Mission Statement:

Quantum Evolve and CMS Distribution empower businesses to scale securely and provide value to your customers through agile, transparent, and outcome-driven cybersecurity services.

High Level Summary Cybersecurity Services:

Vendor agnostic and customer driven approach

Tailored made solutions by certified industry-proven experts
All services require a qualification call to understand what the partner/end customer needs.

High margins and competitive pricing compared to industry standards

Executive Summary

Choosing Quantum Evolve and CMS Distribution gives you a strategic advantage that competitors simply can't match. Unlike traditional cybersecurity providers who deliver generic, one-size-fits-all solutions, Quantum Evolve and CMS Distribution combine deep technical expertise with a proven ability to translate security into commercial value and operational outcomes. You're not just buying a service, you're gaining a partner that understands your business model, your customers, and the realities of scaling securely in a rapidly evolving threat landscape.

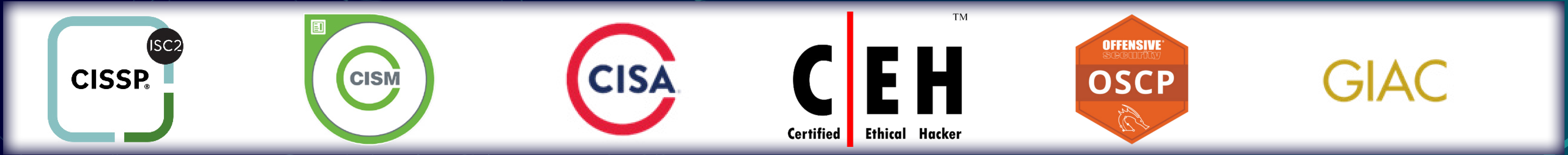
Their approach blends advanced tooling, industry frameworks, and hands-on experience across enterprise, mid-market, and highly regulated environments, enabling them to deliver faster, more relevant, and more effective results than larger, slower consultancies.

What truly sets Quantum Evolve and CMS Distribution apart is their agility, transparency, and obsession with quality. They operate with the responsiveness of a specialist boutique while delivering the rigor and depth typically associated with top-tier global consultancies. Their team works side-by-side with yours, providing clear communication, prioritised remediation roadmaps, and solutions that are practical, repeatable, and aligned to real-world constraints—not theoretical controls or unnecessary complexity. With Quantum Evolve and CMS Distribution, you get a partner that actually delivers outcomes, not just reports, helping you reduce risk faster, build internal capability, strengthen customer trust, and achieve a security maturity level that outpaces your competitors.

Accreditations

QE, CMS Distribution's service partner, maintains a suite of industry-recognised cyber security accreditations and certifications to ensure the highest levels of expertise, compliance, and trust. Organisationally, they hold ISO/IEC 27001 for Information Security Management and Cyber Essentials and Cyber Essentials Plus for foundational cyber hygiene. Their practices align with the NIST Cybersecurity Framework, GDPR, and other relevant regulatory standards.

At an individual level, their team members hold globally recognised qualifications including



This combination of organisational and individual credentials ensures our capacity to deliver robust, resilient, and fully compliant cyber security services, underpinned by deep technical knowledge, governance expertise, and proven risk management capabilities.

Contact Information: CMSCybersecurityServices@cmsdistribution.com

Table of Contents

Quantum Evolve Rate Card

Service Package 1: Assessment Services

CMS SKU	Service Package	Partner Cost	Notes
412549	CMS Shield Package – SMB	£4,200.00	Includes vulnerability assessment, up to 100 users & End Points
412550	CMS Shield Package – Medium	Qualification Call Required	up to 101- 500 users & End Points
412551	CMS Shield Package – Large	Qualification Call Required	up to 501- 1000 users & End Points
412577	CMS Guardian Assessment Package	£6325, per legal entity	Includes vulnerability assessment + ethical hacking + report.
412577 412643	CMS Fortress Assessment Package	£6,325 and £1127 per day for a Cyber Specialist to support remediation, per legal entity	Includes vulnerability assessment + ethical hacking + report + support with remediation. The time required to support any remediation is solely dependent on the outcome of the reports.

Short Description:

For the beginning of the assessment, our solution discovers and validates all related domains against vulnerabilities, misconfigurations, and compliance standards, providing a complete risk picture with quantified impact using the Factor Analysis of Information Risk (FAIR) model.

Ethical hacking engagements simulate real world attacks to independently test resilience, uncover hidden weaknesses, and support compliance with frameworks such as GDPR, ISO 27001, NIST, and PCI DSS.

Deliverables include detailed reports, executive summaries, exploitation evidence, and remediation workshops, giving organisations a clear roadmap to strengthen security and resilience.

Continue

Quantum Evolve Rate Card

Service Package 1: Assessment Services

Detail Description:

Our technology will discover all related sub-domains. All domains are validated against known vulnerabilities, misconfigurations, website issues, cryptographic weaknesses etc. which in-turn, provides a complete picture of where the issues are and how to correct them. The domain infrastructure will also be evaluated for vulnerabilities, weaknesses, and entry points for an attacker with confirmation of any exploits that have been attempted and found to be successful. In addition, we will provide details of your compliance against internationally recognised standards and frameworks, such as General Data Protection Regulation (GDPR), ISO 27001, National Institute of Standards Technology (NIST), Payment Card Industry Data Security Standard (PCI DSS) etc. Reporting is provided to accommodate both Board and Technical level staff and contains quantified risk in monetary terms using the widely adopted Factor Analysis of Information Risk (FAIR) model.

An ethical hack (penetration test) is a controlled and authorised security assessment designed to identify vulnerabilities before malicious actors can exploit them. It simulates real world attack techniques, ranging from external network probing to internal privilege escalation, to test the resilience of an organisation's systems, applications, and people. Ethical hacking provides independent validation of security posture, uncovering weaknesses that routine monitoring may not detect, such as misconfigurations, unpatched software, insecure code, weak authentication, or exploitable human behaviour. For regulated industries, ethical hacking also supports compliance with standards like ISO 27001, NIST CSF, PCI DSS, Cyber Essentials Plus, and GDPR's requirement to ensure "appropriate technical and organisational measures." Ultimately, the objective is to reduce cyber risk by discovering security gaps safely before a real attacker does.

The deliverables from an ethical hack typically include a detailed technical report outlining each identified vulnerability, its severity, exploitation method, business impact, and recommended remediation steps. This is complemented by an executive summary for leadership, providing clear, risk-based findings and prioritised actions. Engagements also include evidence of exploitation (screenshots, logs), a remediation workshop to help teams fix vulnerabilities, and a re test to validate that issues have been resolved. Additional deliverables may include an attack-path analysis, exploit proof-of-concepts, diagrams of compromised routes, and a maturity uplift plan aligned to frameworks such as NIST or CIS Controls. Together, these outputs give organisations a clear roadmap for strengthening security, improving resilience, and ensuring vulnerabilities are fully addressed.

Contact Information: CMSCybersecurityServices@cmsdistribution.com

Table of Content Page ›

Service Package 2: Advisory Services

CMS SKU	Service Package	Partner Cost	Notes
412647	Virtual Chief Information Security Officer (CISO)	Qualification Call Required.	Average SME would require a minimum of 1 day per month. This can be tailored to fit i.e. some organisations may require more days, some less.

Short Description:

CISO-as-a-service, outsourced cybersecurity leader who provides strategic security guidance, risk management, and compliance oversight without the cost of a full-time executive

A Virtual Chief Information Security Officer (vCISO) should be considered when an organisation needs senior-level cybersecurity leadership but does not have the scale, budget, or ongoing demand to justify a full-time CISO. This is common in small to mid-sized businesses, or in larger organisations going through periods of transition such as cloud migration, regulatory uplift, or the implementation of a security programme from a low baseline. A vCISO provides strategic oversight, risk management, governance, policy development, and guidance on security architecture—ensuring the business maintains a coherent and risk-aligned security posture without the cost of a permanent executive hire.

A vCISO also becomes crucial when an organisation is facing increased regulatory, customer, or industry scrutiny but lacks internal expertise to meet security expectations. This includes scenarios such as preparing for ISO 27001, PCI DSS, Cyber Essentials Plus, NIST CSF alignment, incident response readiness, or third-party assurance requests. A vCISO brings external objectivity, experience across multiple environments, and the ability to rapidly uplift security maturity, close compliance gaps, and lead security improvement programmes. They are particularly valuable during or after security incidents, when independent leadership is needed to assess root causes, re-establish governance, and ensure sustainable long-term improvements.

Continue

Service Package 2: Advisory Services

CMS SKU	Service Package	Partner Cost	Notes
412646	Virtual Chief Information Officer (CIO)	Qualification Call Required.	Average SME would require a minimum of 1 day per month . This can be tailored to fit i.e. some organisations may require more days, some less. It is difficult to provide definitive ££s as there are so many considerations that need to be weighed up.

Short Description:

CIO-as-a-service, responsible for overseeing an organization's IT strategy, systems, and digital transformation to ensure technology supports overall business goals.

A Virtual Chief Information Officer (vCIO) should be considered when an organisation recognises the need for strategic technology leadership but does not yet require or cannot justify the cost of a full-time CIO. This is particularly relevant for small to mid-sized organisations whose IT environments are growing in complexity, especially during cloud migrations, digital transformation initiatives, or periods of rapid expansion. A vCIO can provide enterprise-grade strategic oversight, aligning technology investment, governance, and cybersecurity with business goals, without the financial overhead associated with a permanent executive-level hire.

A vCIO is also valuable when an organisation needs mature IT strategy, budgeting, and roadmap development but lacks internal senior-level expertise or has fragmented technology management. This includes organisations that suffer from inconsistent IT decision-making, escalating technical debt, or recurring operational failures. A vCIO provides independent, vendor-neutral guidance to optimise IT operations, manage risk, define architecture standards, and ensure compliance. They are particularly useful during mergers, acquisitions, regulatory shifts, or periods where business leaders need structured, expert insight to ensure technology decisions are sustainable, secure, and aligned to long-term objectives

Continue

Service Package 2: Advisory Services

CMS SKU	Service Package	Partner Cost	Notes
412648	Virtual Chief Technical Officer (CTO)	Qualification Call Required.	Average SME would require a minimum of 1 day per month. This can be tailored to fit i.e. some organisations may require more days, some less. It is difficult to provide definitive ££s as there are so many considerations that need to be weighed up.

Short Description:

CTO-as-a-service, responsible for overseeing an organization's technology strategy, innovation, and product development to ensure technical solutions drive business growth.

A Virtual Chief Technical Officer (vCTO) should be considered when an organisation needs high-level technology leadership to define and execute a technical strategy but does not have the budget or long-term need for a full-time CTO. This is particularly relevant for small and mid-sized businesses that are scaling rapidly, adopting new platforms, or modernising legacy systems. A vCTO can provide guidance on architectural decisions, cloud strategy, product development, infrastructure modernisation, and technology road mapping, ensuring that technical investments directly support the organisation's commercial objectives. They help avoid costly missteps, provide clarity on prioritisation, and bring experience gained across multiple industries and technology stacks.

A vCTO becomes especially valuable during periods of major transformation or innovation, such as migrating to cloud services, implementing automation, integrating AI, or overhauling core business systems. They provide objective expertise during vendor selections, major procurement decisions, and solution architecture reviews. Additionally, a vCTO is beneficial when an organisation lacks internal senior engineering leadership capable of mentoring technical teams, establishing development standards, or ensuring scalable design principles. By offering part-time executive leadership, a vCTO enables organisations to maintain strong technical direction, reduce operational risk, and accelerate digital transformation without the overhead of a permanent C-level hire.

Continue

Service Package 2: Advisory Services

CMS SKU	Service Package	Partner Cost	Notes
412649	Virtual Data Protection Officer (DPO)	Qualification Call Required.	Average SME would require a minimum of 1 day per month. This can be tailored to fit i.e. some organisations may require more days, some less. It is difficult to provide definitive ££s as there are so many considerations that need to be weighed up.

Short Description:

DPO-as-a-service, responsible for ensuring an organization complies with data protection laws, safeguards personal data, and advises on privacy practices.

A Virtual Data Protection Officer (vDPO) should be considered when an organisation needs expert guidance on data privacy and regulatory compliance but does not require a full-time, in-house DPO. This is common for small and medium-sized enterprises, startups, or organisations with limited internal privacy expertise. A vDPO provides strategic oversight on data protection practices, ensures adherence to GDPR, UK Data Protection Act, and other relevant privacy regulations, and develops policies, procedures, and governance frameworks to manage personal and sensitive data responsibly. They help organisations embed privacy by design, conduct privacy impact assessments, and manage cross-border data transfer compliance without the ongoing cost of a full-time hire.

A vDPO is also essential when an organisation is undergoing significant changes that impact data processing, such as digital transformation initiatives, cloud migration, or the implementation of AI and analytics tools that involve personal data. They are particularly valuable during audits, regulatory inspections, or when responding to data subject access requests and data breaches. By providing independent, expert oversight, a vDPO ensures that privacy risks are identified and mitigated proactively, that compliance obligations are consistently met, and that the organisation maintains trust with customers, partners, and regulators, all while offering the flexibility to scale their involvement according to business needs.

Contact Information: CMSCybersecurityServices@cmsdistribution.com

Table of Content Page ›

Service Package 3: Compliance Services

CMS SKU	Service Package	Partner Cost	Description	Measurable Deliverables
412602	Cyber Essentials	Qualification Call Required.	Scoping IT systems, implementing baseline controls (firewalls, access, patching, malware protection), internal self-assessment, preparing certification submission.	Completed self-assessment questionnaire, documented security controls, certification readiness report.
412603	Cyber Essentials Plus	Qualification Call Required.	All Cyber Essentials work packages plus independent technical verification, vulnerability scanning, internal audits.	Verified security controls, vulnerability scan report, external certification.
412604	Cyber Resilience Act	Qualification Call Required.	Identify critical software, establish secure development & update processes, risk assessment, lifecycle resilience demonstration.	Software risk register, secure coding standards, vulnerability remediation reports.
412605	Data Protection (UK DPA / GDPR)	Qualification Call Required.	Map personal data flows, implement privacy policies, conduct DPIAs, define retention schedules, staff training, breach response planning.	Data flow maps, DPIA reports, training records, breach response plan.

Continue

Service Package 3: Compliance Services

CMS SKU	Service Package	Partner Cost	Description	Measurable Deliverables
412606	DORA / NIS2	Qualification Call Required.	ICT risk management, incident reporting procedures, business continuity planning, third-party risk assessments.	Risk registers, incident response templates, third-party assessment reports, continuity plan
412607	EU AI Act	Qualification Call Required.	AI system risk classification, documentation of development processes, model validation & testing, bias/fairness assessment, ongoing monitoring.	AI risk register, compliance documentation, testing reports, monitoring logs.
412608	NIST / SANS	Qualification Call Required.	Gap analysis, risk assessment, control implementation, continuous monitoring, incident response planning, security awareness programs.	Risk and gap analysis reports, implemented controls, monitoring dashboards, incident response exercises.
412609	PCI DSS	Qualification Call Required.	Scope payment card environment, implement technical controls (network segmentation, encryption, access management), vulnerability management, logging/monitoring, testing.	PCI DSS compliance reports, vulnerability scan reports, log review dashboards, attestation of compliance.

Services and cost can vary to best suit size and complexity of the organisation

Contact Information: CMSCybersecurityServices@cmsdistribution.com

Table of Content Page ›

Service Package 4: Cybersecurity Foundation Services

CMS SKU	Service Package	Cost	Short Description
479741	Cybersecurity Essentials for SMBs	Qualification Call Required.	This package provides SMBs with affordable, scalable, enterprise-grade cybersecurity protection and guidance through a subscription model that reduces risk, ensures compliance, and builds long-term resilience without requiring in-house expertise.

Description:

This package is designed to give small and medium-sized businesses affordable, practical, and comprehensive cybersecurity protection without the need for in-house expertise. It focuses on the essential controls that deliver the greatest reduction in risk such as endpoint protection, identity and access hardening, patch and vulnerability management, phishing defence, and basic incident response readiness. The service is delivered in a simple subscription model that scales with the organisation, ensuring predictable cost and continuous protection.

In addition to technology and monitoring, the package includes guidance on policies, user training, and secure operating practices to build long-term resilience. By combining managed services with advisory support, this offering gives SMBs access to enterprise-grade security capabilities at a fraction of the cost, helping them meet customer expectations, comply with regulatory requirements, and reduce the likelihood and impact of cyber incidents.

Continue

Service Package 4: Cybersecurity Foundation Services

CMS SKU	Service Package	Cost	Short Description
491164	Cybersecurity Package for Hardware Businesses (Entry into Cyber) / Cybersecurity Foundations for Hardware Businesses	Qualification Call Required.	This package helps hardware-focused businesses embed cybersecurity into their products and services through a secure by design framework and go to market consulting, enabling them to build credibility, meet customer expectations, and create new revenue streams in the cyber market.

Description:

This package supports hardware-based organisations, manufacturers, distributors, and integrators seeking to expand into cybersecurity services or embed security directly into their product lines. It provides a structured “secure-by-design” framework covering device hardening, firmware security, supply chain assurance, secure configuration, and the development of customer-facing security documentation such as hardening guides and support SLAs. The goal is to help hardware businesses rapidly establish credibility and differentiation in the cyber market.

Alongside the technical support, the package includes go-to-market consulting to help organisations build cyber-aligned service offerings, pricing models, and messaging. It bridges the gap between traditional hardware sales and modern cybersecurity expectations, enabling organisations to create new revenue streams while aligning with best practices and growing customer demand for secure, trusted technology solutions.

Continue

Service Package 4: Cybersecurity Foundation Services

CMS SKU	Service Package	Cost	Short Description
412574	Cybersecurity Posture Assessment (SMB / Mid-Market / Enterprise)	Qualification Call / Discovery Questionnaire prior to pricing	This assessment service delivers a standards aligned evaluation of an organisation's security posture with tailored gap analysis, maturity scoring, and a prioritised remediation roadmap, providing actionable improvements for SMBs, scalable maturity for mid market firms, and compliance aligned reviews for enterprises.

Description:
This assessment service provides a comprehensive, standards-aligned evaluation of an organisation's security posture, tailored to its size, maturity, and industry.

Using frameworks such as NIST CSF, CIS Controls, ISO 27001, and related benchmarks, the assessment covers technology, processes, governance, identity, data protection, and incident readiness. The output includes a detailed gap analysis, maturity scoring, and risk-based findings across all critical domains. The engagement concludes with a prioritised remediation roadmap, enabling security and IT leaders to focus on the actions that will deliver the greatest risk reduction and business value. For SMBs, the assessment focuses on fast, actionable improvements; for mid-market organisations, the emphasis is on scalability and process maturity; and for enterprises, the assessment includes deeper architectural review and alignment to compliance obligations. This makes the offering flexible, impactful, and suitable for organisations at any stage of their cybersecurity journey.

Contact Information: CMSCybersecurityServices@cmsdistribution.com

Table of Content Page ›

Service Package 5: Implementation Services

CMS SKU	Service Package	Cost	Short Description
412645	Solution Implementation Service	Qualification Call / Discovery Questionnaire prior to pricing	This offering combines a curated portfolio of proven security technologies with expert guidance and Quantum Evolve's implementation excellence, giving customers a strategic security advantage, faster time to value, and confidence in achieving stronger, scalable protection against real world threats.

Description:

To ensure our customers achieve the strongest possible security outcomes, we not only provide access to best-in-class technology solutions from our portfolio but also guide them in selecting the tools that will deliver the greatest operational impact. Our focus is on enabling organisations to modernise their security posture, simplify complexity, and close capability gaps with solutions that are proven, scalable, and aligned to real-world threats. By partnering with us, customers gain more than just technology, they gain a strategic security advantage built on expertise, trusted products, and measurable value.

To maximise the return on that investment, we work closely with Quantum Evolve, a specialist implementation and optimisation partner who ensures every deployment is delivered to the highest standard. Their team brings deep technical expertise, hands-on integration support, and a proven methodology to help customers get the most out of the tools we supply. This combined approach, our curated technology portfolio and Quantum Evolve's implementation excellence, ensures customers benefit from faster time-to-value, stronger security outcomes, and ongoing confidence that their solution is performing at its full potential.

Contact Information: CMSCybersecurityServices@cmsdistribution.com

Table of Content Page >

Service Package 6: : Artificial Intelligence and Machine Learning Assessment

CMS SKU	Service Package	Cost	Short Description
AIML-001	Artificial Intelligence and Machine Learning Assessment	Qualification Call / Discovery Questionnaire prior to pricing	The AI Posture Risk Assessment will provide an independent and expert view of the maturity of the customers AI posture, to identify gaps, vulnerabilities, understand cyber risks and identify enhancements to defend against real world cyber threats.

Description:

Quantum Evolve consultants will undertake an AI Posture Risk Assessment that aligns with the customers strategic objectives including compliance where applicable such as with IS27001, the UK's framework for AI regulation, and EU Artificial Intelligence Act. As the assessment should also consider the Legal implications etc. To ensure implemented and related Cyber, digital and security projects continue to contribute to business success. The AI Posture Risk Assessment will provide an independent and expert view of the maturity of the customers AI posture, to identify gaps, vulnerabilities, understand cyber risks and identify enhancements to defend against real world cyber threats.

The AI posture assessment will assist the customer understand:

- The existing AI estate via a virtual, data discovery exercise.
- The current security posture and identify urgent security needs against the threat from AI.
- An independent and expert view on the current maturity of the controls in place to address AI-Related Cyber Threats, Vulnerabilities, and Risk Exposure.

Continue

Service Package 6: Artificial Intelligence and Machine

The AI Posture Assessment provides the following:

- The ability to develop short-term recommendations to address urgent AI-related security needs, such as vulnerabilities or threats that require immediate attention.
- Identify and evaluate emerging AI services, solutions, and capabilities that can help improve their AI-related security posture.
- The ability to decide what activities you need to prioritise.
- The effort required to improve your Cyber Posture in line with your Risk Appetite.
- Identification of risk and priority areas that will improve overall AI-related Cyber Resilience and position the client to be better equipped at limiting exposure to unpredictable Cyber Threats.
- Benchmark customer against its peers – by sector and by size.
- Identify Board-focused deliverables and supplementary detailed technical content.
- Quantify risk in easy-to-understand monetary terms.

Leveraging appropriately previous security reviews, the AI Posture Assessment will collate the information gained to support the analysis and establishment of key risk areas. These risk areas are then available if required to test your controls against ISO27001 and NIST frameworks.

Contact Information: CMSCybersecurityServices@cmsdistribution.com

Table of Content Page ›