



Crown
Commercial
Service



CLOUD AND CRITICAL NATIONAL INFRASTRUCTURE

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

CLOUD AND CRITICAL NATIONAL INFRASTRUCTURE	4
1.1 Short Service Description	4
1.2 Key Service Features	4
1.3 Key Service Benefits	4
1.4 Service Definition	5
1.5 Why PA Consulting Group (PA)? A trusted partner for cloud, AI, and digital technologies	7
1.5.1 Why PA for cloud, data and AI	7
1.5.2 Cloud capability (assess, design, build, assure, run)	8
1.5.3 AI, ML and data (from strategy to scale)	8
1.5.3.1 Quantum and emerging technologies	8
1.5.4 Cyber security and digital trust	8
1.5.5 What PA will bring	9
1.5.6 PA is fully equipped to manage any challenges or requirements you may present	10
1.6 A Genuine commitment to Social Value	10
1.7 Security Clearance	11
1.8 Next Steps	11



CLOUD AND CRITICAL NATIONAL INFRASTRUCTURE

1.1 Short Service Description

Our Critical National Infrastructure & Cloud service provides an approach to architecture and cloud delivery of your mission critical CNI services. The design and delivery of such solutions requires significant control, governance and leadership where quality isn't negotiable to ensure operational resilience, security and other highly critical requirements are met.

1.2 Key Service Features

1. Utilise existing CNI experience across all architecture layers
2. Understand complexity of scaled CNI technical and business architecture
3. Develop architecture principles and guardrails aligned to CNI standards
4. In depth knowledge of key security requirements and standards
5. Target Business and Technical Architectures defining your target state
6. Transition Architectures and roadmaps to the target state
7. Proactive management of architecture backlogs to manage architecture risk
8. Leverage PA's unbiased partnerships with Google, Microsoft and AWS
9. Business Capability Model for your critical business services
10. Technical Capability Model needed to match your business capabilities

1.3 Key Service Benefits

1. Reduce risk: early detection of compliance and architectural risk
2. Compliance: combine cloud, government and regulator best practice/standards
3. Assurance: embed adherence to requirements and control exceptions
4. Insight: based on CNI design and delivery experience
5. Scale quickly: 300+ architects and broader delivery capabilities
6. Cloud security and resilience via up-front strategic considerations
7. Traceability: Line of sight from business to technical capabilities
8. Governance: manage and reduce burdensome architectural assurance
9. Journey: Clear architecture roadmaps and transition architectures
10. Metrics: Clear traceability to a set of agreed KPIs

1.4 Service Definition

CNI programmes are unique and distinctive, there are a series of pitfalls not experienced elsewhere, and the level of rigor to maintain the integrity of the end-product whilst delivering at pace, needs control, governance and leadership. Our hands-on experience buying, designing and delivering CNI solutions into the most secure environments where failure is not an option, allows us to successfully provide services ranging from enterprise architecture to low level detailed infrastructure, data and application designs to being embedded within delivery teams and running of these services.

Whilst most architecture approaches are valid in such environments there are distinctive differences between a regular and CNI architecture and its delivery:

1. **Compliance:** solutions need to align with various guidelines and standards such as from NCSC, cloud suppliers, supervisory bodies and wider industry. Compliance and the evidence thereof is a continuous process starting during early phases including transition state definition, going into low level designs, testing and operational running. Retrospective compliance can be extremely costly if this mandates changing the core of a technical or business design so continuous control is paramount.
2. **Assurance:** extreme levels of criticality require significantly more assurance to internal and external stakeholders ensuring the right solution is bought, build, designed, delivered and changed. Whilst compliance supports assurance it is not the only means to gain trust into technology, people and services being provided. By taking assurance into account upfront it can be better planned for and limiting impact on delivery.
3. **Requirements traceability:** CNI focussed transformation is often at a scale where traceability of initial designs to operating the service can become diluted in their meaning and understanding. Where these concern requirements as specifically found within CNI such as resilience, security and service this is not an acceptable position. Utilising the right tools, governance and approaches enables full traceability into the end state.
4. **Security and resilience:** Whilst always part of any architecture, the criticality of CNI requires extreme levels of security controls to minimise risk of services being interrupted. Confidentiality, integrity and availability form the backbone of the technical and business architectures. Closely related are the levels of resilience built into the system, people and processes. It is important the drive to create a resilient solution does not result in more weaknesses introduced effectively making it less resilient. We bring our own security and resilience SMEs with hands-on experience and combine this with best practice from cloud suppliers, government security organisations and regulators to ensure your requirements can be met and are evidenced through testing and regular exercises.
5. **Risk based design and testing:** threats to service (confidentiality, integrity and availability) need to be understood and tested at an unparalleled level of detail requiring architecture and technical expertise to define the likelihood and impact of failures so this can be tested and mitigated for. Through upfront work an exhaustive view can be created and matched to risk acceptance levels.
6. **Risk management:** even minor architecture risks can become a threat to success in an environment where quality is paramount. Earlier identification is critical and the right capacity needs to be allocated to manage these whilst still managing overall delivery.
7. **Integrated design:** often technical designs and delivery are to extent remote from the business and operational activities. CNI designs must however take an approach where service is at the forefront as operational resilience is the primary business objective. By embedding architecture and business within each other's teams from upfront design all the way into service enables truly integrated technical and business designs.

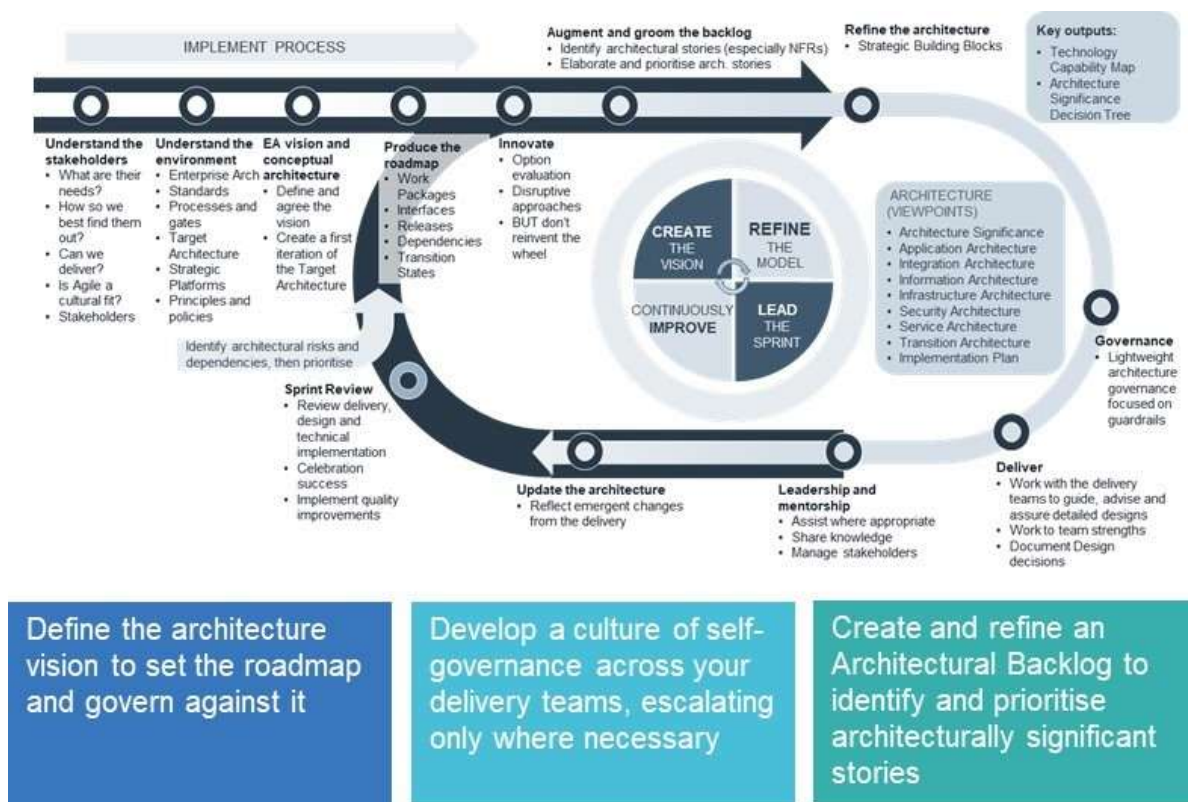
Whilst CNI architecture is unique and emphasises various activities it integrates with common architecture approaches. PA's Architecture Assurance Process recognises the need to be

iterative, flexible and work through the increased level of governance and milestones CNI programmes must go through.

Architecture Assurance Process

The architecture approach sets the vision and target architecture, focus on the boundaries that delivery teams can operate within and produce roadmaps to address the architectural backlog. In this way, we create a streamlined approach that accelerates project delivery whilst managing CNI specifics. In this we will:

- Define the architecture runway and associated backlog focussing on Technical and Business designs and their alignment
- Define the transition states to mitigate overall delivery and operating risks
- Identify and mitigate architectural risk
- Prioritise the architecture focus based upon the architectural risk
- Utilise best practice from cloud suppliers, provide wider industry and hands-on experience and ensure alignment with regulatory frameworks and government security approach
- Work and utilise existing relationships with cloud suppliers, government agencies and regulators to enable early buy in and guidance to help define the transition and end state(s).
- Define the architectural policies and standards for delivery to operate within



Target Architecture and Roadmap

A key early output will be to define the Target Architecture so that the direction is clear, this is critical for CNI programmes where rework can be particularly expensive. From the Target Architecture we then develop a roadmap in collaboration with business and technical teams with the objective to minimise the end-to-end delivery and operational risks to all internal and external stakeholders. The approach to breaking down the transition states is subject to finding a balance between speed of delivery, overall risks, change volume being introduced and quality standards that must be met.

To complement these states, we will define a set of associated capabilities views, standards and patterns libraries. All these will be provided as accessible and easily maintainable digital tools.

What does this give you?

- A clear and visible view of the target state.
- Clear linkage between the business capabilities and the technical capabilities that enable their delivery.
- Clear set of transition states to be able to move to the target state.
- Set of clear standards, patterns and principles to be used across the suite of delivery initiatives.

What do the deliverables look like?

- Set of enduring Principles that future IT programmes should apply
- Decomposition of capabilities highlighting the relative strength displayed for each across the organisation
- Collection of artefacts that describe the existing high-level architecture
- Clear roadmap that reflects the organisation's priorities for future programmes of work – Driven through Gap analysis of Capabilities and Current Architecture against Business priorities

Insights and lessons learnt

- Share the knowledge freely – don't be too private
- Endorse the profile of the EA function across the organisation
- Create and maintain an Architecture Backlog



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

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

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.