G-Cloud 14

PwC and G-Cloud: Knowledge, experience, value

PwC GBEST 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 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 to be 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 them:

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

PwC GBEST Services

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

PwC GBEST Services

Simulated targeted attack services using the methodologies of real-world attackers, including attacks against people and processes using social engineering techniques. Working either covertly or cooperatively with client IT and response teams as required.

GBEST Services Features

- Red team attacks including phishing, vishing, SMiShing and other social engineering techniques
- Simulated targeted attack
- Attacks based upon real world Threat Intelligence driven threat scenarios
- Mature risk management and delivery approach
- Cross discipline engagements uncover vulnerabilities across people, process and technology
- Certified under CREST STAR, STAR-FS, CBEST, GBEST, TBEST and NBEST schemes.
- Staff qualified to the highest levels
- Collaborative projects, working with clients to improve security posture
- Purple team and Rapid Find, Tune and Fix capabilities.

GBEST Services Benefits

- Identify vulnerabilities in applications and systems
- Discover weaknesses in your development and testing processes
- Better training for defensive practitioners (e.g. SOC or blue team)
- Assess security performance levels, including systems, people and processes
- Understand the impact of a security breach
- Measure the resilience of your organisation's cyber defence
- Collect evidence to justify security spending
- UK and worldwide delivery capability

The service features and benefits within this service definition document are presented below:

By understanding what real cyber-attacks look like we can see that traditional vulnerability scanning and penetration tests do not exercise all, or even most, of an organisation's controls. Exercises such as GBEST do not just focus on identifying weaknesses within technology but also look at security behaviours, detective controls and response capability. This allows us to provide a more holistic view on what a threat actor could really achieve during the course of a cyber attack.

A GBEST assessment will be requested by the Cabinet Office that uses threat intelligence to simulate an Advanced Persistent Threat (APT) targeting your digital estate. We will simulate an APT by adopting the tools, tactics and procedures used by real world-attackers. The assessment will determine the ability to detect and respond to the various stages of a cyber attack in accordance with the GBEST guidelines.

We have a wealth of experience working across UK government departments. We've successfully delivered a significant number of regulated, threat-intelligence led penetration tests, spanning across a wide range of UK schemes including GBEST, CBEST, TBEST, CREST STAR and STAR-FS. In addition we have experience delivering multinational projects through overseas schemes such as TIBER in Europe and Hong Kong's iCAST.

Security testing exercises set by regulators are complex projects with multiple stakeholders. We can bring our significant experience of running GBEST, TBEST and CBEST exercises, as well as other similar global initiatives, to help guide you through the process whilst delivering value to you and your key stakeholders.

We have a number of advisors working across Whitehall departments who are able to provide great value and insight into current trends and security concerns across many government departments. We are able to leverage this expertise and experience to build our capabilities and methodologies.

Our methodology and approach are practical and rooted in our deep existing knowledge of the industry and the cyber threats that truly affect our clients. We incorporate data from the threat intelligence team to develop in-depth and realistic attack scenarios. By being grounded in current threat intelligence, our testing lets you truly understand how a targeted cyber-attack would impact your organisation.

PwC is uniquely placed to support you for the following reasons:

1. Deep cyber security experience on a global scale – We have a world leading security practice from which we have selected the right team with a broad mix of skills including red team and social engineering subject-matter experts with industry leading qualifications and experience.
2. Our proven track record – We have worked extensively on regulated penetration tests, including GBEST, CBEST, and TBEST engagements. We also work with key stakeholders across these schemes such as the Bank of England and the Cabinet Office. We have wider global experience with similar schemes including Hong Kong's iCAST and the European Central Bank's TIBER-EU scheme.
3. Exceptional skills and expertise. An Ethical Hacking team that has been operational for over 10 years with a headcount of over 55 penetration testers. The team also holds leading industry accreditations such as CREST and CHECK – including CCSAM and CCSAS. Our testers have conducted red team security assessments for a number of organisations and across a wide range of industries.
4. Our staff hold a range of security clearances including those from the most sensitive organisations and have experience delivering many complex engagements across the range of classifications and sensitivities.
5. Our experience shows that a combination of technical expertise coupled with a broad range of experience enables us to provide a robust and innovative approach. PwC has staff with direct experience of performing security research for internal government clients and as such has a clear view of how key objectives can be achieved.
6. We believe that our skills and expertise will enable us to deliver the cross functional, yet board-friendly assessments that we know that you will expect from your chosen partner.

We are able to provide you with further information on our methodology as required to support your requirements.

.