

Digital Risk and Cyber Security Management



The requirement

Public sector organisations are under continuous pressure to modernise services, adopt cloud technologies, and accelerate digital transformation. At the same time, the cyber threat landscape is increasing in complexity and scale, with risk exposure expanding across cloud platforms, supply chains, third-party services, legacy estates, and hybrid operating models.

Many organisations also face challenges such as limited specialist capacity, fragmented security ownership across programmes, and uncertainty about how to manage digital risk effectively while maintaining delivery momentum.

Clients require cyber security and digital risk services that enable secure transformation, improve resilience, and provide practical assurance while remaining proportionate, cost-effective, and aligned to government standards.

Redesmere's solution

Redesmere delivers a range of Digital Risk and Cyber Security Management Services, offering flexible access to experienced cyber professionals.

We help clients understand their digital risk exposure, assess security posture across cloud platforms and third-party dependencies, and implement targeted improvements that reduce vulnerabilities and improve resilience.

Our service can be delivered as defined projects, ongoing advisory support, or a managed service model providing continuous assurance and risk management. This enables organisations to focus on core competencies and service outcomes, while we provide specialist cyber security capabilities, structured risk insight, and expert guidance to protect users, data, and essential public services.

A key component of our service focuses on developing the capabilities and teams our clients need to onboard new cloud technologies and services. This component of the service provides a comprehensive suite of organisational and people-development capabilities designed to complement and enhance the adoption, optimisation, and ongoing management of cloud services.

Our teams are multi-disciplinary with significant expertise in cloud strategies, business architecture, technical architecture, cloud transformation, digital transformation, programme turnaround, programme control, delivery enablement and independent assurance.

We are truly independent from incumbent and potential new service providers, and do not have any conflicts of interest.

When to use these services?

The service provides an end-to-end capability to identify digital risk exposure, assess cyber security posture, and produce clear assurance that helps organisations understand what risk exists, why it matters, and what actions to prioritise. It supports cloud and hybrid environments, enabling teams to improve security while maintaining delivery pace and operational resilience.

Clients typically use the service to replace fragmented security activity with a consistent approach to risk management, improve confidence in decision-making, and strengthen governance through clear, evidence-led reporting.

Where accountability is distributed across teams, suppliers, or platforms, the service provides a consistent assurance layer that improves oversight and reduces duplication.

What are the benefits?

- » Reduced cyber risk exposure across cloud and digital services.
- » Improved resilience and business continuity for critical services.
- » Stronger assurance that security is embedded into delivery decisions.
- » Faster delivery with appropriate security controls “built in”.
- » Clearer visibility of the organisation’s digital risk landscape.
- » Better prioritisation of investment through risk-based planning.
- » Improved audit readiness and governance confidence.
- » Access to specialist capability without requiring permanent headcount.
- » Greater stakeholder confidence in secure transformation outcomes.

How we work

We tailor our services to our clients’ specific requirements, agree the objectives and outcomes that are to be achieved, and document these in formal Statements of Work (SoWs).

An integral part of each SoW is the implementation plan for the services which sets out how the objectives and outcomes are to be achieved as a series of epics.

The vast majority of our client engagements are outcome-based arrangements, with milestone-based payments that are linked to the achievement of the objectives and outcomes set out in the SoWs.

We maintain detailed plans throughout each engagement which we use to review progress and to reprioritise work with our clients on a regular basis.

A key component of most of our implementation plans is “Service Transition” which we use from the outset of each engagement to plan and manage any offboarding activities.

Our services are usually provided during normal business hours. However, we recognise that some cloud transformation activities need to be performed out of hours and at weekends which we are happy to incorporate into the service if necessary.

We are able to operate using our own or our clients’ tooling, cloud and Office 365 infrastructure.

What is distinctive about us?

Redesmere’s core proposition is that:

- » Our small multi-disciplinary teams are hand-picked for each individual client engagement.
- » We have the skills, track record and gravitas to make a real difference.
- » Our people have extensive experience of digital transformation, delivery and cloud implementation programmes.
- » Our independence means that we do not have any conflicts of interest to get in the way.
- » We are able to provide our services through time and materials, fixed price or output-based contracts, when appropriate.

How to contact us?

e: hello@redesmere.com

t: +44 1625 810180

w: <https://redesmere.com>