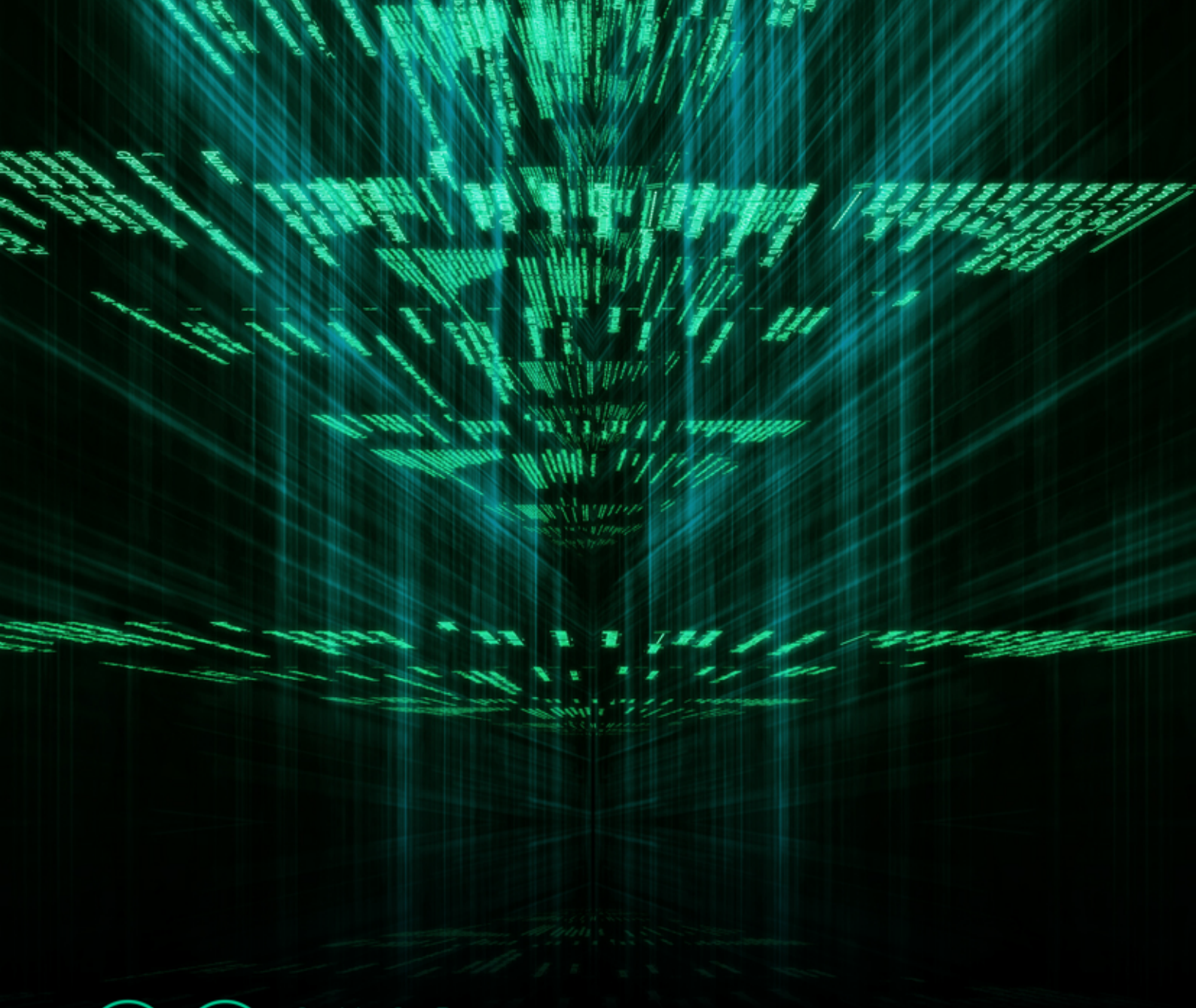


QUOD ORBIS

Continuous Controls Monitoring Buyer's Guide

www.quodorbis.com

Continuous Controls Monitoring: A Buyer's Guide

Navigating the security, risk, and compliance landscape: five key challenges for IT leaders – now, and in the future

> Cyber Risks have never been monitored closer by the exec team and nor have cyber threats been more prevalent.

Quod Orbis' **Continuous Controls Monitoring Buyer's Guide** aims to explain how Continuous Controls Monitoring (CCM) can help organisations to navigate these challenges, delivering value by highlighting what organisations should look for in providers of CCM solutions.

What exactly is Continuous Controls Monitoring? We'll look in detail at Continuous Controls Monitoring shortly. But for now, think of it as a means of ensuring that all of an organisation's cyber security, risk, and compliance tools are in place, that their controls are configured appropriately and working properly, and that they are providing the security, risk, and compliance reassurance that organisations need.

Which, when you think about it, is a vitally important capability for those organisations to possess.

Another day, another security breach

Mounting compliance burden

Stretched IT organisations

Human vulnerabilities

Board level concern

Another day, another security breach.

New cyber threats emerge all the time—and existing threats rarely fade into obscurity. No organisation can afford to lower its guard: the costs and consequences of complacency are too high.

Mounting compliance burden.

Organisations face increasing regulatory pressure, needing to comply with both national and international requirements. From GDPR to industry-specific requirements, frameworks such as ISO 27001, ITIL®, NIST, PCI, and COBIT set out best practices—but don't provide the actual tools to comply.

Stretched IT organisations.

Basic security, risk, and compliance assurance consume increasingly expensive resource, and rare skill. Compliance with standards such as the PCI Data Security Standard can consume weeks or months of IT resource in the run-up to an annual compliance audit.

Human vulnerabilities.

The evidence from real-life breaches reveals a familiar litany of failure: deactivated controls, alarms ignored, procedures not followed, systems and software not upgraded, and employees swamped with alert fatigue. The reality is prosaic: a failure of basic security fundamentals.

Board-level concern.

Regulators are no longer largely toothless—and boards know it. Take GDPR- fines can reach 4% of global turnover, and which are routinely in the tens of millions. And financial penalties are not the only issue of concern: reputational loss, brand damage, customer loss, and intellectual property theft are all of serious interest to organisations' boards.

Introducing Continuous Controls Monitoring

Asset Management

All organisations need to have confidence that all assets and identities are being monitored. This is a complex challenge for any company and it has prevented many businesses from realising the value of CCM.

CCM enables a real-time, intelligent asset discovery process. By connecting to all technology investments in an organisation (including non-cyber security tools such as HR platforms) an advanced CCM should collate all assets discovered and create a live repository that is self-attested continually being checked against each other and visually displayed in dashboards.

The objective is confidence that when monitoring controls a business has 100% of its asset covered and eliminates gaps. This aids resilience, compliance and enables quantitative cyber risk measuring.

Despite such concerns, the depressing conclusion for many IT leaders is that they don't need yet another security, risk, and compliance 'point solution'.

This, they realise, would just sap the productivity of the IT organisation. Instead, what they need is a means of ensuring that their existing security, risk, and compliance processes and point-solutions are actually in place, correctly configured, up to date, working properly, and doing their job.

What might such an approach look like?

It should be extensive, for a start, covering all of an organisation's security controls—potentially hundreds of them—and embrace every device, every system, every individual piece of network infrastructure, and every server.

It should also go beyond just security controls, but also **embrace business controls, risk controls, and relevant financial and compliance controls**.

It should be **automated**, rather than manual. People can be error-prone, are expensive, and introduce delays. Automated systems are obviously to be preferred.

It should **deliver hard, concrete, quantified data on cyber security, risk, and compliance**—not subjective judgements or opinions.

It should offer a more granular assessment than a simple 'yes or no, go or no-go' approach, and also be capable of prioritisation, and focus. Not all security controls are equal, and many are best interpreted with the aid of tolerance bands.

And it should be **real-time, and continuous**. A rear-view mirror, or a snapshot in time—once a quarter, say—is pointless. Breaches and disruption can happen any time.

Continuous Controls Monitoring

Such an approach exists: Continuous Controls Monitoring. It sometimes goes by other names—continuous security monitoring, continuous controls automation, continuous compliance, for instance—but the core approach is the same.

Namely to gather—**continuously and in real-time** all the data and evidence by connecting to your data sources, frameworks and controls to assess the state of an organisation's IT security, risk, and compliance, by continually monitoring all of a business's internal controls, via telemetry.

The result: security, risk, and compliance data that is factual and objective. Security, risk, and compliance data that is immediate. Security, risk, and compliance data that is drawn from right across the organisation's risk and vulnerability landscape. And security, risk, and compliance data that is delivered automatically.

How Continuous Controls Monitoring benefits organisations

Continuous Controls Monitoring is fast, efficient, and a far more robust approach to security, risk, and compliance than—say—questionnaire-based approaches, or periodic audits.

Organisations immediately benefit from its real-time insights and its impartial, objective, and independent perspective on security, risk, and compliance. Organisations also value the complete, holistic picture that it provides—a picture that is both technology-agnostic and data source-agnostic, and which offers a 'single source of truth', rather than multiple perspectives.

Risks are reduced, and fewer breaches result as controls effectiveness is constantly monitored and improved. The result: **complete visibility** into the organisation's performance in threat management, risk management and compliance, as well as visibility into compliance tracking and monitoring.

Thanks to its automated nature, Continuous Controls Monitoring also delivers a **rich seam of vital information** on security, risk, and compliance, enabling a ready provision of **board-level reporting data as well as operational control information**, and making it very straightforward to assess the organisation's security, risk, and compliance posture against any maturity framework, or against the organisation's internal Key Risk Indicators.

Similarly, that same rich seam of automated security, risk, and compliance information goes on to drive better-informed investment decisions, through the development of business cases that are based on hard, factual information on controls effectiveness and gaps.

In short, Continuous Controls Monitoring delivers an enhanced security posture, while also simultaneously freeing-up employee time through automation, driving down cost, and boosting productivity.

Consequently—and not surprisingly—in an era of rising cyber insurance premiums, a number of organisations that have deployed Continuous Controls Monitoring have reported lower cyber insurance premiums. Similarly, organisations that were previously unable to obtain cyber insurance coverage have found that cover was now being offered.

The clarity you need for asset management

By connecting to many pieces of technology, from cyber tooling to HR and business process tools your CCM platform sees all the assets on the network and records them in real time. It will highlight any gaps in coverage you might have. It will tell you what software is installed on each asset and if its patched correctly. I will also be intelligent enough to know what should be on each asset and when. CCM automatically correlates multiple pieces of data and technology together and presents this back to you.

A single view of the truth

Continuous Controls Monitoring brings heightened cohesiveness to an organisation's Security, Risk, and Compliance teams: no longer are they working in individual silos; they're working together, in unison, sharing the same single view of the truth.

Complete visibility into the organisation's controls environment in real time.

Instant discovery of any coverage issues, such as key controls missing from critical assets.

Early warning of potential security, risk, and compliance issues, enabling remediation before any adverse impact to the organisation.

Fewer 'false negatives', delivering increased security, risk, and compliance assurance.

A reduction in alert fatigue.

Increased efficiency and productivity.

Improved staff retention, as routine manual security, risk, and compliance assurance tasks are eliminated.

Skills gap shortening.

Total visibility of all your assets.

Building beyond the basics: what to look for in a Continuous Controls Monitoring solution

Not all Continuous Controls Monitoring solutions are the same. And not all providers of Continuous Controls Monitoring solutions are the same.

Which matters, as organisations move beyond the basics of what a Continuous Controls Monitoring solution delivers.

At Quod Orbis, we believe that it is important that a Continuous Controls Monitoring solution is capable of integrating with **any data,** from **any source,** and is able to work with **any security, risk, and compliance framework,** and **any** control.

We believe that it is important that a Continuous Controls Monitoring solution should also be **capable of integrating with any business system**—human resources, finance, ERP, GRC, or ITSM, for instance.

We believe that Continuous Controls Monitoring solutions should be **easy to manage, easy to learn, and easy to exploit to the full**, thereby maximising the return on organisations' investment in them.

We believe that CCM solutions should provide **visibility of all business assets on the network and report on them in real-time** to provide the basis for complete monitoring so that businesses can have the assurance of understanding all their assets and their effectiveness.

We believe that Continuous Controls Monitoring **solutions should deliver flexible reporting for any stakeholder, at any level**—as well as integrating readily into organisations' existing centralised reporting mechanisms, such as Crystal Reports, or PowerBI.

We believe that a Continuous Controls Monitoring solution should **possess a service proposition**, giving organisations ready access to a team of dedicated experts who live and breathe security, risk, and compliance, supporting organisations through implementation and beyond, and helping to maximise the value of the investment in a Continuous Controls Monitoring solution. Plus, as a service, organisations can have 100% confidence that the data being analysed is accurate and evidence-based.

And most importantly, we believe that a Continuous Controls Monitoring solution should **deliver actionable intelligence, enabling security, risk, and compliance teams to prioritise their actions better, remediate risks** more quickly, and eliminate manual data gathering and provisioning.

Exploring use cases: security and risk

How Continuous Controls Monitoring helps Security specialists

- **Critical information delivered in real time:** no need to rely on, or wait for, different operational and IT teams to report.
- **Security solutions, assets and controls** of all the organisation's security solutions and controls, eliminating the false sense of security that can often arise from having multiple tools.
- **Quantified and evidence based output:** impartial, accurate, real time information from a single source of truth.
- **Totally objective status reports,** wholly independent of any department's interpretation of data, or judgements.
- **Multiple data sources are both aggregated and correlated,** providing a complete, holistic picture that is technology agnostic and data source-agnostic.

- **Instant insight into coverage issues,** such as key controls missing from critical assets.
- **Early warning of potential security, risk, and compliance issues,** enabling remediation before they impact the organisation.

How Continuous Controls Monitoring helps Risk specialists

- **An automated, real time view of risk, governance and compliance** with coverage of all your assets, instead of a point in time (typically annual) view of risk.
- **Quantitative and objective reporting,** based on hard, factual data.
- **Alignment of risks to actual control efficacy,** eliminating interpretation and judgement regarding a control's status and effectiveness.
- **Through eradicating false, outdated, or misconstrued information regarding risk,** governance, and compliance, the Risk team can focus on critical priorities.
- **Continuous support from experts** if the organisation's provider of its Continuous Controls Monitoring capability offers it—and not all providers do—to manage the Continuous Controls Monitoring platform, enabling Risk teams to focus on the information that the platform is supplying, without the distraction of managing that information flow.

- **Truly effective organisational GRC** (Governance, Risk & Compliance) and IRM (Integrated Risk Management) programmes, thanks to the near elimination of manual tracking of risks and controls.
- **The flexibility to support any organisational approach or framework** in respect of risk reporting and modelling.

Exploring use cases: compliance and audit

How Continuous Controls Monitoring helps Compliance specialists

- Manual attestations replaced by **automated, continuous, real-time compliance**—delivering significant time and cost savings, as well total accuracy.
- If the organisation's provider of Continuous Controls Monitoring solutions provides it, the **capability to interact with any regulation, and any framework, and any standard**—including bespoke internal standards.
- **Security compliance automation, continually updated** with the latest legislation and framework revisions, providing simple compliance re baselining.

- Manual, point in time compliance activities replaced by **automated real-time compliance**, together with compliance tracking and compliance monitoring.
- No more 'pre audit scrambles': Continuous Controls Monitoring provides the organisation with **all the evidence that it requires, in one single source of the truth**.
- **Dramatically reduced duplicated effort, time, and cost across the multiple audits** that organisations must undertake—internal audits, external audits, ISO 27001, Sarbanes-Oxley, the Payment Card Industry Security Standards Council's PCI Data Security Standard, and so on.
- Continuous Controls Monitoring provides the basis for **effective and cost-efficient Governance, Risk and Compliance programmes, and Integrated Risk Management programmes**.

How Continuous Controls Monitoring helps Audit specialists

- **The assured ongoing effectiveness of all security controls,** through ongoing 24/7 monitoring, assessment, and analysis.
- **Ongoing reporting** on the security posture of information systems.
- Organisational risk tolerance at **maintained at predetermined levels of acceptability**.
- **Ready reporting** of both the effectiveness over time of the organisation's security controls, and any changes to those controls that might have occurred.
- **Board-level reporting** of cyber security status information, 'out of the box'.

The service dimension: what should organisations expect?

At first glance, it might be expected that the service offerings of the various Continuous Controls Monitoring solution providers in the marketplace might be broadly comparable.

Not so. Some providers prefer to focus mainly on the 'hard' technology of Continuous Controls Monitoring, while others—Quod Orbis among them—believe that a rich service offering enables users to leverage their investment in Continuous Controls Monitoring to the full.

Here at Quod Orbis, we believe that our service 'wrap', as we call it, is especially distinctive, freeing users to focus on what they do best—running their organisations—while much of the day-to-day minutiae of managing and monitoring the organisation's Continuous Controls Monitoring solution is best left to experts.

Higher-level service expectations

So as a prospective buyer of a Continuous Controls Monitoring solution, what should be your expectations of a Continuous Controls Monitoring solution provider's service offering?

At a high level, we believe that it is reasonable to expect three key service 'phases':

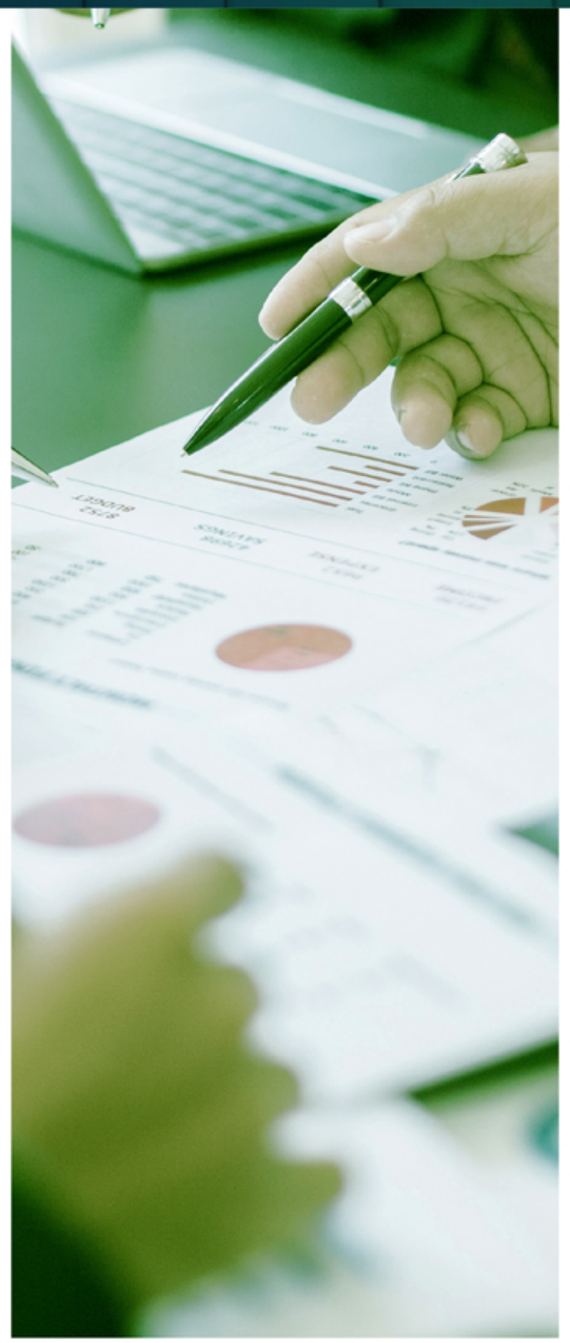
- During initial onboarding, intense collaboration between the provider and the customer organisation, designed to **discover business assets which are the controls that matter to the organisation's security, risk, and compliance assurance posture**, and how those controls are best assessed and interrogated.
- **Collaboration here is key:** the customer organisation is best qualified to know their business and its controls, while the Continuous Controls Monitoring solution provider understands their solution best, and best understands how to exploit is capabilities to the full.
- During the subsequent implementation, there will be a requirement for **continuous support** from the Continuous Controls Monitoring solution provider's internal experts, in order to make sure that **controls are being interrogated and assessed correctly**, and that in each case the requisite level of security, risk, and compliance assurance is being delivered as desired.
- Again, the issue here is one of relevant levels of expertise and domain knowledge: the Continuous Controls Monitoring solution provider's experts know and understand Continuous Controls Monitoring best; while the customer organisation is best placed to determine that the level of assurance that is being delivered is one that meets their needs.
- Once fully onboarded, customer organisations should expect to benefit from their Continuous Controls Monitoring solution **provider expertly managing and monitoring their controls 24/7, providing complete assurance** that their security, risk, and compliance posture is fully operational, and providing expert remediation should any issues arise.
- They should also expect to be **allocated their own Customer Success Manager** to act as an interface to their Continuous Controls Monitoring solution provider's experts, and provide ongoing updates for control frameworks, advice on any regulatory and framework changes, and recommendations on how best to respond to those changes.

Operational expectations

What about operational support? Again, service offerings differ. Here at Quod Orbis, but we believe it is reasonable to expect:

- **Critical metrics** monitored including asset visibility.
- **New controls and metrics** to be continuously onboarded.
- **Continuous checks** of platform availability.
- **Real-time** snapshots of data.
- **Optional** consultancy support.
- **Integrations with ITSM** tools for issue prioritisation and resolution.
- **Personalised dashboards** per user, team, or requirement.
- **Fully exportable** reporting including third party tools.
- **Data to be anonymised** prior to extraction and reporting.

Continuous Controls Monitoring: simply a better cyber security solution



It's not difficult to see that Continuous Controls Monitoring is both a different approach to IT security, and a better approach. It's a fast, efficient, and a far more robust approach to security, risk, and compliance than—say—questionnaire-based approaches, or periodic audits.

It brings real-time insights, and proves an impartial, objective, and independent perspective on security, risk, and compliance. It's both technology-agnostic and data source-agnostic, providing a 'single source of truth', rather than multiple perspectives.

And not only does Continuous Controls Monitoring deliver a rich seam of vital information on security, risk, and compliance—enabling a ready provision of board-level reporting data, and making it very straight forward to assess the organisation's security, risk, and compliance posture—but that assessment can be against any maturity framework, or any given standard. PCI compliance, for instance, has never been easier.

At Quod Orbis, in short, we believe that choosing Continuous Controls Monitoring is the only rational decision when it comes to improving the organisation's security, risk, and compliance posture. But from which provider?

This Continuous Controls Monitoring Buyer's Guide has highlighted what Continuous Controls Monitoring is, how it works, and how it benefits organisations. In doing so, it has strived to—objectively and impartially—outline those aspects of a Continuous Controls Monitoring solution that we believe to be most important to organisations.

So where—and how—to begin your Continuous Controls Monitoring selection process? We'd suggest the following ten questions would be a very good starting point for any conversation with a Continuous Controls Monitoring solution provider.

Continuous Controls Monitoring buyer's guide: ten questions to ask a prospective provider

One

To how many data sources, controls, and frameworks can your Continuous Controls Monitoring platform connect?

Is there a maximum limit?

Two

Are controls monitored 24/7 to ensure that the organisation's security, risk, and compliance posture is up to date and fully effective at all times?

Three

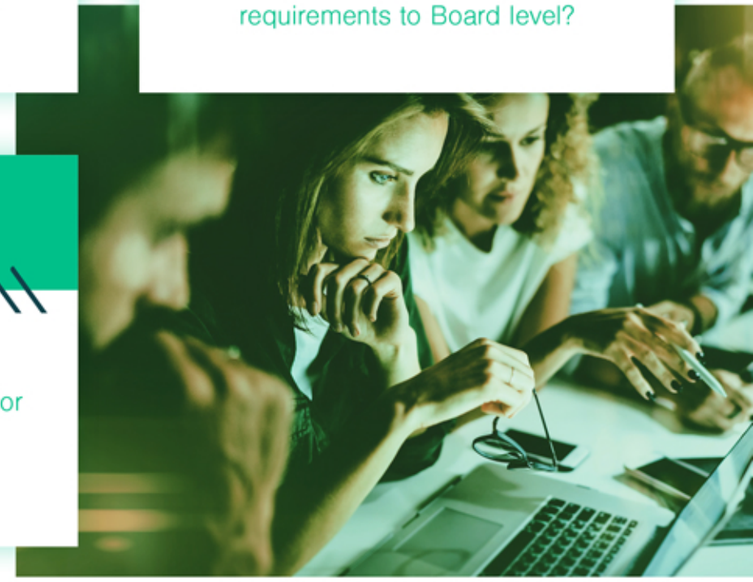
Once onboard, how flexible is the Continuous Controls Monitoring solution in terms of being able to evolve as customers' underlying needs evolve?

Four

Does the platform's reporting capability embrace the requirements of every stakeholder—from operational requirements to Board level?

Five

Can the Continuous Controls Monitoring solution align to all major global regulations and internal control frameworks?



Six

How can you support our cyber risk quantification reporting requirements?

Seven

Can your Continuous Controls Monitoring solution connect to our cloud, legacy, and on-premise systems?

Eight

Can your Continuous Controls Monitoring platform offer continuous compliance for industry and bespoke control frameworks?

Nine

How do you ensure your Continuous Controls Monitoring platform remains 100% accurate to your control state for the life of the contract?

Ten

Can you demonstrate the ROI savings attainable through automating your control monitoring process?

Quod Orbis Limited, 2nd & 3rd Floor, 2 Burgon Street,
City Of London, London, EC4V 5DR, United Kingdom

T +44 (0)20 3962 2206 www.quodorbis.com