G-Cloud 15

Information Assurance Audit & Review Services

January 2026

Contents

Transforming Business using the Cloud

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

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
- 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 them:

- As a partner through the complete lifecycle of strategy through to execution

- With point business issues encountered during implementation or running the business.

Information Assurance Audit & Review Services

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

Information Assurance Audit & Review Services

PwC performs independent assessment of maturity and compliance with security standards/guidance and propose improvements. We can also perform assessment of cyber frameworks and governance structures and cover due diligence of cloud solutions based on NCSC and HMG security guidance. We can provide an independent view on whether the cloud solution meets security objectives/outcomes/ HMG guidance.

Information Assurance Audit & Review Services Features	Information Assurance Audit & Review Services Benefits
• Security Review & Recommend • Security Assessment / Security Assurance • Security Audit and Compliance • Technical Security Review • Security Risk Review • ISO/IEC 27017, ISO/IEC 27001 and ISO/IEC 27002 • NCSC 14 Cloud Security Principles • Cloud Security Alliance Cloud Controls Matrix (CSA CCM) • NIST Cyber Security framework • Maturity assessment, maturity model improvement plan, due diligence assessment.	• NCSC Certified Cyber Services and Professionals (CCP) • UK-wide and International delivery capability • Independent assurance to the Board / senior management • Confidence that security controls are designed and operated effectively • Due diligence of the security posture of the supply chain • Security Benchmarking.

Our view on the service features and benefits in this service definition document are presented below.

We help our clients assess their current security posture, understand the information security risks of their technology, people and suppliers and mitigate these. We typically:

- Review the information security posture of an organisation via health checks against ISO/IEC 27002, SANS / CIS top 20 critical controls, Cyber Essentials, NCSC 10 steps to cyber security, ISF Standard of Good Practice for Information Security, SWIFT CSP. Propose improvements in a prioritised manner via an improvement plan and roadmaps

- Review technical design documentation to identify cybersecurity risks posed by the design of proposed technical solutions
- Controls Assurance is a particular service offering for which organisations rely on us to provide them with an appropriate level of assurance. We have experience in measuring and monitoring a range of industry-standard controls included within the ISO 27001 & 27002, COBIT and NIST 800-53
- Cybersecurity due diligence and divestiture readiness assessments
- Cybersecurity regulatory gap assessments across all major UK / EU regulatory frameworks (e.g., DORA, TSA, NIS, NIS 2, CAF)
- Review the organisational information security culture and propose improvements
- Review the cyber security strategy, governance, and risk management framework and propose improvements
- Review the security capabilities related to higher risk environments such as cloud and OT environments
- Deliver co-sourced internal audits across the security programme
- Carry phishing tests to understand and mitigate the threat to the organisation and help the client in focusing spending by understanding the exposure and training required
- Penetration testing and vulnerability assessments. PwC are a NCSC approved organisation with accredited penetration testers qualified to assess HMG systems up to and including SECRET classification
- Third party contract reviews to assess the information security / cyber content and propose improvements.