Crown Commercial Service

PENETRATION TESTING

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

PENETRATION TESTING

1.1 Short Service Description

PA Consulting provides Cyber Security services including CREST accredited Penetration Testing. Our experience enables us to provide assurance of critical systems, including cloud (AWS, Azure, GCP) and hybrid environments. We can assess endpoints, build and configuration, firewall rules, switches, infrastructure, Active Directory, embedded devices, mobile and binary applications.

1.2 Key Service Features

1. CREST Certified Security Professionals vetted to SC Levels
2. In-depth assessment of Infrastructure Configuration, Web and- Cloud-Based Applications
3. Requirements driven, tailored security testing
4. Comprehensive reporting - Executive Summary, Identified Vulnerabilities and Recommendations
5. Reproducible steps to validate and replicate identified vulnerabilities
6. Assessment against Industry Best-Practice, Vendor Guidance, recognised Security Baselines
7. Providing relevant Common Vulnerabilities assessment and Exposures (CVE) information
8. Internal or External, Black-Box or White-Box security testing approaches.

1.3 Key Service Benefits

1. Trusted security specialists cleared through National Security Vetting processes
2. Prioritisation and mitigation advice included in vulnerability remediation plans
3. Enhanced Assurance of Systems and Services processing Information Assets
4. Expertise leveraged from experience across all Industry Sectors
5. Risk ratings based upon threat, impact, ease of exploitation
6. Enhanced threats understanding by working closely with Client Teams.

1.4 Service Definition

PA works closely with clients to convey and help eliminate security weaknesses, and our consultants feature prominently in the global cyber security arena as a result of their security research. For example, research into trust zone exploitation in relation to embedded devices assessment.

We pride ourselves on being staunchly independent and on being an active member of many professional groups such as the Certified Register of Ethical Security Testers (CREST) and we are accredited to practice and audit for ISO 27001.

Our core services for Penetration Testing include:

- Internal and External Infrastructure Assessments
- Security Assessment of Web Applications and Web Services
- Mobile Application Assessment
- Binary Application Assessment
- Code Review of Applications
- Database Assessment
- Design and Architecture Review (Threat Modelling)
- Social Engineering and Phishing Assessments
- Embedded Device Security Assessments
- Cloud Configuration Reviews

1.4.1 Internal and External Infrastructure Security Assessments

Organisations are often concerned about the security of their internal and external facing infrastructure. An internal Infrastructure security assessment usually implies that an organisation wants to identify whether a user who has access to internal resources can gain unauthorised access to information. Unauthorised access can be gained in several ways, including (but not limited to) weak/default passwords, compromise of Enterprise Active Directory services, poorly configured systems or missing security patches.

Similarly, an external infrastructure security assessment implies that the organisation wants assurance that the components and servers presented externally (on the Internet) are well configured and do not suffer from any security vulnerabilities that could be leveraged or exploited by an attacker.

1.4.2 Security Assessment of Web Applications and Web Services

A web application is an application that is accessed via web browser.

A web application assessment is carried out to ensure that the web application has a satisfactory level of security, and that the organisation's data, confidentiality, integrity and availability are not exposed to unacceptable risk.

Our web application security assessment methodology involves analysing the application for design weaknesses and technical flaws at the interface and, where possible, in the code itself. The application testing will involve systematic analysis of the application, regardless of the development language.

While assessing web applications and web services we follow the Open Web Application Security Project's (OWASP) recommended testing methodology and guidelines.

1.4.3 Mobile Application Assessment

With the increased popularity of smart phone devices in recent years, their presence in business has also subsequently increased.

Once downloaded onto a user's device they allow various functions to be performed, much in the same way applications are run on a computer. Examples of areas in which applications

operate in include banking, e-commerce, and e-books. Typically, mobile applications interact with a server on the internet in the same way web sites do, therefore a major phase of mobile application testing is performed in a similar fashion. It is also paramount that any information stored by applications on the mobile device is kept secure due to the possibility of such a device being misplaced. PA includes this in all testing to protect both the end user and service provider. Examples of common attack vectors include unauthorised access to information, privilege escalation, access to business-critical data, and security of data at rest or at transit. PA delivers security assessment of iOS and Android based applications.

1.4.4 Binary Application Assessment

A wide variety of binary applications are usually deployed within an organisation. These applications can suffer from several security vulnerabilities which create risk when exploited by a threat actor, including loss of an organisation's reputation, financial frauds, loss in confidentiality, integrity and availability of an organisation's data. We analyse binary applications against several security vulnerabilities. These include design flaws, authentication flaws, input validation, security of data in transit, secure communication, logical flaws and many more.

1.4.5 Code Review of Applications

Alongside penetration testing, web application testing and other forms of application testing, we see the need to undertake a code review to ensure rigorous levels of information security and secure coding are in place. Whilst penetration testing and application testing examines code that is running and executed, very often in more complex application testing scenarios, there will exist code that may have security flaws buried deep inside it. A code review therefore allows the penetration tester to review the lines of code or modules directly to check for flaws such as input validation, flaws in scripts and connectivity security with databases. When coding reviews are undertaken in conjunction with a full penetration test the consultant can test an application in its "live state" and then check for flaws in the code thus making the overall process efficient and comprehensive.

1.4.6 Database Assessment

Database security is the most undervalued component of an organisation's security and hence the most vulnerable. Our consultants analyse the security of the database from several perspectives, which include:

- Attacks from internal users (authenticated and un-authenticated access)
- Security of the data within the database (e.g. encryption/hashing techniques used for storing sensitive data)
- Database hardening and security
- Protecting sensitive data from privileged users (e.g. DBA)
- Defence in depth mechanisms.

We have expertise with many popular database products including (but not limited to), such as Microsoft SQL Server, Oracle Database, MySQL (all versions and all platforms), Amazon Relational Database, NoSQL, Cloud SQL, MongoDB and many others.

1.4.7 Review of the Design and Architectural Risk Analysis (Threat Modelling)

We understand that protection of information is a key asset for any organisation. As they grow, they will either have to buy or build new systems to interact with this information. The level of security of these systems starts with the architectural design.

Architectural Risk Analysis, also known as Threat Modelling, is the process of analysing the design of a system and identifying potential security weaknesses. It looks at the design from multiple facets and determines how the system will interact with potential attacks. It will examine the mitigations that are built into the design and evaluate them against these possible attacks.

The Architectural Risk Analysis methodology that we follow is described below.

Stage 1: Security Requirements Analysis
Stage 2: Architectural Risk Analysis
Stage 3: Reporting

As with all our assignments a report will be provided and on request, a presentation can be provided documenting the findings of the test and the recommendations. A high-level management summary will be included followed by an in-depth description of the elements of interest, the various views with findings and their substantiations.

1.4.8 Social Engineering and Phishing Assessments

Social engineering is the process of manipulating or deceiving a person(s) into performing actions or divulging sensitive information. Readily available information may allow an attacker to obtain details about an organisation, employees and the infrastructure utilised by them. We recognise that all organisations are different and as such a personal approach will be undertaken by our consultants.

We offer Social Engineering Services which can be separated into the following stages:

Stage 1: Information Harvesting
Stage 2: Phishing Assessment
Stage 3: Social Engineering Threat Assessment (S.E.T.A.)
Stage 4: Social Engineering Penetration Test (S.E.P.T.)
Stage 5: Reporting.

The aim of all stages is the extraction of company information. This may include information on employees, company information, internal and external IT infrastructure and other information that may be seen as relevant to each individual test. The methods in which this is achieved vary depending on the stage in which the test is conducted.

While assessing cloud-based web applications and web services we follow the Open Web Application Security Project's (OWASP) recommended testing methodology and guidelines.

1.4.9 Embedded Device Security Assessments

We take a holistic approach when assessing consumer, enterprise embedded devices, analysing both the software implementation and hardware design with a focus on whether the device takes reasonable steps to protect against its perceived threats. Where threats are not known, we can assist in a threat modelling process.

This can include assurance for example that a device follows good security practice to prevent unauthorised access to physical diagnostic ports and that hardware security features are enabled e.g code read-out protection. Additionally, reverse engineering of software may take place to ensure software exploit mitigation is in place and that known vulnerable code patterns or functions are not in use.

Where the ecosystem extends to additional services such as the use of mobile applications, these too can be considered for an assessment.

A high-level an assessment of a single device would include but not be limited to the following, where visibility can be obtained:

- Network based services e.g. SSH, web-based interfaces and CGI based-services
- Physical interfaces (UART, USB etc) (where applicable, can be identified and unlikely to cause destruction)
- Review of bespoke network-based attack surfaces to highlight potential security flaws i.e. buffer overflows
- Identification of weak or otherwise default credentials and or key material (such as hard-coded SSH keys or engineer passwords) - via inspection of available data, including firmware and via inspection of a running device's system (where underlying system access can be gained)
- Poorly implemented authentication, authorisation or credential transport mechanisms
- Analysis of firmware update mechanism (if applicable) – susceptibility to traffic sniffing, network on-path attacks, lack of encryption, authentication and or verification mechanisms
- Use of insecure protocols and or transport mechanisms when sending sensitive data generally
- Insecure ecosystem – when identified and applicable, passive analysis S3 storage buckets
- Analysis of device management including logging, alerting and monitoring
- Wireless network security - testing for notable wireless attacks such WPS pin brute-forcing and fragment attacks (where applicable)
- Firewall - review of WAN/LAN-based firewall controls and guest network functionality

1.5.0 Cloud Configuration Reviews

We recognise organisations are migrating resources to the cloud more and more frequently, and thus cloud-hosted applications and hybrid Enterprise environments are becoming more common. We can review cloud environments including but not limited to Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP).

Our approach to cloud testing employs both automated and manual assessment against applicable security standards, such as the CIS and applicable platform specific benchmarks. We use both the cloud service provider tooling, as well as other suitable tooling depending on the nature of the environment and the scope of the assessment.

As part of our baseline assessment, we will consider the following core elements as part of our cloud security assessment:

- User Access Control
- Environment Monitoring
- Network Security
- Resource Security
- Public Facing Footprint

Where required, scenario-based testing can also be conducted, for example to determine if an assumed breach of a cloud-application could result in a further breach of unintended cloud resources, whether a resource could be compromised to gain unintended access to the cloud environment, or whether an account’s permissions could be abused to elevate their privileges in the environment.

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