# G-Cloud 14

PwC and G-Cloud: Knowledge, experience, value

Cyber Resilience & Recovery
**May 2024**

pwc

# Contents

# Preparing to recover from destructive attacks

A successful cyber attack is a unique disaster scenario. Hosting environments, data and supporting services become untrusted and, as a result, effective recovery requires new capabilities. Considering these factors in advance can prevent severe impact to delivery of key business processes and services in the event of a cyber attack.

We have worked with many clients across the critical national infrastructure to support the effective review and improvement of cyber recovery plans. Our expert team has a diverse skill set including enterprise wide resilience, crisis management, IT disaster recovery and cyber incident remediation. Enabling effective business recovery is a strategic consideration facing many private and public sector organisations, especially as regulation in this area expands.

While many organisations have invested in preventing cyber incidents, the majority have not considered how they will recover from them. Even those with isolated backup and vaulting solutions rarely consider the steps required to inspect, validate and recover data at speed. Facilitating these activities not only requires the right technical solution, but a structured approach to disaster recovery and business continuity. Among our clients we see common challenges in developing an effective recovery capability, including:

- Limited understanding of likely cyber disaster scenarios;
- The assumption that vaulting solutions will deliver effective cyber recovery;
- Inability to identify dependencies, sequence recovery and align with existing business continuity and disaster recovery programs; and,
- Lack of trusted environments for forensics and recovery.

Failure to meet these challenges will have a significant impact on an organisation's ability to recover. In the event of a high-impact incident, those who are not adequately prepared can expect a long road back to normal operations, excessive financial costs and possible reputation damage.

Organisations typically benefit from a combination of one or more of the following:

- Documenting enterprise wide priorities in the form of critical business functions.
- Aligning IT systems and services to critical business functions.
- Assessing current IT disaster recovery capabilities and identifying gaps.
- Building technical plans, playbooks and runbooks to facilitate effective cyber recovery.

A careful assessment of an organisation's needs and current resilience is required, enabling concerns to be identified and addressed before recovery is needed.

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.

# Cyber Recovery Services

## Recovery Strategy and Playbooks

PwC can help you to prepare for a high impact or destructive cyber incident.

Our services are designed to give you confidence that your organisation will respond effectively in a crisis. We work with you to understand the technology which supports important business services. We use this information to create robust plans that enable you to plan for effective cyber recovery before an incident occurs. If you already have plans we can review them, using our knowledge of sophisticated cyber attacks to identify any gaps. We can also help you 'stress test' these plans, by conducting technical testing or crisis exercises.

Our team is made up of experts with knowledge of cyber incident response, IT disaster recovery and crisis management. Our incident response team is assured by the National Cyber Security Centre (NCSC) on the Cyber Incident Response scheme as a Level 1 provider.

### Cyber Recovery Strategy

- **Organisation wide view** - determine which are your important business services and the other teams and processes on which these services rely, as well as the resilience of any workarounds available.
- **Identify technology interdependencies** - understand the interdependencies of the technology on which important business services rely, including third party services.
- **Understand your supply chain** - establish which third parties are crucial to the operation of your organisation, and how you would function in the event they suffered a significant cyber security or business resilience incident.
- **Document enterprise priorities** - develop a plan that provides you confidence you have full control of your systems, whilst carefully balancing technical investigation and organisation recovery.
- **Build knowledge** - the majority of individuals have never responded to a live cyber incident and therefore may not have the necessary subject matter expertise. A playbook helps to improve awareness among your team, and identify where you should consider third party support such as crisis experts, incident responders and external legal counsel.

### Cyber Recovery Playbook

- **Decreased response time** - the playbook sets out the initial containment actions and decision making authority, allowing responders to take these actions swiftly.
- **Consistency and visibility** - the playbook can link to action cards for the different response teams, ensuring consistency in response.
- **Supports investigation** - supports cyber security investigation and evidence preservation, ensuring that known details about the attacker are taken into account during the response.
- **Regulatory compliance** - provides action cards for Legal and Compliance teams, ensuring that regulators are informed at the correct time and that regulatory compliance considerations for your organisation have been taken into account.
- **Effective change** - decrease the mental load on responders and leaders, providing more space to set future strategy and make the most of opportunities that present themselves during a crisis.

## Cyber Recovery Strategy - Features

- **Design an enterprise wide strategy for effective cyber recovery.**
- **Identify technology dependencies and how IT supports your organisation.**
- **Understand how your IT supply chain could affect your resilience.**
- **Document enterprise priorities for business recovery after a cyber incident.**
- **Build knowledge among staff responding to cyber incidents.**
- **Decrease response time after a destructive cyber incident.**
- **Ensure consistency in your approach to recovering technology & systems.**
- **Enhance regulatory compliance by recovering effectively from cyber incidents.**

## Cyber Recovery Strategy - Benefits

- **Decreased response time**
- **Consistency and visibility** .
- **Supports investigation** cyber security investigation and evidence preservation,
- **Regulatory compliance** provides action cards for Legal and Compliance teams.
- **Effective change**
- **Ensure consistency in your approach to recovering technology & systems.**
- **Enhance regulatory compliance by recovering effectively from cyber incidents.**