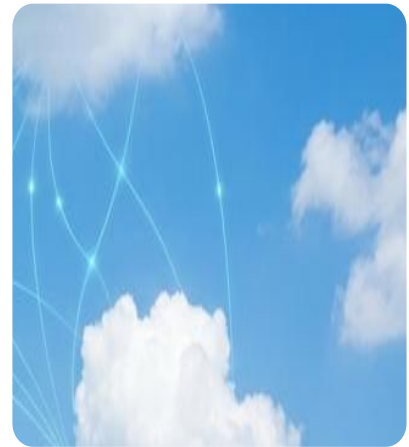




Crown  
Commercial  
Service



# AI Security

---

GCloud Service Description Document

**Bringing Ingenuity to Life.**  
[paconsulting.com](https://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

|                                                                                             |    |
|---------------------------------------------------------------------------------------------|----|
| AI Security                                                                                 | 4  |
| 1.1 Short Service Description                                                               | 4  |
| 1.2 Key Service Features                                                                    | 4  |
| 1.3 Key Service Benefits                                                                    | 4  |
| 1.4 Service Definition                                                                      | 5  |
| 1.4.1 AI <b>Security</b> advisory                                                           | 5  |
| 1.4.2 <b>Secure Design and Development</b> for AI systems                                   | 5  |
| 1.4.3 <b>Leverage AI to Protect from Cyber Attack</b>                                       | 6  |
| 1.5 Why PA Consulting Group (PA)? A trusted partner for cloud, AI, and digital technologies | 6  |
| 1.5.1 Why PA for cloud, data and AI                                                         | 6  |
| 1.5.2 Cloud capability (assess, design, build, assure, run)                                 | 7  |
| 1.5.3 AI, ML and data (from strategy to scale)                                              | 7  |
| 1.5.3.1 Quantum and emerging technologies                                                   | 7  |
| 1.5.4 Cyber security and digital trust                                                      | 8  |
| 1.5.5 What PA will bring                                                                    | 8  |
| 1.5.6 PA is fully equipped to manage any challenges or requirements you may present         | 9  |
| 1.6 A Genuine commitment to Social Value                                                    | 9  |
| 1.7 Security Clearance                                                                      | 10 |
| 1.8 Next Steps                                                                              | 10 |



# AI Security

## 1.1 Short Service Description

PA's AI Security approach enables clients to understand and use AI ethically and securely. Secure design and development of AI help assure AI products are secure-by-design, considering relevant use case threats. Leveraging AI to protect from cyber-attack enhances and strengthens security programmes by addressing automation, orchestration and AI augmentation.

## 1.2 Key Service Features

1. Mapping AI use across the enterprise
2. Conducting AI security risk health check
3. Helping leaders navigate a complex and evolving landscape
1. Application threat assessment, monitoring and maintenance
2. AI Secure-by-design, secure development, testing and deployment
3. Identifying attacks using MITRE ATLAS, Microsoft Failure Modes, Google SAIF
4. Validating defence in depth to identify the best places to deploy AI defences
5. Specifying AI specific requirements and architecture principles
6. Developing security roadmap aligned with organisational and technological ambition
7. Looking across people, process, technology to innovate when creating defences.

## 1.3 Key Service Benefits

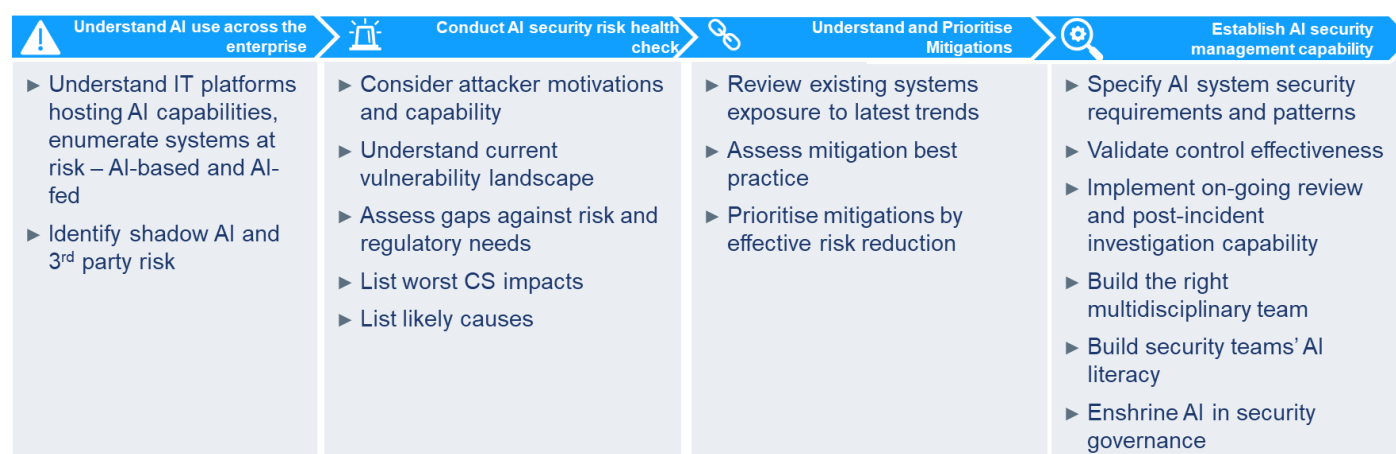
1. Understanding IT platforms hosting AI capabilities
2. Identifying shadow AI and third-party risk
3. Building security teams AI literacy to improve security capability
4. Implementing AI-aware data governance and protection
5. Adopting cutting edge approaches/technology to reduce compromise/breach likelihood
6. Reducing employee burden/workload with automation, orchestration and AI
7. Risk assessment improvement of supply chain compromise and data provenance
8. Upskilling teams to use AI security tools to increase effectiveness
9. Providing advice and guidance on relevant AI security updates.

## 1.4 Service Definition

### 1.4.1 AI **Security** advisory

Use of AI is rapidly growing, often in unplanned and ungoverned ways, for example the huge uptake of generative AI services such as ChatGPT. It is a challenge for security, privacy and data governance leaders to understand adoption and deployment of AI across the enterprise and the security risks this presents such as unclear supply chains, unsecure training data or disclosure of sensitive data to AI systems.

We help security leaders understand and secure organisational use of AI – including identifying ‘shadow’ AI use by employees, assessing suppliers and vendors to map and mitigate emerging threats and provide a framework for ongoing management of AI risk. Our approach is explained further in the following diagram.

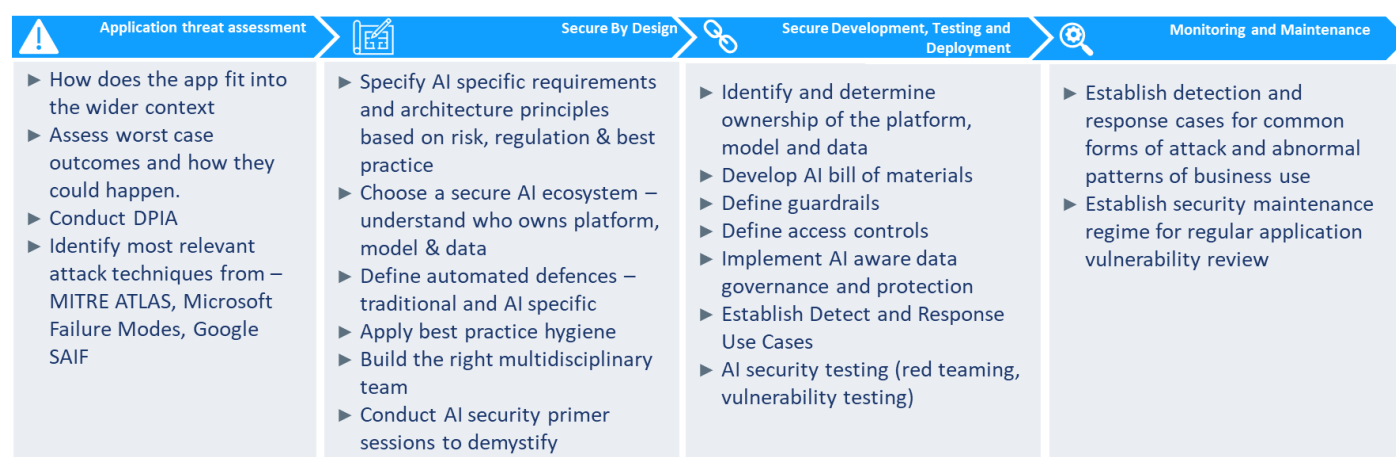


### 1.4.2 **Secure Design and Development** for AI systems

We work with clients to ensure the innovative development of AI systems. The nature of these – both their innovative business use, and the evolving AI technology and threat landscapes, mean that they face distinct security challenges – they can be attacked in different ways, with different business consequences.

We have enhanced and refined our tried and tested approaches to secure-by-design and secure development to address the unique challenges and threats associated with AI.

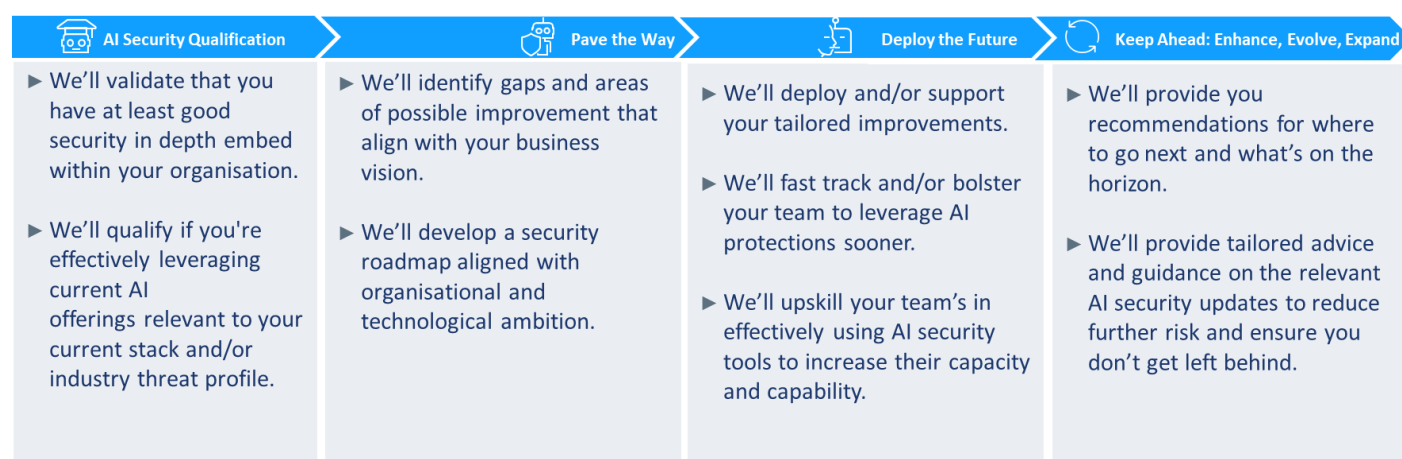
This includes constantly updated assessments of the threat to systems and the application of emerging standards and frameworks. Our approach is explained further in the following diagram.



### 1.4.3 Leverage AI to Protect from Cyber Attack

The security landscape is continually changing as are ways to leverage AI to do business. In this part of our service, we look across people, process, and technology to innovate your cyber security defences. We look to find features and new ways of working to significantly save cost, increase monitoring capacity and reduce organisational risk.

Our approach is explained further in the following diagram.



## 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](mailto: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](https://paconsulting.com) and connect with PA on [LinkedIn](#) and [X](#).

### Corporate Headquarters

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

This proposal has been prepared by PA Consulting Group on the basis of information supplied by the client, third parties (if appropriate) and that which is available in the public domain. No representation or warranty is given as to the achievability or reasonableness of future projections or the assumptions underlying them, targets, valuations, opinions, prospects or returns, if any, which have not been independently verified. Except where otherwise indicated, the proposal speaks as at the date indicated within the proposal.

[paconsulting.com](https://paconsulting.com)

All rights reserved

© PA Knowledge Limited 2026

This proposal is confidential to the organisation named herein and may not be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical or otherwise, without the prior written permission of PA Consulting Group. In the event that you receive this document in error, you should return it to PA Consulting Group, 10 Bressenden Place, London, SW1E 5DN. PA Consulting Group accepts no liability whatsoever should an unauthorised recipient of this proposal act on its contents.