G-Cloud 15

Human Cyber Risk 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 support them:

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

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

Human Cyber Risk Services

This section describes in more detail the service features and benefits included within this service definition document. We currently have three propositions which are part of this service: Awareness, Behaviour and Culture (ABC), Cyber Workforce and Cyber Business Change which are described below.

Security Awareness, Behaviour and Culture Services

People are seen by attackers as the weak link in security, this is because people have been under invested in and not adequately understood or considered in security. These services re-prioritise the people component by transforming security behaviours of staff to develop a secure culture and improve security posture, reducing human cyber risk.

Security Awareness, Behaviour and Culture Proposition Features	Security Awareness, Behaviour and Culture Proposition Benefits
• Define security behaviours for staff • Assess existing security behaviour using qualitative and quantitative data • Identify and understand how organisational culture impacts security • Implement security training, leadership awareness campaigns • Redesign of security processes and controls.	• Clear security behavioural expectations • Identification of root causes of existing poor security behaviour • Understanding how security culture fits within organisational culture • Improved security behaviour of staff.

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

1. Our perspective

People are often seen as a risk, the 'weak link' in cyber security to be 'managed' through training and awareness activities alone. There is however, substantial evidence to prove that this attitude, and these activities, are not working. Security leaders need to fight the urge to tick a training and awareness box and gain a better understanding of human behaviour to be able to make a difference to security behaviour and attitudes towards security. We believe a behaviour led approach is needed, grounded in the following four beliefs:

- **People, process and technology:** Security is often seen as a technology problem resulting in substantial underinvestment in the people component. More investment in people represents a huge opportunity to impact security for the better

- **Training and awareness isn't enough:** We need to do more for people. Simple e-learns and occasional communications are not enough, they don't properly engage people and motivate them to be secure. We need to understand root causes and drivers of poor behaviour and address these

- **Empower people don't fight them:** People are complicated, we are not rational, we are driven by feelings and emotions. We should leverage this in support for security rather than making false assumptions or attempting to unrealistically constrain it

- **Valuing security in decision making:** People in organisations make trade offs between different values in decision making every day. Security is often not the top priority, nor should it be, but it needs to move up the list. Security needs to increase in importance within the organisational culture.

2. Our approach

We have four clusters that inform our approach:

1. **We understand the bigger picture:** Security behaviours are driven by broader values, beliefs, attitudes and norms which are shaped over time by our environment and social context, this includes our organisational and national cultures. We pay attention to these and understand how they influence security behaviour then leverage aspects where possible for the good of security.

2. **We design for people not against them:** Security is often designed by security professionals, with policies and controls often mandated from the centre. These often don't work for real people in the organisation, slowing or hindering them from achieving their work goals. In this situation security doesn't get done, or workarounds are developed which may not be secure but facilitate

better productivity. We consult and design for people, appreciating where approaches may need to differ by teams or communities.

3. **We make security business critical**: People in organisations make trade offs between different values in decision making every day. Security is seldom the top priority, nor should it be, but it needs to move up the list. We help senior leaders to embed security in their decision making and equip them to lead on cyber security.

4. **We are positive about security**: The language and tone around security is often negative. Fear, uncertainty and doubt used too frequently in the world of security does not help motivate secure behaviour. People are often described as 'stupid users'. We change this narrative, help set the right tone around security, incentivise good behaviour and help shape the image of the security teams.

3. Outcomes

We focus our work on specific security behaviours and address the root causes of poor security behaviour. We start by identifying those areas that are easy to address, allowing us to make a noticeable impact on specific behaviours quickly. Over time, as behaviours and habits change, attitudes and mindsets towards security start to change and you will see a shift in how security is valued across your organisation. We will:

- Help you set the strategic direction for their ABC programme with objectives and a clear vision or definition with supporting behaviours

- Work with you to define groups who pose enhanced cyber risk based on clear criteria including threat intelligence, including developing key personas in those groups enabling tailored interventions to areas of greater risk

- Assess your current security culture including areas of poor behaviour and root causes and produce an assessment summary report

- Develop a roadmap with interventions to address the root causes of the poor security behaviours identified in the behaviours assessment. Metrics will also be suggested to measure the success of the programme

- Design and deliver the tailored activities and interventions that are included in the roadmap.

Cyber Workforce

Increasing regulatory expectations, technology advancement, and the increasing risk of cyber attacks and data breaches mean that cybersecurity skills are more important than ever. They play an increasingly

important role in business operations, and underpin the security of people, assets and data. Despite the importance of these skills, attracting and retaining Cyber Talent remains a significant challenge given the cyber skills shortage in the market:

- The UK cyber security workforce gap is estimated at 3,800 professionals *(Cyber security skills in the UK labour market 2025).*
- Around half of UK businesses (49%) reported a basic technical cyber security skills gap, while 30% reported gaps in more advanced technical areas *(Cyber security skills in the UK labour market 2025).*

There are two core elements to our approach to Cyber Workforce Planning:

- **Operational Cyber Workforce Planning**: To allow you to identify and close skills gaps in your existing Cyber Workforce through the application of skills frameworks and development of training pathways
- **Strategic Cyber Workforce Planning**: To allow you to proactively anticipate future staffing requirements and identify 'no regret moves' of action, taking into account the impact of technology and alternative ways of working.

Cyber Workforce Service Features

- Utilising a best-practice cyber skills framework to enhance the capabilities of the cyber workforce
- Conducting a comprehensive skills gap analysis within the cyber workforce
- Creating targeted training and development pathways
- Providing recommendations for optimising the current cyber workforce alignment with strategic objectives, which may include proposing adjustments to roles and responsibilities.

Cyber Workforce Service Benefits

- Establishes a solid foundation for building the cyber workforce, aligning skills with industry best practices.
- Provides consistency, clarity, and expectations in assessing current skills and identifying gaps for future needs.
- Equips the cyber workforce with the necessary knowledge and skills to adapt to the evolving cyber landscape.
- Facilitates upskilling, attraction, retraining, and transformation initiatives within the cyber workforce, achieving the vision for a future-ready workforce.

Cyber Business Change

1. Our perspective

Organisations need to continually adapt and change their cyber security people, process and technology to proactively mitigate risks, comply with regulations, adapt to technological advancements, and respond to incidents or breaches. This can be small organisational changes or larger transformations.

People are central to the success of cyber security change. However, they are often **not appropriately engaged**. A lack of engagement throughout cyber security change can leave people resistant to change, unclear on what is changing, the reasons why and what it means for them.

2. Our approach

Our understanding of the importance of considering employees' needs and engaging with them throughout the change lifecycle has led to the development of our people-centric approach to cyber security change and transformation.

- We help clients set the **strategic direction** for cyber security change through the definition of a unified change vision
- We **identify stakeholders and conduct analysis** to understand their commitment, impact and attitude towards the change to ensure they are efficiently engaged
- We work with project team(s) and business to **define and assess change impact** and measure and report on how ready the business is to accept the change
- We work with the client to **deliver activities unique to each project** which will enable stakeholders to embrace the new ways of working
- We **iterate change planning and delivery** and help design and monitor adoption of the new ways of working.

3. Outcomes

Our approach to supporting clients through cyber security change projects aims to achieve positive outcomes. For instance, we assist clients in establishing a clear and agreed-upon strategic direction for the change or transformation, ensuring alignment among key stakeholders. Additionally, we prioritise engaging stakeholders in a timely and effective manner, fostering their commitment to the change from the outset.

Another important outcome of our approach is enabling clients to understand the impact of the cyber security change on individuals and their work processes. This understanding ensures that the change is appropriate and well-received. To drive the change effectively, we provide impactful and engaging activities, such as tailored workshops, which significantly contribute to the overall success of the transformation.

Cyber Business Change Proposition Features	Cyber Business Change Proposition Benefits
• People-centric approach to cyber security change and transformation • Definition of a unified change vision for strategic direction • Stakeholder identification and analysis for efficient engagement • Change impact assessment and readiness measurement • Tailored activities to enable stakeholders to embrace new ways of working • Iterative change planning and delivery for flexibility and adaptability	• Enhanced employee engagement throughout the change process • Clear and agreed-upon strategic direction for cyber security change • Efficient stakeholder engagement and alignment • Thorough analysis of stakeholder commitment, impact, and attitude • Comprehensive assessment of change impact and readiness