G-Cloud 14

PwC and G-Cloud: Knowledge, Experience, Value

PwC Cyber Security Consultancy Services

May 2024

pwc

Contents

Transforming Business using the Cloud

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

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

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

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

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

- Alignment of business and technology objectives. This is essential to fully realise the targeted benefits of any cloud transformation or any refinement of existing cloud services. There can be a tendency to adopt cloud systems to fit current ways of working, rather than adopt and standardise processes where possible. The trade-offs between business, customer and technology requirements must be considered to make informed design decisions;
- Availability and reliability of services. The avoidance of operational downtime to mitigate in lost revenue, unnecessary operational cost or reputational damage that can disrupt a business’ operations;
- Decentralised support structures. The need to tailor and revise the approach to operational security to cover the support structures employed by cloud service providers that will have a different risk profile for sensitive information.
- Data handling practices. Data classification and data-handling practices that reflect the data flow within a cloud environment must be understood and tailored accordingly to protect customer data.
- Data privacy. Compliance with GDPR to understand where and how information can be stored or processed. The cloud model enables data to bounce swiftly around the world by using available server capacity in various geographic locations, but this must be within the bounds of what is permissible. This is ever more of a concern as organisations review their front office, back office and out of office experiences.
- Future Technology Trends. Cloud applications are the stated direction of travel for the major application vendors, but any upgrade path must also cater for the future technology needs of the organisation and seek to minimise technical debt where possible.

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

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

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

Cyber Security Consultancy Services

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

Cyber Security Consultancy Services

Our Cyber Security Consultancy services offer expert security risk advice on a wide and complex range of cyber security areas, ranging from security transformation to targeted research & development.

Cyber Security Consultancy Services Features

- Cyber Security Transformation, Innovation & Change
- Cyber Security Strategy, Roadmaps, Requirements & Planning
- Security Architecture & Design
- Security Research & Development
- Cyber Security Advice & Guidance
- Security Review & Recommend
- Thought Leadership, whitepapers
- Large scale, complex, tailored, specific, urgent, effective, expert security support
- Supply Chain security, supplier security review
- Security incident advice and guidance

Cyber Security Consultancy Services Benefits

- Assist organisations in gaining confidence in their cyber security
- Address urgent security issues faced by Public Sector organisations
- Provide expert Cyber Security support, tailored to client requirements to assist with Preparing to defend against Cyber threats, ensuring Cyber threats are detected, and that organisations are resilient and can recover in the event of an incident
- Share and create security thought leadership
- NCSC Assured Cyber Security Consultancy
- UK wide & International delivery capability

Our views on the service features and benefits within this service definition document are presented below:

1. Cyber Security Transformation

We have developed a new approach to Transformation with Cyber Security built-in to improve resilience, reduce costs, and facilitate innovation with confidence.

We help our clients by providing solutions which address the fundamentals of security, aligned to their strategy but also based on data. We develop strategies and capabilities to combat cyber-threats; incorporating cyber-security into everyday business decisions and processes; and responding, investigating and remediate cyber security related incidents.

2. Research & Development

We have a dedicated in-house R&D capability which conducts technical and multidisciplinary research on vulnerabilities, attack and defence vectors, emerging technologies, and other security-related topics. Many of our projects are designed and executed in-house and published or presented at national and international conferences such as DEF CON, Black Hat USA, ISF Congress, and others. We also undertake bespoke research for clients on specific technologies and topics.

Examples of previous projects include:

- **Granular behavioural attribution** – statistical analysis of attacker keystrokes on compromised servers to perform case linkage analysis using logistic regression and ROC curves. This was presented at DEF CON in 2018 and featured in Wired.
- **Air-gap bypasses and drone attacks** – research into the use of infrared and high-frequency sound to issue commands to air-gapped machines, exfiltrate sensitive data, disrupt motion detectors and security devices, and interfere with the navigational system of drones. This was presented at DEF CON in 2017, as well as 44Con, BruCon, and ISF Congress
- **Remote Online Social Engineering** – exploring an emerging attack vector whereby threat actors assume long-term false identities on social media and establish rapport with targeted victims. This was presented at Black Hat USA in 2018, as well as ISF Congress.
- **Acoustic cyberweapons** – Examining the feasibility of attacking and repurposing various commodity smart devices as localised, low-cost acoustic weapons, together with an exploration of possible countermeasures. This was presented at DEF CON in 2019 and received international media coverage in the BBC, Metro, Wired, The Times, New York Times, Times of India, and various other publications and sites.
- **Human side-channels** – examining techniques to track, attribute and frustrate threat actors using forensic linguistics, behavioural analysis, and cultural references as a form of captcha. This was presented at Black Hat USA 2019, as well as ISF Congress, 44Con, and BruCon.

3. Supply Chain Risk Management

Supply Chain or Third Party Risk Management (TPRM) is an increasing challenge in an interconnected world. Challenges facing organisations continue to grow, and security of data is at the top of the agenda when engaging third parties. Although the maturity of TPRM varies across organisations and industries, risk management processes are often manual, time consuming, and require a high level of effort; leading to increased cycle times and leaving room for manual error. Some businesses are now looking for ways to optimise TPRM processes throughout their lifecycle by reducing cycle times, automating workflows, and streamlining processes.

PwC's TPRM team is composed of experienced professionals who help clients enhance how they manage third party risks and continue to identify opportunities to optimise TPRM processes and utilise technology to enhance efficiency and quality. We understand the important role vendor management plays in operations as you rely on numerous suppliers and contractors.

We believe that vendor management should be supported by an established and consistent Vendor Management Policy. A robust vendor management function allows organisations to realise the benefits of the relationships with vendors while maintaining a successful framework for managing and mitigating the IT and Security risks inherent in operating with third parties and ensuring compliance with contractual obligations.

We have strong experience in third party management. We developed and delivered supplier assurance methodologies and have successfully managed end-to-end many projects with big organisations like yours in the UK and internationally. Typically our TPRM services include:

- **Third Party Risk Management** – Clients are struggling to manage the myriad of risks associated with their use of third parties. We can support clients with this challenge by assessing, designing and operationalising a Third Party Risk Management Framework
- **Third Party Assessments** – Actually assessing third parties is an integral component of a third party risk management framework. We help clients develop and execute approaches that examine how their third parties are managing risks from the goods or services provided.
- **Third Party Technology** – Clients struggle to select, implement and utilise the right technology solution. We help clients define their solution requirements, evaluate and select fit-for-purpose solutions and partner to implement new technology into their business
- **Third Party Incident response** – Up to 75% of firms experience a third-party incident and do not have the capability or capacity to manage. We help clients by managing end to end remediation, ensuring no perpetuation of the incident and comprehensive root cause analysis'
- **TP Value** – Clients put significant effort into agreeing contracts with third parties. Over time, the anticipated value can fail to materialise. We help clients identify and recover value from third parties as well as defining practical, sustainable solutions to address underlying issues.

4. Security Architecture

- Help to implement security architectures and commensurate controls with risk profiles using our core Security Architecture Patterns which can be tailored to meet the individual needs of organisations to develop defensible and resilient solutions.
- Develop security architecture requirements for systems/services aligned to SPF and NCSC guidance.
- Development of Security Controls Catalogues – definition of standard sets of security controls – to enable reuse and standardisation within organisations (aligned to NCSC guidance and standards such as the ISO 27000 series, ISF Standard of Good Practice and NIST SP 800-53).
- Advice on how to build, implement and manage technology securely.
- Assist clients in network segregation – our 'Trust Zones' and 'Zero Trust' approaches help organisations to segment their environments to protect their critical assets.
- Implement "Privacy by Design" – our Privacy Architects work closely with our Legal experts to ensure that privacy law and regulations are supported in system architectures.
- Assist in development of services around SIEM technologies.
- Support organisations in designing their IdAM solutions to ensure that only the right people have access to critical data assets.