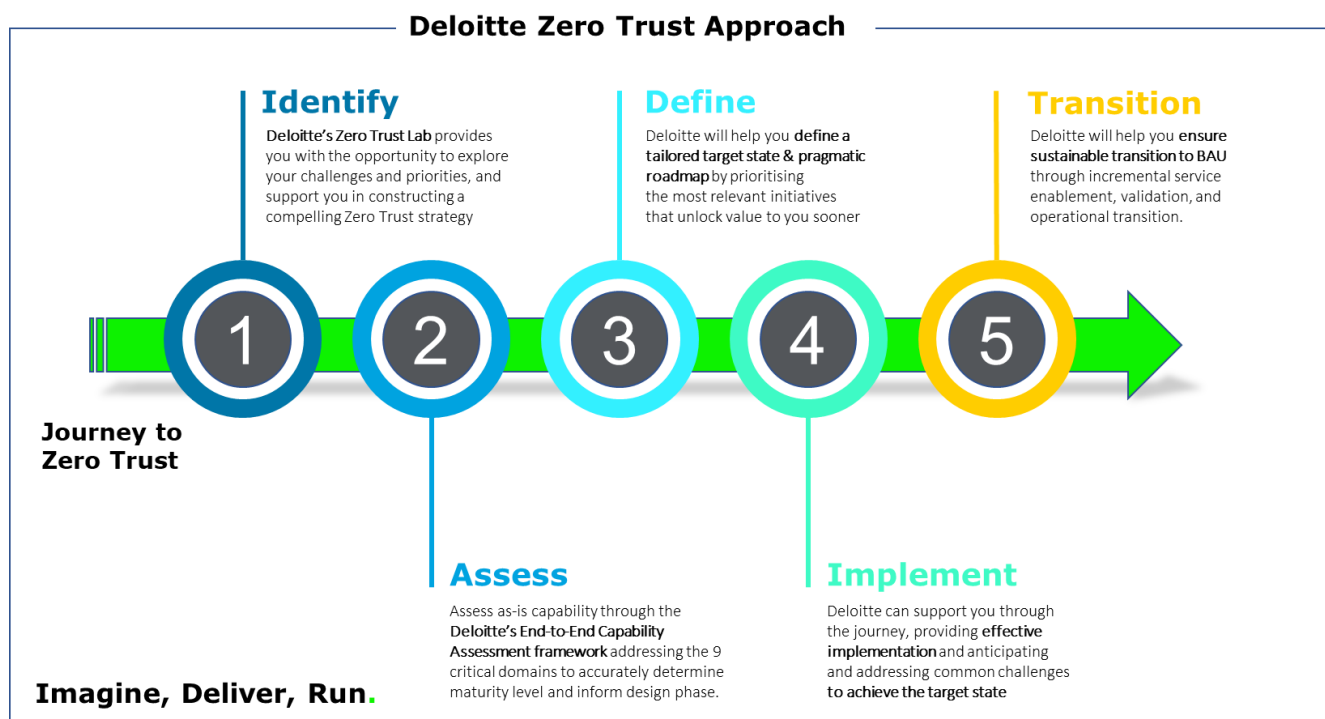
How does it work? All communications, regardless of location, are treated from the same starting point of having no inherent trust. Trust is established by a dynamic policy, informed by a range of signals –from behavioural analytics to threat intelligence -and is constantly revalidated.

Deloitte’s Zero Trust functional architecture helps provide a target state for the end-to-end Zero Trust vision.

Our approach

We understand that the challenges in achieving this are often different based on the user needs, organisational context and strategy, technology maturity and application estate within our clients. This enables us to develop customised plans that include an assessment of technical, personnel and organisational risks, the development of risk management plans, security operating models, and security monitoring requirements to provide operational assurance during the transition to the Zero Trust model.

We will work closely with you to help you craft and shape the network security evolution journey and support the transformation efforts using an established and proven approach. We put your specific needs and priorities at the heart of our approach. We reflect on what you do as a business, who your people are, the work activities that they undertake, what technology we need to put into place to be effective and how to best deliver this to ensure an effective and reliable service. We follow a user-centric transformation approach to determine your technology wants and needs – both current and future.



Our overarching method helps clients plan delivery of cyber security by bringing together perspectives on organisation design, process design, technology and other related factors into a single framework. We help clients align key elements of design with each other.

The adoption of Zero Trust should be viewed as an organisation-wide journey, that is as much about repositioning how management of cyber risk is approached across the organisation as it is about evolving technology capabilities. At Deloitte, we use a framework which encompasses nine foundational domains which help shape the Zero Trust journey and deliver desired business outcomes.



Architecture & Governance	Adaptive Zero trust roadmap with plan for adoption underpinned by EA frameworks, standards & principles
Network	Private networks retired and use of public networks & use of micro-segmentation to isolate workloads and secure them individually using a least privilege mindset
Identity	Password-less, context aware authentication. Privileged Access is ephemeral, access granted just-in-time
Operations	Preventative & predictive security operations using heavily automated operations leveraging AI & ML
Devices	Dynamic access based on continuously monitored device trust levels
Applications	Secure access to existing enterprise & legacy applications, Zero Trust enabled future products & service and enterprise application lifecycle management
Data	Enterprise information protection controls through trust levels based on enterprise-wide classification
Policy Engine	Centralised security policy management with adaptive enforcement for resources access based on contextual data
Adaptive Cyber	Dynamic security organization closely aligned to business priorities and continuously adapting to the rapidly evolving external/internal environments

Inputs & contributions required from the client

This service is designed for clients looking to assess their network security maturity, develop/refine their Zero Trust and network segmentation strategy as well as identify and execute practical steps to embed capability and build the desired maturity. This often entails changes to products, services, organisation structures and budgets as well as to technology architectures. As a result, it relies upon executive sponsorship and appropriate governance for wide-reaching business change.

Our service is designed to be delivered with our clients rather than to our clients. Clients' contribution as part of our service around access to relevant staff, stakeholders, data and technology is essential to achieving a successful outcome.

Outputs

The deliverables of this service will depend upon the roles that are agreed for Deloitte's scope in the Service Order. They will be documented in the Service Order. Indicatively, the kind of deliverables that we may produce are:

- Network security maturity assessment, to be architecture and high level roadmap
- End to end plan, encapsulating design, build, deployment and migration schedules

- Zero Trust Business case
- Implementation and deployment of secure infrastructure to enable business agility
- First line of defense in response to Security Incidents or as part of the recovery programme.

Service Constraints

To gain full value from this service the buyer will need executive level governance to make decisions, resolve issues, set strategic direction, and to provide inputs like: Strategic objectives; Committed delivery milestones; Budget constraints; Driving priorities and Policy. Additionally, the service is most effective if linked with the buyer's internal technical capability and business expertise. The buyer should also consider any other third parties involved with legacy systems and/or new deliveries relevant to the engagement scope. This may require the buyer to facilitate non-disclosure or other commercial agreements for these parties to be engaged in an effective and collaborative way.

4 Contact Details

Please send your requirement to publicsectorbidteam@deloitte.co.uk. Alternatively, if you wish to discuss your requirements in more detail, please send us the following information and we will be happy to contact you:

- Your organisation name
- The name of this service
- Your name and contact details
- A brief description of your business situation
- Your preferred timescales for starting the work.



This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London, EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2026 Deloitte LLP. All rights reserved.

