G-Cloud 15

Cyber Crisis and Resilience 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 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 better 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 Cyber Crisis Management Services

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

PwC Cyber Crisis and Resilience Services

We enable organisations to prepare for, respond to and recover from cyber attacks, including those that originate from, or affect, technology and data in cloud environments. We support organisations to identify their most critical business services and build resilience to all threats and risks, including cyber. We bridge the gap between technical challenges and strategic impacts of cyber incidents and crises through well-documented and exercised plans and processes. We provide live incident support and undertake post-incident reviews.

PwC Cyber Crisis and Resilience Services Features	PwC Cyber Crisis and Resilience Services Benefits
• Horizon scanning and scenario planning • Cyber crisis resilience - preparedness, response and recovery, including frameworks, plans, response guides and scenario playbooks • Incident and crisis manager training • Facilitated walkthrough, desktop and simulation exercises • Strategic live crisis management support • Post-incident reviews.	• An understanding of the risks and threats to identify gaps in crisis and resilience capabilities • Informed view of critical business services and ability to remain resilient in the face of disruption • Clarity on ownership and authority for response to cyber threats • Responders with skills and confidence for efficient response and recovery • Established frameworks, guides and tools to accelerate effective response efforts • Insight into root cause of incidents and crises and clarity on areas of strength and gaps for improvement.

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

1. Horizon scanning and scenario planning

Horizon scanning and scenario planning can help you to reduce uncertainty, spot faint threat signals before they occur, and identify opportunities. Our cyber crisis and resilience specialists can help you to:

- Identify the key threats facing your organisation, sector and industry. Understanding these threats allows you to identify any gaps in your planning and capability, and alter your risk and issues management processes and structures accordingly

- Determine your critical operations and establish the capability required to maintain fundamental systems and processes during periods of disruption

- Assess your proficiency and offer bespoke horizon scanning reporting on an ongoing basis.

2. Cyber crisis resilience - preparedness, response and recovery

All organisations need to be able to successfully respond to and recover from cyber attacks, including those that originate from, or impact, your cloud infrastructure. Our cyber incident and crisis specialists can help you to:

- Understand your Critical Business Services and the technology, people, premises and third parties you rely on to deliver them

- Understand your key gaps in your ability to maintain the resilience of these services. This includes a thorough analysis of your existing capabilities, such as incident and crisis management, and business continuity. This will identify prioritised areas for improvement in line with current industry best practice and standards

- Design an overarching cyber response and recovery framework. This will guide your core response strategy, link together all cyber and crisis response documentation, and provide clearly defined business objectives for your end-to-end response

- Develop documentation to underpin the framework and guide responders at all levels of your organisation. This includes cyber decision-making guides to aid senior decision makers, scenario-specific playbooks according to your most pertinent threats, and business recovery runbooks to manage the long tail of a cyber incident.

3. Incident and crisis management training

Your technical teams, senior leadership teams and Board need to know how to effectively respond during an incident, including to rapidly triage known facts, establish priorities, and factor these into the response strategy that aligns with your core values. Our training covers:

- Understanding of what an incident / crisis means for your organisation

- Decision-making and strategy development interactive exercises

- Cyber-specific challenges for responding to an incident and crisis

- Enhancing the relationship between technology domains and organisational leaders

- Effective meeting management
- Introduction of the psychological and physiological effects of crises
- Common pitfalls in incident management
- Good practice processes, skills and behaviours for effective cyber crisis management.

4. Desktop and simulation exercises

Once your key responders and executives have been trained in the theory of crisis response and your plans, we recommend a programme of exercising to build capability and develop maturity over time. Our exercising programme develops over three phases:

1. **Facilitated discussion-based walkthrough.** Provides the opportunity to embed your new frameworks and plans, increase familiarity with roles and responsibilities and sense check the new structures

2. **Desktop exercise.** This is the next step in complexity and challenge. Participants receive several injects at the start of each phase outlining the latest situation. They then typically carry out a mock incident management meeting, discuss next steps between themselves with relatively little facilitation. This provides the opportunity to rehearse your structures and processes in a safe and relatively calm, yet challenging, environment

3. **Simulation.** This is our most intense exercise and can involve multiple teams playing in parallel for several days. We simulate the real pressures of an incident using a combination of techniques including mock news feeds, phone calls, emails, social media etc. These exercises allow you to rehearse your capability under pressure and develop the 'muscle memory' on which you will rely during a real incident.

5. Strategic live crisis management support

Our specialist responders have a broad range of capabilities to provide you with rapid response support during a live incident. We can help to:

- Establish the strategic response structures which will coordinate decision making across all business functions
- Identify all stakeholders and develop a communication strategy that ensures they are appropriately engaged and informed where necessary
- Provide a project management office capability for the duration of the crisis or incident

- Investigate to determine the scope of malicious activity and impact to the business

- Plan the rebuild and recovery of the systems, applications and processes impacted by the incident or crisis with priorities agreed with functional leaders.

6. Post-incident review

Following incidents and crises, we can help to recover and restore your 'business as usual' operations, understand the root cause and address lessons learned by completing the following activities:

- Facilitate a post incident or crisis review to help establish root cause(s), identify lessons learned and form plans to address both

- Realign strategic programmes to ensure they are addressing the root cause(s) and lessons learned.