Crown Commercial Service

SECURITY ARCHITECTURE

GCloud Service Description Document

Bringing Ingenuity to Life.
paconsulting.com

Corporate Headquarters
10 Bressenden Place
London
SW1E 5DN
+44 20 7730 9000
paconsulting.com

Prepared by: PA Consulting
Reference: PA RM1557.15
Version: 1.0

Contents

SECURITY ARCHITECTURE

1.1 Short Service Description

PA's Security Architecture services provide integrated technology, people and process-based security controls. Using an Agile, secure by design approach (incorporating SABSA and TOGAF) we react to changing threat-landscape, providing traceability between controls and adaptive business goals. Designing and embedding this improves operations and increases compliance while managing budget and risk.

1.2 Key Service Features

1. Certified, experienced security and architects with SC/DV Level vetting
2. Experience with TOGAF, SABSA and NATO methodologies
3. Best practice to define, operationalise and embed end-to-end architectural approaches
4. Creating architectural artefacts including use-cases, models, diagrams, security patterns
5. Design/implementation of controls (ISO 27001, NIST) to ensure secure delivery
6. IDAM/IAM, Zero-Trust, SOC, Endpoint, Application and Data Security specialists
7. Expertise in Threat and Risk Assessment methodologies
8. Use of XML and ArchiMate modelling
9. Threat Modelling
10. Integrate emerging technologies into security architecture; e.g. AI, Cloud, IoT.

1.3 Key Service Benefits

1. Secure mission-critical enterprises
2. Product and devices developers
3. Improved transitioning to cloud infrastructure for organisations
4. Improved security of organisations with IT/OT infrastructures
5. Improved security for organisations undergoing transformation programmes
6. More effective measurement of security capability across the enterprise
7. Improved information security risk management enabling better investment decisions.

1.4 Service Definition

Our Security Architecture service covers the needs of organisations for designing, deploying and reviewing security controls. Our specialists have extensive experience in threat modelling and secure design review. We can assess existing architectures against best practice and secure design patterns with a business-driven, risk-based approach. Moreover, we are experienced in accelerating the creation of end-end secure architectures both at the strategic level and at the technical level. Finally, we support our clients in creating, augmenting and operationalising their security architecture functions from the more technical SMEs positions up to CISO level.

A common challenge we observe, is that many organisations focus security requirements on single architectural components, often at detriment to the bigger picture, including: how those components interact, the associated risks and most importantly, the business requirements they are supporting. The objective of security architecture is to create and maintain a coherent representation of security, starting at the business level, down to the component level. This allows prioritisation and traceability of security initiatives.

We build and maintain security architectures which link back to business principles and client vision, in a world that is intrinsically technology driven. We are seeing customers spend (and sometimes overspend) in order to secure their assets by buying technology, but they struggle to link these financial efforts to measurable improvements in their security posture and their strategic objectives. Our Security Architects provide experience, insights and expertise to bridge the gap and maximise the efficiency of spending for security.

We provide expertise and experience in the following specialist areas of security architecture:

- **Security Architecture Framework**: Based on the foundations of SABSA and TOGAF we have developed a structured way in which we can apply security architecture to a client's business needs to identify the people, process, information and technology controls required to deliver its outcomes in a secure way. We combine these approaches with cyber security frameworks like NIST CSF, ISO27001, CAF, NIS Regulations etc. to make sure that our work aligns to the needs of our clients' organisations. We can apply this on behalf of our clients, or work with them to develop, support and embed the security function within the business.
- **Threat and Risk Assessment**: Risk management, and the identification of credible threats to an organisation, are important business activities for our clients and should be supported by security architects at all levels. We ensure that risks to a business are considered and their impacts managed holistically rather than in isolation. We use a range of risk management methodologies and we provide expertise in threat assessment, threat modelling and threat intelligence.
- **Identity and Access Management (IDAM / IAM):** Effective IDAM is a key enabler for the successful delivery of secure and seamless services across any channel, device and location. Through our experience of delivering IDAM across many sectors we have built a comprehensive set of tools designed to accelerate the design and implementation of IDAM architectures and services for our clients.
- **Zero-Trust**: Networks and Infrastructure form the backbone on which services operate and with the accelerated uptake of Cloud services and remote working the opportunities for threat actors is increasing. We have extensive experience in assisting our clients to architect and manage well defined networks and infrastructure moving them towards a Zero-Trust architecture.
- **Endpoint Security**: A growth in connectivity requirements coupled with an increasingly remote, mobile workforce is compounding the need for a robust approach to endpoint security. We have experience in supporting businesses in understanding the blueprint of their

infrastructure and associated devices, offering a myriad of architectural solutions to best manage the evolving threat landscape.

- **Security and Operations Monitoring**: The ability to detect and respond to cyber threats within an organisation is critical. Organisations can no longer rely on preventative controls alone to protect their critical assets. We help clients to navigate the complexities of building a robust Security Operations and Monitoring capability, including vulnerability management, threat intelligence, incident response and detection and response capabilities (including SIEM/SOC).
- **Application Security**: We work with our Digital Team to evaluate the security of existing applications and develop, add and test security features for applications being developed. We are experienced at applying the Secure Development Lifecycle and our own security-by-design processes to application development and assessment to improve the security of our clients at all levels.
- **Data Security**: We have experience of securing architecture at the data layer providing protection from unauthorised access and from corruption throughout its lifecycle. We can provide data and information architecture diagrams, develop and link processes to the data in your organisation, map security controls to your data and test these to build a robust security capability around a fully understood data and information landscape.
- **Cryptography**: Cryptography is fundamental to how we secure data and interactions in a digital world. This reliance on these systems to simply 'work' means that the improper design and maintenance of cryptography services can leave an organisation and individuals significantly exposed. We have a wealth of experience across sectors helping clients to securely define, establish and operate cryptography services.
- **Threat Modelling**: Threat Modelling allows an organisation to better understand its threat landscape and cyber security characteristics, helping identify areas of concern and mitigate them. PA combines industry standards and best practices with its expansive and highly experienced security SMEs ensuring an enhance security outcome.

Our assignments are often based on the models in the table below and we always tailor these to our clients' specific needs and focus:

Threat modelling	Threat modelling aims to identify, enumerate and categorise threats for a specific system.	We are able to apply all the most common threat modelling methodologies: STRIDE, PASTA, OCTAVE etc and can develop ad-hoc methodologies for specific tasks. We have also experience in developing bespoke tooling to facilitate the creation and maintenance of flexible threat models. The delivery methodology is usually in phases: • Interviews with stakeholders and documentation review • Development of the threat model • Adding the threat modelling methodologies to the risk management framework
Secure Design Review	The objective of a design review is to assess the security of the architecture of a specific system.	Typically based on a Threat model, we will assess how well currently deployed controls follow best practice and secure design patterns using the most appropriate references and methodologies (typically involving secure implementation of IAAA, segmentation, encryption, monitoring, auditing etc.). This analysis will be performed with a risk-based approach and will consider business criticality of the systems.

		A report with recommendations to remediate risks and issues will be provided as well as a suggested improvement roadmap.
Enterprise and Solution Security Architecture Improvement	The service's objective is to create an end-to-end security architecture for an enterprise or component solution.	We will help our clients to develop end-to-end security architecture approach to secure their enterprise both from the organisational/strategic level and from the more detailed technically detail level. Standard approaches like SABSA and TOGAF are used as reference to achieve this. Typical deliverables for this service are: architecture models (e.g. ArchiMate or Visio diagrams), HLD/LLD documents, roadmaps, process design and implementation etc.
Augmentation and Capacity Building	Supporting customers' Security Architecture function	We can support customers in creating and augmenting their own security architecture function, providing expertise to define processes and governance structures (like Design Authorities) and augmenting staff on a temporary basis from technical SMEs up to information security management.

1.5 Why PA Consulting Group (PA)? A trusted partner for cloud, AI, and digital technologies

PA Consulting Group (PA) is a leading technology and innovation consultancy and one of the UK government's most trusted advisors, combining strategy, delivery assurance and deep engineering to turn complex ambition into assured outcomes. We bring end-to-end capability across cloud architecture, data and AI, cyber, and advanced technology R&D, backed by a track record of scaling innovation in the public and private sectors.

Our UK work is anchored by secure, standards-led delivery. PA maintains ISO/IEC 27001 certification across global operations, demonstrating disciplined information security and operational control, and applies UK government good practice (GDS, NCSC CAF) across cloud and digital programmes.

We combine consultancy with real engineering. At our Global Innovation & Technology Centre (Cambridge), 300+ scientists, designers and engineers operate extensive labs and studios to prototype and industrialise solutions, bridging physical and digital from concept to production.

1.5.1 Why PA for cloud, data and AI

- **Hyperscaler alliances without vendor lock-in.** PA is Premier Tier with **Google Cloud** (13+ years; 150+ certifications; specialisations in infrastructure, data analytics, app dev and security) and holds deep **AWS** and **Microsoft** credentials, accelerating secure data foundations and generative AI at scale while keeping advice independent and outcome-led.
- **Responsible AI you can trust.** Our Responsible AI framework, governance toolkits, and risk policy make AI adoption transparent, auditable, and compliant, embedding lifecycle controls, model documentation, and human-in-the-loop safeguards aligned to evolving regulation.
- **Impact beyond pilots.** We help organisations become *intelligent enterprises*, using data and agentic AI to create and protect value, with pragmatic roadmaps from use-case selection to scaled operations.
- **Proof through delivery.** Our client stories span enterprise data platforms, IoT and analytics (e.g., Rentokil Initial), and product innovation at scale (e.g., Unilever) where PA has put data and AI at the heart of continuous, market-leading improvement.

1.5.2 Cloud capability (assess, design, build, assure, run)

PA applies an assured cloud delivery approach to complex government and regulated environments, blending client-side delivery assurance, multi-cloud architecture, and resilient operations:

- **Strategy & readiness.** Maturity assessments, target operating models for hybrid/multi-cloud, and cost/benefit modelling; proportionate GDS compliance and ISO 27001 controls embedded upfront.
- **Design & architecture.** Secure, well-architected patterns across Azure, AWS, and Google Cloud; data platforms, identity and access, and cross-domain solutions for sensitive estates.
- **Build & deploy.** Cloud-native engineering, DevSecOps (CALMR), CI/CD, infrastructure-as-code; automated testing and quality assurance to accelerate safe release.
- **Migration & modernisation.** Legacy transformation, platform reviews, and workload migration tuned to resilience and cost; pragmatic FinOps to keep spend predictable and efficient.
- **Operate & optimise.** Observability, incident management, performance tuning, backup/restore, and change management, maintaining business continuity and reducing total cost.
- **Client-side delivery assurance.** Forward-looking, risk-based assurance that keeps complex programmes on track, covering governance, architecture, testing, migration, service readiness and cutover. See our *IT Delivery Assurance* service.

1.5.3 AI, ML and data (from strategy to scale)

- **Strategy & governance.** AI blueprints, operating models, and policy; enterprise data governance; regulatory readiness; centre-of-excellence setup and change adoption.
- **Engineering & MLOps.** Data platforms on Azure/AWS/GCP, pipelines and feature stores; robust ML lifecycle with monitoring, drift detection and auditability.
- **Generative & agentic AI.** Secure integration of LLMs (including Copilot) into workflows for measurable productivity and quality gains, using guardrails, system cards and ROI framing.
- **Responsible AI.** Lifecycle controls and assurance tooling to manage bias, security and transparency.

1.5.3.1 Quantum and emerging technologies

PA's applied physics and quantum engineering teams help clients unlock near-term value, combining quantum techniques with classical systems for decision support, advanced sensing and secure communications:

- **Decision support & optimisation.** Hybrid quantum/classical algorithms to accelerate complex planning, routing and resource allocation where speed and quality of decisions matter.
- **Quantum sensing & RF.** Novel quantum radio and Rydberg-based sensing to enhance spectrum use, detection sensitivity and resilience in contested environments.
- **Commercialisation insight.** Advisory at the "whole-stack" level, hardware, supply chain, interfaces, and ethics, to move from lab to market within national strategies.

These capabilities are industrialised at our Cambridge centre, turning concepts into robust prototypes and pre-production systems across sectors like defence, energy and transport.

1.5.4 Cyber security and digital trust

Digital trust is central to PA's approach. We design security into architecture, operations and culture, aligning to NCSC CAF and GovAssure, and delivering testing, red-team, SOC design and OT/IoT security:

- **Transformation & architecture.** Secure-by-design patterns, cloud security, identity, and cross-domain data protection (including NCSC-approved Oakdoor data diode products).
- **Assurance & regulation.** CAF/GovAssure alignment and pragmatic remediation plans for government organisations.
- **Testing & resilience.** CREST-aligned penetration testing, red-teaming, incident readiness, and operational resilience.

1.5.5 What PA will bring

Ideation & Strategy

- Cloud strategy and advisory services
- Cloud readiness assessments
- Cost/benefit and ROI modelling
- Security and compliance by design.
- AI/ML and data strategy (blueprints, operating model, governance) with Responsible AI policy and guardrails.
- Quantum opportunity framing and whole-stack commercialisation roadmaps.

Design & Architecture

- Bespoke enterprise and cloud architectures
- Integration with existing IT infrastructures
- Hybrid/multi-cloud design
- Continuity and disaster recovery
- Data platforms and MLOps patterns
- Security, privacy and resilience embedded by design in technical designs
- User-centred-design
- Secure cross-domain solutions and high-side/low-side integration where required.

Development & Deployment

- Cloud-native engineering
- Containerisation, microservices and serverless
- DevSecOps (CALMR) with CI/CD and automated testing
- Generative AI and Copilot enablement with measurable productivity outcomes and run-controls.

Implementation & Migration

- Data migration and legacy modernisation
- Vendor selection and management
- Infrastructure-as-code with progressive, low-risk cutover.

Operations & Management

- Observability, incident management, SIEM/SOC design
- Performance optimisation and cost management (FinOps)
- Backup/restore
- User training and change adoption.

Innovation & Scaling

- Scalable cloud infrastructure to support growth
- AI/ML implementation and scaling
- IoT integration
- Ongoing innovation sprints and R&D, supported by our Cambridge engineering labs for rapid prototyping and pre-production.

1.5.6 PA is fully equipped to manage any challenges or requirements you may present

Across strategy, design, build and run, PA blends independent advice with hands-on engineering, operating to ISO 27001 and UK government standards, and backed by hyperscaler partnership depth. Whether the brief is modernising a sensitive cloud estate, industrialising AI responsibly, or de-risking a quantum-adjacent programme, we bring the multidisciplinary team to get from idea to reality, safely, quickly, and at scale.

1.6 A Genuine commitment to Social Value

At PA, we believe in the power of ingenuity to create a positive human future. Central to this ambition is our commitment to developing high-quality opportunities that enable individuals to acquire leading-edge skills, all within an environment that supports personal wellbeing and growth. We invest in our people through comprehensive training and development, ensuring they are fully prepared to tackle our clients' most complex challenges and advance their own careers.

We recognise that diversity drives innovation. Therefore, our recruitment practices are inclusive, welcoming individuals from all backgrounds. Every member of our team is empowered to reach their full potential through inclusive policies, processes, and a culture that is continuously improved using robust data.

We are passionate about creating genuine opportunities for those facing significant barriers to employment. Since 2023, our Digital Apprenticeship Programme has offered a Digital and Technology Solutions Degree through the University of Roehampton or Northumbria University. Our apprentices typically include first-generation professionals, college leavers, and individuals from ethnic minority backgrounds, many living in deprived areas. Additionally, we offer summer internships for undergraduates entering their final year, hosted at both our central London office and the Global Innovation and Technology Centre in Cambridge.

Economic responsibility is integral to our purpose. PA is accredited as a Living Wage employer, and where relevant, we ensure that our suppliers and subcontractors are paid at least the minimum living wage. We are also a signatory to the Prompt Payment Code, demonstrating our commitment to fair and responsible payments to suppliers.

Our carbon reduction targets have been validated by the Science Based Targets initiative (SBTi). We have a published carbon reduction plan and are committed to achieving carbon net zero by 2040, in alignment with PPN 06/21 criteria for UK public sector contracts exceeding £5 million. In 2024, we achieved a silver EcoVadis rating, reflecting our ongoing progress in sustainability.

We are dedicated to delivering targeted social value and will collaborate with you to determine the most effective approach for you, ensuring our efforts have the greatest possible impact.

1.7 Security Clearance

PA are fully compliant with industry best practices for information security, which includes compliance with the UK MOD Industry Personnel Security Assurance (IPSA) standard, against which we are independently audited every three years. PA also has multiple sites with FSC (previously List X) where our dedicated in-house Security Vetting team are based. This allows PA to achieve security vetting of its employees in a time effective manner ensuring the correct processes are always followed (In accordance with the Security Policy Framework/GS007). As a matter of standard process, PA puts all its eligible employees through the Baseline Personnel Security Standard (BPSS), set out by the Cabinet Office. Those employees working on, or planning to work on, government projects are automatically put forward for SC clearance which are processed via UK-SV (formally the Defence Business Services – National Security Vetting). PA also process DV vetting through the UK-SV and other agencies, these are generally client sponsored.

PA currently have a large pool of cleared individuals (80% of UK Staff). Should a resource be identified where clearance is needed, the PA Security Vetting team will then process the individual through the relevant clearance procedure. The team will also be able to validate all existing clearances held by PA employees when requested.

1.8 Next Steps

This service is intended to help customers develop and deliver successful outcomes regardless of the life cycle stage they are at. PA prides itself on working with clients and helping them to deliver outcomes whilst also providing them the ability to ‘stand on their own’ so that they can move their solutions forward without future involvement. Please contact us on GCloudFramework@paconsulting.com to discuss your needs further.

About PA.

We believe in the power of ingenuity to build a positive human future.

As strategies, technologies, and innovation collide, we create opportunity from complexity.

Our diverse teams of experts combine innovative thinking and breakthrough technologies to progress further, faster. Our clients adapt and transform, and together we achieve enduring results.

We are over 4,000 strategists, innovators, designers, consultants, digital experts, scientists, engineers, and technologists. And we have deep expertise in consumer and manufacturing, defence and security, energy and utilities, financial services, government and public services, health and life sciences, and transport.

Our teams operate globally from offices across the UK, Ireland, US, Nordics, and Netherlands.

PA. Bringing Ingenuity to Life.

Discover more at paconsulting.com and connect with PA on LinkedIn and X.

Corporate Headquarters
10 Bressenden Place
London
SW1E 5DN
+44 20 7730 9000

paconsulting.com