

Zero Trust Assessment G-Cloud 15





Table of Contents

1	Service Overview	3
1.1	Assessment Model	3
2	Business Need	3
3	Our Approach.....	4
4	Buyer Responsibilities	4
5	Service Management	5
6	Protection of Data	5
7	On-boarding and Off-boarding	5
8	Skills and Knowledge Transfer	5
9	Partnerships/Alliances.....	6
10	Vendor Accreditations/Awards	6
11	Sub-contractors	6
12	Business Continuity and Disaster Recovery	6
13	Pricing	7
14	Ordering and Invoicing	7
15	Termination Terms	7
16	Further Information	7



1 Service Overview

We offer Zero Trust services by combining our deep technical expertise, end-to-end collaborative ways of working, and strong partnerships to provide you with a simplified, streamlined, and cost-effective solution, tailored to meet your business needs. The start of your Zero Trust journey begins with a maturity evaluation assessment but we can also provide, advisory services on ZT strategy, architecture & design, implementation, roll-out, and managed services.

1.1 Assessment Model

Our assessment model is based off the CISA Zero Trust maturity model, with the scope illustrated by the CISA framework shown below:

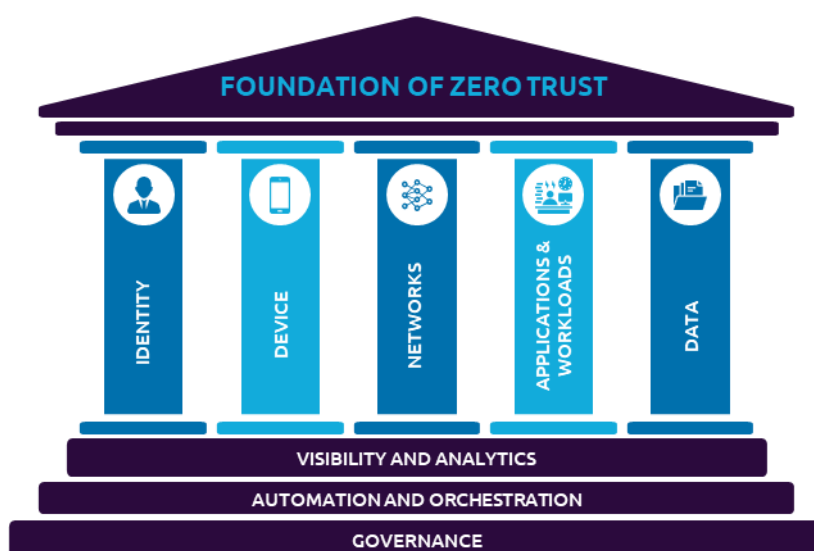


Figure 1: CISA Framework for Zero Trust

This diagram is for illustration only and does not represent any obligation or responsibility of Capgemini.

We have extended the CISA model assessment criteria so as to include elements that we have identified as being crucial to successful Zero Trust initiatives such as an increased focus on the control plane, which provides the policy information and policy enforcement elements of the zero trust model and through incorporation of requirements relating to Operational Technology within the Devices pillar of the standard model. We complement the established CISA framework with insights from the NCSC architecture design principles relating to Zero Trust.

2 Business Need

The traditional enterprise security model of a hard shell and a soft center is obsolete; the network is no longer a clearly definable perimeter when dealing with hybrid multi-cloud ecosystems cutting across a wide range of cloud providers from AWS and Microsoft through to ServiceNow and Salesforce. We need to implement new security approaches that are able to protect systems and data wherever they may be hosted and however they may be accessed – whether by human users, by devices or by other systems and services.

According to CIPD, 74% of UK organisations support a hybrid working model to leverage the benefits of remote working and so improve the employee experience. Organisations reap enormous business advantages by enabling remote workers to access business applications and data, wherever they may be. This change in working practices is only one element of enterprise digital transformation, with “cloud now” business as usual, IT/OT convergence commonplace, and Agentic AI and GenAI the subjects of an increasing number of mandates for change. Today’s organisations need an efficient and reliable security approach that adapts to the complexity of the modern enterprise, whilst addressing an increasingly aggressive threat landscape.



Zero Trust is an established security philosophy providing a proactive approach to secure all elements of the CISA framework – identity, devices, workloads, networks, and data. Zero Trust aims to verify each access request explicitly; authenticating, authorizing, and encrypting all communications, providing dynamic, context-based access control, all predicated on an underlying assumption that any element of the ecosystem may be compromised.

3 Our Approach

We assess the Zero Trust readiness of your organisation in alignment with the vendor-neutral CISA maturity model, industry-standard NIST zero trust architecture guidance and the NCSC architecture design principles for Zero Trust. We work with you to identify the scope of your proposed zero trust initiative and so tailor the scope of our assessment appropriately. We recognize that different organisations have different aims for their zero trust initiatives and that one size does not fit all. Once the scope has been agreed, we conduct our assessment through a series of workshops, one-to-one interviews and document review, pulling the information together to then produce our assessment of the As-Is position against the criteria of the (extended) CISA framework and to produce a high level transformation roadmap that breaks the overall programme into a set of clear activities and work packages that can be scoped and delivered in a staged manner. We validate our initial findings and recommendations with key stakeholders and project sponsors prior to issuance of our final report.

Our approach leaves buyers with a clear view as to next steps and with the insight needed to produce the business case(s) necessary to move forward with their Zero Trust initiatives and is suitable for use wherever the buyer may be on their journey to Zero Trust (i.e. from derivation of Vision through to optimization of operation).

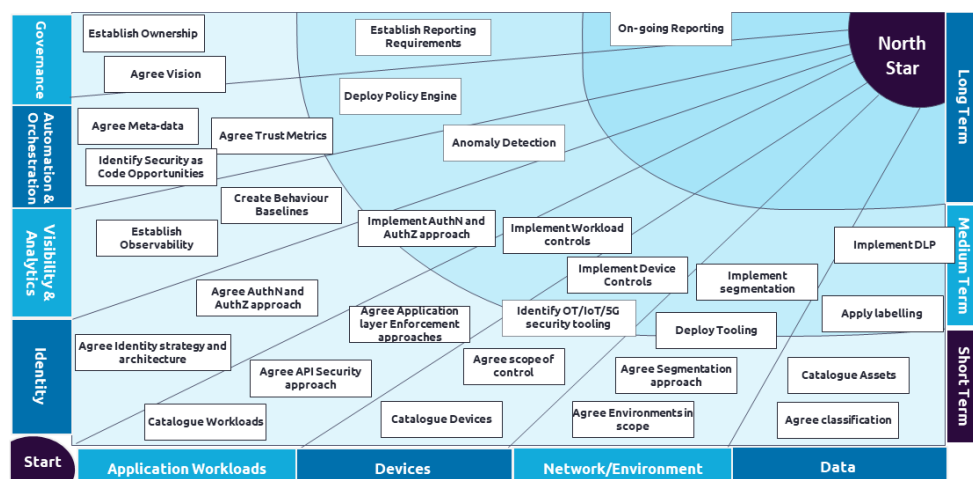


Figure 2: Illustrative Transformation Roadmap

This diagram is for illustration only and does not represent any obligation or responsibility of Capgemini.

4 Buyer Responsibilities

Please refer to the Supplier Terms listed with this service on the Platform. These may contain additional Buyer obligations/costs the Buyer is subject to that are not identified anywhere else in the Supplier's Application or on the Platform.

The Buyer responsibilities as part of this service are as follows:

- The Buyer will define the scope of the area to be assessed.
- The Buyer will provide any training and awareness education to the security assessor as is required by the on-boarding requirements.
- The Buyer will provide a project manager to act as a single point of contact and an escalation route for the full duration of the project.



- The Buyer will make available appropriate subject matter experts and documentation (business and technical) to the project as appropriate to support the security assurance assessments.
- The Buyer will be responsible for providing detailed requirements by the mutually agreed date.
- The Buyer will announce the assessment to all appropriate individuals, asset and process owners.
- All internal and external user communications will be managed by the Buyer.
- The Buyer will accept the security assurance assessments report via post assessment presentation and be responsible for managing the recommendation identified from the assessment activity.

If these responsibilities do not match your expectations, then please contact us in order that we can explore options to vary our approach.

5 Service Management

Capgemini's service can be consumed in the following deployment and delivery models, all fully managed by Capgemini. Please contact us to discuss which of these fits your requirements. These are:

- **Offshore resources:** Our consultants work from our offshore locations. This provides a very cost-effective solution with access to a large pool of related skills.
- **Onshore resources:** Our consultants work from our UK offices. This provides a cost-effective solution for buyers that require UK delivery.
- **Dedicated resources:** Our consultants work on your sites, embedded as part of your team. This provides a solution for buyers that require skills augmentation and a high degree of control over the work.

6 Protection of Data

This service is based on a security classification of 'Official', however should you have a requirement for a different security classification that you would like us to consider, please contact us to discuss.

7 On-boarding and Off-boarding

Capgemini shall undertake on-boarding and off-boarding activities agreed within the Order Form (including as a minimum an exit plan in line with the Call-Off Contract terms) which will be charged for in accordance with the Pricing section for this service.

8 Skills and Knowledge Transfer

Capgemini recognises that skills and knowledge transfer is a critical element in the provision of G-Cloud services to public sector clients. Where possible and applicable, this forms part of the delivery plan for the service agreed at the start of the engagement. Our consultants and engineers are experienced in providing skills and knowledge transfer for major private and public sector clients.

Where appropriate, we may use a standard approach, tailored to topic, skills-gap and individual, to ensure consistency and effectiveness. The approach, Capgemini's Assess-Plan-Implement framework, has been used repeatedly by our teams to structure the work involved in transferring skills and creating new teams capable of driving and sustaining change long after the end of the formal programme. The framework can be applied throughout a project to understand knowledge transfer objectives, plan training delivery methods and materials, and deliver and evaluate success.



9 Partnerships/Alliances

Capgemini has a collaborative solution with Zscaler that provides a simplified ZT approach and eliminates the need for cumbersome Virtual Private Networks and complex data center-hosted security technologies. This simplification reduces the total cost of ownership whilst helping to make security transparent to your users. We also have experience with, and access to, a range of solutions from other vendors such as Illumio and Microsoft.

10 Vendor Accreditations/Awards



For the 13th year in a row, Capgemini has been recognised as one of the World's Most Ethical Companies® by the Ethisphere® Institute. This is an acknowledgement of our ethical culture that makes us an employer of choice and responsible player in the eyes of our clients, shareholders, and the wider community.

Capgemini can provide security delivery professionals with the following industry certifications:

- NIST Cybersecurity Framework (NCSF);
- Certified Information Privacy Professional/Europe (CIPP/E);
- Certified GDPR Practitioner;
- Certified ISO/IEC 27001 Lead Implementer;
- Certified ISO/IEC 27001 Lead Auditor;
- Certified Information Systems Security Professional (CISSP);
- Certified Cloud Security Professional (CCSP)
- Certificate of Cloud Security Knowledge (CCSK)
- Certified Information Security Manager (CISM);
- Certified Information Systems Auditor (CISA);
- Certified Ethical Hacker (CEH);
- TOGAF9, SABSA and other architectural methodologies including Capgemini's own;
- IT security specific MSc or PhD;
- Membership of the Chartered Institute of Information Security Professionals (CIISec)
- Certified in Risk and Information Systems Control (CRISC)
- Computer Hacking Forensics Investigator (CHFI)
- Capgemini delivery staff hold a wide range of vendor specific certifications for many types of cybersecurity tooling.

11 Sub-contractors

Capgemini UK may use the following subcontractors to deliver this service:

- Capgemini Technology Services India Limited.

12 Business Continuity and Disaster Recovery

No disaster recovery plan is provided as part of these Services.



13 Pricing

This service is priced in accordance with the SFIA Rate Card attached. Capgemini can also provide offshore resources at reduced rates where appropriate. Projects can be priced either on a Time & Materials or Fixed Price basis.

14 Ordering and Invoicing

Please refer to the Supplier Terms for this service.

We would be pleased to arrange a call or meeting to discuss your requirements of our service in more detail.

15 Termination Terms

Please refer to the Supplier Terms for this service.

16 Further Information

For more information about this or any of our G-Cloud services, please contact our Public Sector Team.

Phone: 0370 904 4858

Email: publicsector.opps.uk@capgemini.com including the following information:

1. The name of this service.
2. The name of your organisation.
3. Your name and contact details.
4. A brief description of your business situation.
5. Your preferred timescales for starting the work.

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, generative AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2024 global revenues of €22.1 billion.

Make it real. | www.capgemini.com



This presentation contains information that may be privileged or confidential and is the property of the Capgemini Group.

Copyright © 2026 Capgemini. All rights reserved.