G-Cloud 15

Managed Cyber Risk Services – Service Description

January 2026

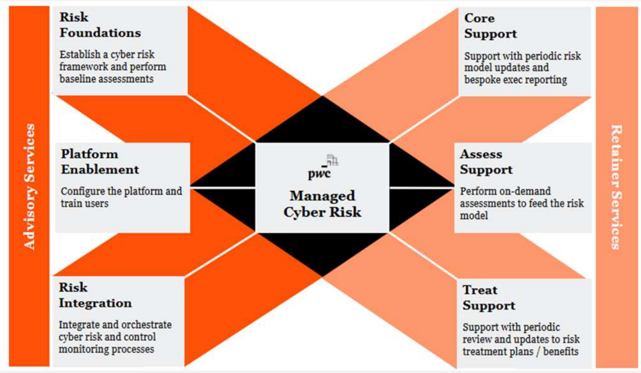
Contents

Managed Cyber Risk Services

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

Manage Cyber Risks Features

MCR solution includes cyber risk advisory and retainer services enabled by a tech platform.



Key questions MCR reporting helps answer

- Is our risk exposure within our appetite?
- How real is the threat we face?
- How well are we securing ourselves?
- How should we treat our risks?
- How can we maximise RoI in risk reduction?

Managed Cyber Risk Key Benefits

Accelerates time to value
MCR includes pre-loaded content that enables the rapid operationalisation of a cyber risk management framework.

Improves cyber risk oversight & ownership
MCR provides the insights your executives need to fulfil their cyber risk management responsibilities.

The breadth of assessments we provide
We provide a wide range of on-demand security assessments tailored to your requirements.

Compliments existing GRC investments
Effective risk management combines top-down and bottom-up approaches. MCR integrates with GRC platforms to deliver this.

1. Managed Cyber Risk Services

Cyber is a top tier risk for most companies which is driving demand from Executives for greater transparency. However, reporting and managing cyber risks can be a complex exercise. Therefore, PwC provides tailored services according to each client's needs.

Managed Cyber Risk (MCR) is a strategic cyber risk analytics and orchestration solution which accelerates your journey towards real-time quantified risk decision-making. It includes cyber risk advisory and managed services enabled by a tech platform powered by Microsoft.

Our approach is founded in the principles of pragmatism, flexibility and explainability, recognising both the scrutiny cyber risk attracts and the wide variety of maturity in risk management practises that exists across the industry.

PwC's MCR solution includes an extensive catalogue of pre-loaded content and optional services led by our cyber risk professionals who are passionate about the topic and can work with you to make the process of managing cyber risk end to end easy for you.

2. Managed Cyber Risk: Service Catalogue

Maximise the benefits of MCR retainer services with our flexible set of days. The table below provides an indicative effort breakdown available in typical service volumes to enable clients to understand how services are drawn against an MCR contract. The following assumptions apply:

- Support days are available for one year at a standard blended daily rate, based on a blended onshore/offshore team.
- Additional services and the required hours can be discussed as needed during contracting in line with the ancillary services listed in our G Cloud 15 Pricing Document for this service. .
- We can provide an onshore only service for an additional fee.
- Full details of our pricing for this service are provided in the associated pricing document.

Retainer	Service	Activity	Assumptions	Indicative Effort (days)
Core Support	**Re-calibrate the risk model**	Review and re-calibrate the cyber risk model	Core risk model updated	3.5
	Curate bespoke reports	Create or update a bespoke ExCo or Board status report	Will collaborate with you to create the report template leveraging our good practise examples	3.5
	Configure CCM connections	Review OOTB connection	Review connections to popular platforms already available in MCR where configuration and available metrics are largely consistent across clients (e.g., MS DfC, AWS SH, GCP SCC, Palo	2 to 6

Retainer	Service	Activity	Assumptions	Indicative Effort (days)
			Alto Prisma, Wiz CSPM). There are five PwC activities, three of which are optional (support XSPM config review, support XSPM config, configure network connectivity, test access and connectivity, and connection troubleshooting)	
		Configure tailored OOTB connection	Configure connections to popular platforms already available in MCR that typically require bespoke setup for each client, where configuration steps and available metrics vary (e.g., ServiceNow and Sentinel).	TBC
		Design custom connection	Design connections to platforms not currently available in MCR. These may later evolve into OOTB connections and may or may not need client-specific tailoring. A feasibility analysis during the client MCR setup engagement is required to determine scope and approach.	TBC
Assess Support	**Perform technical assessments**	Perform a risk impact assessment	For 1 OU and 7 risks	1.5
		Perform a threat likelihood assessment	1 OU and 27 threat scenarios	3
		Perform a controls maturity assessment	TBC based on the depth and scope of the assessment	TBC
Treat Support	**Prioritise control improvements**	Help shape an investment case by identifying priority projects to maximise risk reduction benefits	The projects are already configured in the MCR platform. The effort depends on the complexity of the portfolio.	1 to 5
		Validate or recommend planned control uplifts by projects	The projects have a documented scope. The effort depends on the complexity of the portfolio.	1 to 5
	Stay abreast of good practises	Run a workshop to share latest cyber threat trends and good practises to mitigate them	One workshop with supporting presentation	2
		Perform a deep-dive design effectiveness review of a current level 1 control and recommend improvements to address latest threat trends (e.g. new techniques).	One report up and supporting presentation	5

4. Why PwC? | Our industry recognition

PwC is recognised as leader on the Forrester wave latest report: Cybersecurity Consulting Services in Europe, Q4 2025

According to the report:

"PwC develops operating models and strategies, translating them into practical execution across clients' workflows, processes, and technology. Its board and executive coaching services equip CISOs with coaching, best practices, and peer networks to ensure they can influence their board effectively to make cybersecurity a priority."

It goes on to say:

"Customers praise PwC for delivering large, complex projects quickly with skilled talent across all cybersecurity domains and seniority levels."