



G-Cloud 15

Security Architecture Services

January 2026



Contents

Transformation Business using the Cloud 3

Security Architecture Services..... 5

Our Service Delivery Approach 6

PwC Alliances 9

Transformation Business using the Cloud

Enabling business and enterprise transformation using cloud is a complex, strategic consideration facing many private and public sector organisations. We have worked with many Central and Local Government clients to support the implementation of their business objectives using cloud technology.

Cloud technology and services have the potential to reduce cost, remove technology bottlenecks, and facilitate rapid business innovation. As a result, for most organisations globally, adopting cloud technology has become a question of “when and how” rather than “if”.

Opportunities for enterprises generally include a combination of one or more of the following:

- Implementing private and/or hybrid clouds for infrastructure and applications
- Smarter use of public cloud infrastructure for optimising existing business functions
- Using cloud for implementing new business services or digital operations
- Reducing cost by moving to consumption-based pricing models that only charge for the actual IT capacity and services used.

Migration or adoption of cloud must be properly choreographed for success. We understand the realities and the business and technical risks that should be fully considered, understood and mitigated before such a move. Critical considerations include:

- **Alignment of business and technology objectives.** This is essential to fully realise the targeted benefits of any cloud transformation or any refinement of existing cloud services. There can be a tendency to adopt cloud systems to fit current ways of working, rather than adopt and standardise processes where possible. The trade-offs between business, customer and technology requirements must be considered to make informed design decisions
- **Availability and reliability of services.** The avoidance of operational downtime to mitigate in lost revenue, unnecessary operational cost or reputational damage that can disrupt a business' operations
- **Decentralised support structures.** The need to tailor and revise the approach to operational security to cover the support structures employed by cloud service providers that will have a different risk profile for sensitive information
- **Data handling practices.** Data classification and data-handling practices that reflect the data flow within a cloud environment must be understood and tailored accordingly to protect customer data

- **Data privacy.** Compliance with GDPR to understand where and how information can be stored or processed. The cloud model enables data to bounce swiftly around the world by using available server capacity in various geographic locations, but this must be within the bounds of what is permissible. This is ever more of a concern as organisations review their front office, back office and out of office experiences
- **Future Technology Trends.** Cloud applications are the stated direction of travel for the major application vendors, but any upgrade path must also cater for the future technology needs of the organisation and seek to minimise technical debt where possible.

A careful assessment of an organisation's needs and different cloud service provider's controls is required, enabling concerns to be addressed and the correct path to the cloud is selected.

As a trusted advisor PwC provides the framework, and the wealth of private and public sector experience, to consider the combination of Business, customer experience and Technology activities outlined above. There is no single answer that covers each and every client organisation; we tailor our frameworks to client circumstances to support them:

- As a partner through the complete lifecycle of strategy through to execution
- With point business issues encountered during implementation or running the business.

Security Architecture Services

This section describes in more detail the service features and benefits included in this service definition document.

We have a dedicated Security Architecture practice that helps our clients to design security into their businesses and technologies and advise on securing:

- **Cloud platforms**, such as GCP, AWS and Azure
- **Cloud applications**, such as Salesforce and Microsoft Dynamics
- **In the Cloud or to the Cloud capabilities**, such as Security Operations and Data Loss Prevention.

Our bespoke Security Architecture Frameworks, processes and patterns, aligned to SABSA and TOGAF, enables us to assist clients with building their Enterprise and Technology Security Architectures and apply them.

Our cyber security architecture services facilitate the secure design, development and implementation of your technology solutions for the Cloud and in the Cloud, as you cloud-enable your business. This includes cloud security design, solution security design, and secure development and implementation of cloud capabilities and solutions. We achieve this by:

- **Secure By Design approaches:** Applying Secure 'By Design' approaches that align to the NCSC 'Secure By Principles' to create systems that are resilient to attack and easier to manage and update
- **Assets and Accelerators:** Bringing assets and platforms that enable us to rapidly advise and direct, articulate and evidence secure design, and equip designers and delivery teams to engineer a secure solution first time
- **Cloud Security and Platform Security Expertise:** Providing real expertise / specialist resources in the specific technology platforms themselves to help advise and inform direction, design and implementation
- **Architecture Centre of Excellence:** Driving excellence and security design and architecture professionalism into our Security Architecture professionals. Our Centre of Excellence drives ways of working / best practices, asset adoption, behaviours and industry awareness to ensure that our people are always excellent is what they do and in their delivery to clients.

PwC delivers a distinctive security strategy portfolio, encompassing security posture and optimisation assessment, security strategy and policy development, security programme design and execution, operating model and people change.

Our Service Delivery Approach

Security Architecture is at the heart of everything we do. Architecture is how we connect business and security objectives, goals and drivers to the organisation, its people, organisation, operations and technology, to enable effective decision-making and drive success, pace, efficiency and optimisation.

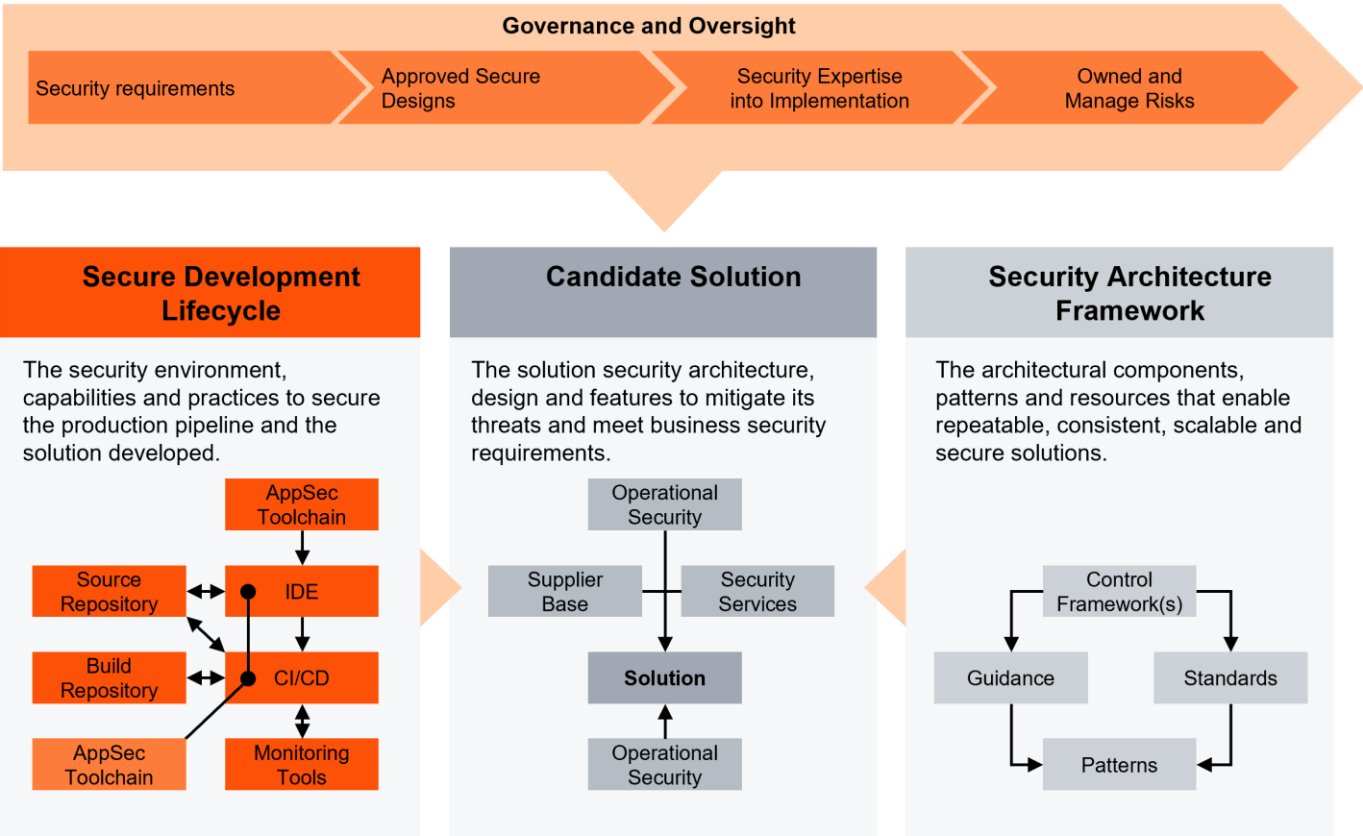
We use the principles of SABSA Enterprise Security Architecture as the framework for security architecture and the ‘Secure By Design’ principles to drive our ‘Secure By Design Model’ to set out the domains that need architecture, and architecting and connecting together.

Security Leadership and Culture

The security leadership, incentives and culture to enable and embed effective and secure delivery and operation that meets business objectives.

Security Delivery Pathway

The security steps, processes and governance in place and operated to ensure that what is delivered is secured to the level agreed.



We recognise that to support organisations achieve their security architecture goals there is a diversity of needs, demands and expertise required in different shapes and sizes, we deliver the service based on different types of needs.

Your security strategy service may include one or more of the following:

- Technical Support:** You need well-defined and standard support to a project building a *Candidate Solution* to help make recommendations around a solution and a design or to your security architecture

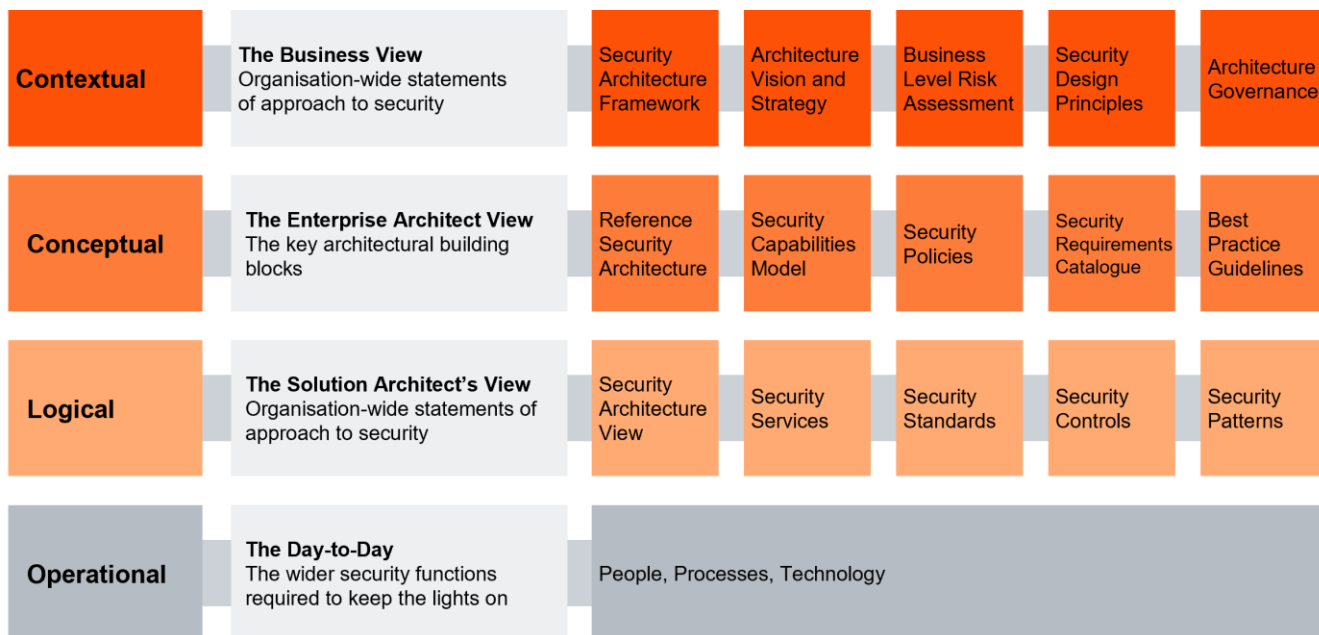
team developing the components of a *Security Architecture Framework* such as security patterns. For example, solution Threat Modelling, Design Options papers.

- **Architectural Support:** You need bespoke or more specialist support where there is a large delivery programme or more strategically impacting delivery, such as re-defining your *Security Delivery Pathway*. For example, Solution Security Designs.
- **Enterprise / C-Suite Support:** You need support on ccomplex issues or handling leadership to resolve challenges impacting the whole enterprise, such as a fundamental architectural direction or technology choice.

We use it to structure our Security Architecture support approach for programmes, projects and organisations. It provides us with a layered methodology, enabling traceability and justification of every security element which we add to designs. This structured approach gives us a powerful means of ensuring consistency across multiple interdependent projects and programmes. It also gives us the means to link everything back to:

- The overarching security risks which an organisation faces
- The strategic goals of the organisation.

By doing this we make sure the security controls are implemented, and decisions taken are always appropriate within the context of the organisation and the circumstances faced. Our framework and approach consist of several mature artefacts:



Our dedicated Security Architect has experience of designing and implementing security in complex environments for our Government, Banking, and Private Sector clients. Additionally, our entire Cyber Security team of over 350 people receive Security Architecture training and development, so they learn to think in this way. These are also practitioners of other security disciplines, and we leverage these to provide specialist non-architecture insight to bring the most value to our security architecture work.

We offer different models to provide commercial flexibility to align with your needs and the demands you are facing and what you need support with. We have developed these different models based on our working with numerous clients. They provide commercial flexibility to align with your needs, including fixed fee and time and materials, and offer different delivery locations to deliver these services, including Greece and Egypt.

Clearest requirement	Commercial Option	Best suited-for	Pro's	Con's	Most Regulated
	Fixed catalogue draw-down Prefdefined catalogue of security packages against a call-off oncontract.	Longer-term regular services positioned within an established function (e.g., regular pipeline of programme / project change activity).	• Commercially quick to commission each piece of work. • Well-defined and predictable outputs. • Easier to forecast and consumption planned.	• Needs a Secure-By-Design process in place. • Service mobilisation can be slow to formalise catalogue and terms. • Most rigid on terms and dependencies.	
	Flexible drawdown Ad-hoc defined work-packages, or mix of predefined and ad hoc, delivered against a call off contract.	Ad-hoc demand for support to meet different requirements.	• Mobilisation of service can be quick to initiate and provide immediate support. • Good flexibility to respond to requirements.	• Individual support requests can take longer to mobilise than a fixed catalogue. • Difficult to forecast and requires active planning.	
	Virtual team subscription Predefined level of capability and capacity as monthly subscription, like a virtual team.	Diverse support from a security architecture function from scratch needing continuous parallel support (e.g., need to develop architecture processes, support projects, design patterns, develop strategies).	• Entirely agile and flexible to requirement with no package contacting overhead. • Committed ongoing capacity to deliver work. • Continuity of resources supporting delivery. • No requirement to forecast.	• Most hands-on requiring your engagement to routinely task and steer. • Committed cost and resource becomes a standing army if not continuously loaded.	
	Virtual bench Architects as virtual bench to be called upon when required.	Need urgent support but with limited budget and unclear long-term demand / requirement.	• Mobilisation is fast. • Only pay for what you use. • Flexibility for meeting the requirement.	• No continuity of resource. • No guarantee of availability. • Hands-on engagement to manage resources.	

Benefits of a PwC Security Architecture

PwC Security Strategy Services Features	PwC Security Strategy Services Benefits
• Service execution is backed-up with tried and proven assets • Industry good-practice aligned architecture products • Commercial flexibility to support fixed-price and T&M • Portfolio of assets and proven methodologies to accelerate execution • Security Architecture Capability Assessment • Secure By Design development, implementation and execution • Design and implementation of Security Architectures • Security monitoring strategy, design and implementation • Enterprise and Technical Security Architecture • System Threat Modelling • Security Architecture Frameworks, Patterns and Models • Security Architecture Function Resource Augmentation • Project and Programme Technical Security Consultancy.	• Build sustainable security into delivery practices to support 'Secure By Design' principles and strengthen security resilience • Tailored service aligned to your needs and position to achieve outcomes • Development of a platform for architecture that can be leveraged beyond the service and / or after the service has concluded • Alignment of security capabilities and solutions and outcomes to business strategy and key risks • Immediate access to specific / niche security expertise to advise and provide guidance • Ensures design and implementation optimisation of Cyber Security Monitoring • Reduces security complexity through seamless, usable and reusable security • Integrated within the wider Enterprise Architecture and Risk Management • Aligned with security architecture frameworks (TOGAF, SABSA) • NCSC Certified Cyber Professionals (CCP) and SABSA certified professionals and UK wide delivery capability.

PwC Alliances

By combining PwC's expertise and our Alliance partners' technology, we can help you to solve your most critical business issues. Whatever your focus - moving to the Cloud, greater innovation, or business transformation PwC are here to help. Read more about PwC's partnerships and awards here:

<https://www.pwc.co.uk/services/alliances.html>



Confidential. This document does not constitute a Call-Off Contract for Services with PricewaterhouseCoopers LLP. Where we are engaged to provide Services, our Services will be governed by a subsequent Call-Off Contract that may be entered into between us. If you receive a request under freedom of information legislation to disclose any information we provided to you, you will consult with us promptly before any disclosure. All information contained in this document or otherwise provided or made available as part of any Award Procedure is confidential and may not be disclosed to anyone else without our prior consent.

© 2026 PricewaterhouseCoopers LLP. All rights reserved. 'PwC' refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.