
QUOD ORBIS
5
Myths About Continuous Controls Monitoring
www.quodorbis.com

\\ Contents

\\ Introduction

Continuous Controls Monitoring (CCM) has come a long way.

What started as a tool for tracking financial controls has now evolved into a powerhouse for real-time cyber security and compliance. As organisations embraced digital transformation, the need for faster, more accurate risk detection skyrocketed—far beyond what periodic audits could handle. Automation supercharged CCM, making it a game-changer in today's complex security landscape.

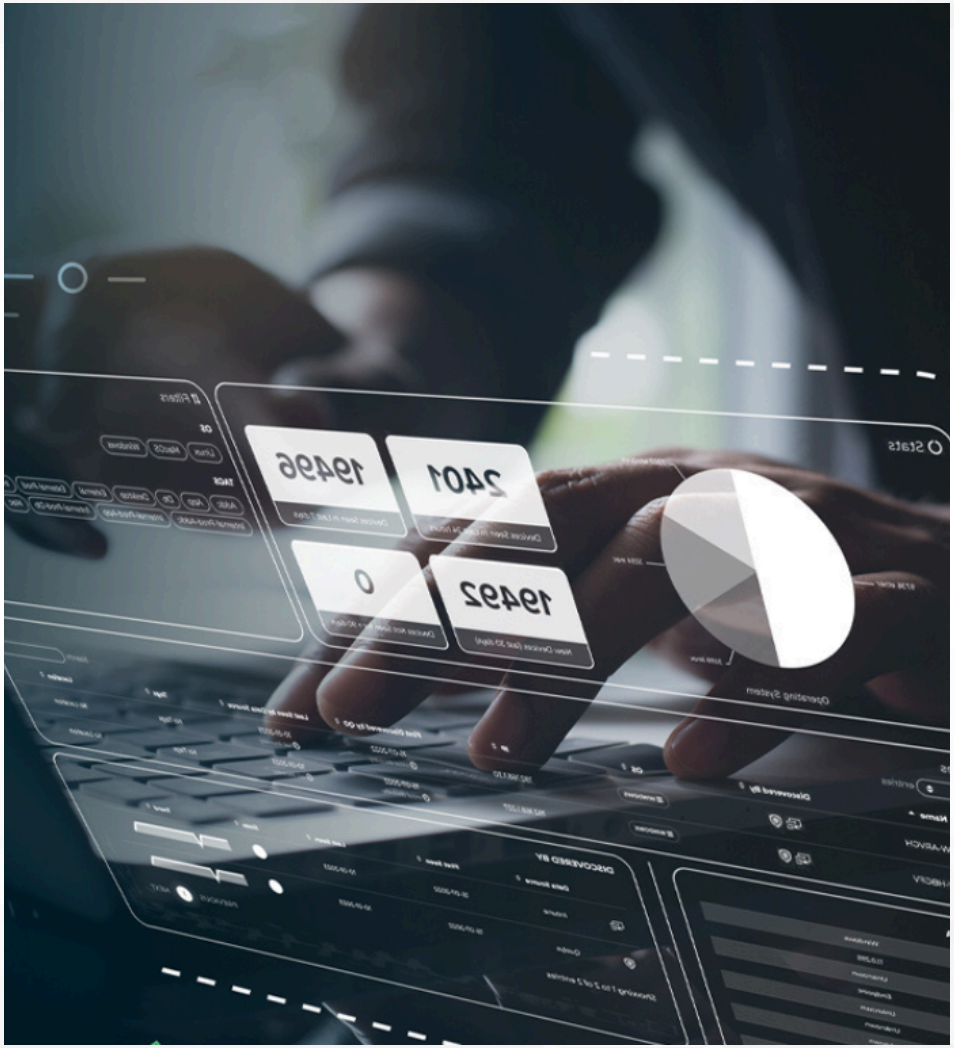
Initially, Gartner positioned CCM within the Governance, Risk, and Compliance (GRC) space, focusing on policy alignment and regulatory demands.

As cyber threats surged across hybrid and multi-cloud environments, CCM emerged as a critical tool for:

- Continuously validating security controls.
- Addressing the limitations of traditional perimeter defences.
- Providing a "single source of truth" for cyber security, risk, and compliance.

But with its rise, myths have taken root—myths that could hold your organisation back from fully leveraging this powerful technology. This eBook busts five of the biggest myths about CCM and reveals the truth behind them.

Ready to find out what's holding you back? Let's dive in.



\\ Myth No. 1
Organisations Must Be Cyber Mature

Let's be honest, organisations usually have complex ecosystems that have grown unwieldy after years of unrestrained technological adoption. Every investment was made to help counteract the exponential rise in evolving threats and regulatory change, but now these businesses are left with swollen tech stacks that lack efficiency.

Many organisations believe their cyber security programme is simply not mature enough, as they lack well-established cyber security frameworks and processes to integrate CCM effectively. Couple that with a perception that CCM is far too complex to adopt with their advanced tailored dashboards, organisations may simply feel that they are not quite there in terms of their maturity. Over worked teams with limited budgets, and a pinch of uncertainty about CCM's ROI, adds to the existing perception that CCM can only be adopted by a team with robust cyber security measures, significant funding and basic controls that are operational.

A technology that supports growth in maturity

This perception has evolved over the years, but nothing could be further from the truth!

Continuous Controls Monitoring supports cyber maturity growth. It is certainly not the finish line, it's the catalyst.

The fact of the matter is, CCM is a maturity enabler and can be adopted from any entry point that an organisation needs. Its real-time insights help businesses identify gaps, prioritise resources, and build their maturity incrementally.

Focus can start with KRI's/KPI's, or a certain framework.

Scalable and accessible technology

CCM is not a one-size-fits-all solution. Instead, it's designed to be scalable and adaptable to organisations at various maturity levels. Value is delivered immediately without requiring a full implementation, such as through monitoring critical controls.

"We've had some light bulb moments in the platform where particularly around vulnerabilities, the CCM platform has highlighted things we simply didn't know and the trending information will start to demonstrate areas we need to keep an eye on."

Chris Taylor Information Technology Manager at Martin-Baker Aircraft

Proactive risk reduction

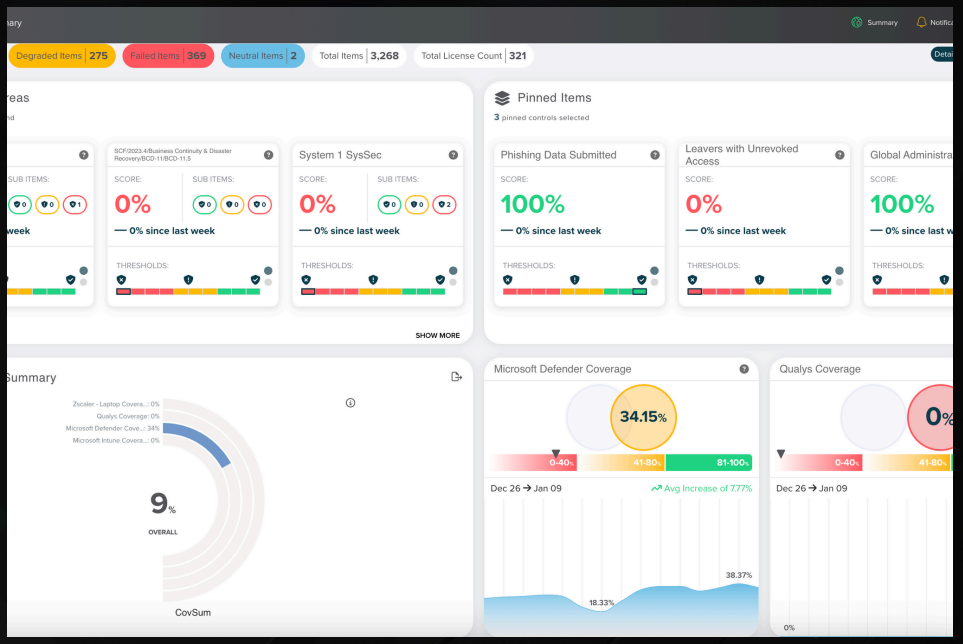
Proactivity is an immediate result of CCM - the technology addresses risk in real-time, rather than relying on point-in-time assessments. If organisations wait until they feel they are mature enough, they will leave themselves exposed to risks that often lurk in the shadows.

Compliance and cyber security as key drivers

Whilst traditionally perceived as only being a cyber security tool, CCM is now becoming more recognised as a highly effective way of monitoring compliance.

Aligning to any framework, CCM can monitor your entire ecosystem to ensure you have complete visibility over your cyber security and compliance posture.

> Gartner coins Continuous Compliance Automation as the technology to support regulatory compliance. However CCM is the one tool that provides asset visibility, continuous monitoring of your cyber risk and compliance posture.



Cost effectiveness through efficiency

Organisations perceive that CCM is expensive to purchase, costly to adopt and a drain on resource throughout implementation. This is certainly not the case.

CCM pulls information from all your disparate tools to provide a cohesive single source of truth. If you align with the right vendor, they should support with scoping, implementation and ongoing maintenance so that your teams maximise the value the technology delivers.

If your organisation feels immature, then consider the quick wins

CCM can always start small, maybe focusing on KRI's or a handful of critical controls. From there, it can expand to match a business' maturity.

If you grow, the platform grows with you.

Scalable Evolution at Your Own Pace – Start Small, Grow Strategically

The capability of CCM is not restricted to organisations deemed 'completely' mature. Organisations can start at a foundational level and grow the platform in the areas that are most critical.

A typical way that CCM can evolve with an organisation could be:

Phase 1 – Identify Your Entities

Phase One: Entities

- **Identity & asset visibility**
- **Tuning of identity/asset data**

(provides fundamental base for everything else)

- **Coverage controls, e.g.**
  - Key controls expected
  - EDR on all end-points etc.
- **CMDB comparison & improvement**

CAASM

Ensure that you have complete visibility of your assets across the organisation.

CCM supports your cybersecurity maturity by starting with the identification of all assets within your organisation—whether IT, IoT, or cloud-based. This is crucial because CCM is a maturity x10 enabler—most organisations struggle with knowing what assets they actually have, as there is no complete CMDB on the planet.

Gartner heavily invested in the CAASM category to address this challenge, but these solutions remain point-in-time snapshots unless integrated with a CCM approach.

Gaining full visibility into your asset landscape is the foundation for effective risk management, allowing you to detect gaps, enforce security policies, and monitor compliance in real time.

Control No.1 in Every Framework- Know what you need to protect

Phase 2 - KRI's/KPI's

Phase Two: KRI/KPI

- **Key Risk Indicators**
- **Key Performance Indicators**
- **Own organisations KPI/KRI's and/or augmented by QO recommendations (such as Ransomware related)**

CCM CSPM SSPM

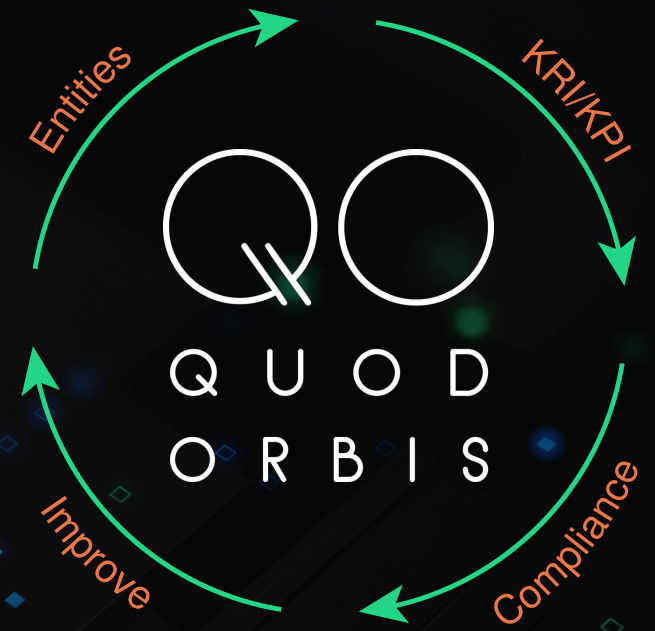
Continuous Controls Monitoring (CCM) enhances KRIs and KPIs with real-time visibility into security and compliance.

1. Automated, Real-Time Data – Eliminates manual audits with accurate, up-to-date risk and performance insights.
2. Early Risk Detection (KRIs) – Tracks unauthorised access, anomalous behavior, and security non-compliance.
3. Performance Monitoring (KPIs) – Measures MTTD, MTTR, patching effectiveness, and compliance rates.
4. Customisable Dashboards – Provides clear, actionable insights for decision-making.
5. Benchmarking & Trends – Compares KRIs/KPIs against industry standards to highlight improvement areas.
6. Compliance Readiness – Tracks security controls to demonstrate regulatory alignment.

Reduced Noise & False Positives – Filters irrelevant alerts to focus on real risks.

Phase 3 - Compliance

This is the culmination of efforts to automate in-scope frameworks, aligning compliance with business maturity and data availability.
CCM acts as the driving force that propels an organisation's security and compliance posture forward. As the business matures through earlier phases —likely involving establishing visibility, managing risks, and optimising processes—this final phase solidifies those efforts by embedding automation and ensuring continuous adherence to regulatory frameworks.



Phase Three:
Compliance

- **Automation of as much of in scope frameworks as possible**
- **Based on organisation maturity and data availability**

CCM CCA

Why This Is the Last Cog in the Wheel:

1. Automation Completes the Cycle:
By automating compliance frameworks, organisations reduce manual effort, enhance accuracy, and create a self-sustaining system that continuously monitors and improves controls.

2. Data-Driven Decision Making:
The maturity gained through CCM allows for a data-driven approach, ensuring compliance efforts are aligned with the organisation's operational realities.

3. Readiness for Advanced Assurance (CCA):
The transition from CCM (Continuous Controls Monitoring) to CCA (Continuous Compliance Assurance) signifies that the organisation has reached a level where compliance isn't just a checkbox but an ongoing, integrated practice.

4. Strategic Growth:
With compliance automation in place, businesses can focus on innovation and growth without the constant burden of regulatory uncertainty.

\\ Myth No. 2

Existing Tools Already Do the Same Thing

Everywhere you turn, vendors are vying for your attention, each one proclaiming their technology as essential; the ‘perfect’ solution to fill a gap in your tech stack.

The emergence of new technologies only amplifies this. All of a sudden, everyone has content explaining how their tools already support or integrate the latest trend.

It’s easy for the lines to blur. One tool starts looking indistinguishable from the next. Vendors begin leaning heavily into new buzzwords, like Continuous Controls Monitoring, claiming their solutions already provide the same capabilities.

But how can you be certain? Between SIEMs, GRC tools, and manual processes, it’s tempting to assume your stack already covers CCM functionality. However, true understanding requires a deeper dive into what CCM actually entails and how your existing tools measure up – or most likely, fall short.

Let’s unblur the lines.

1. SIEM technology

SIEM tools log and analyse information from firewalls, servers, and applications, providing real-time and historical insights. They detect threats by correlating log data and identifying potential security incidents, alerting teams based on pre-determined rules.

SIEM technology investigates incidents and reports on compliance against frameworks such as PCI and GDPR, offering centralised visibility into an organisation’s security posture.

Sounds like Continuous Controls Monitoring, right?
Wrong.

CCM is proactive, SIEM is reactive

SIEM solutions rely on log data that is pushed into the system, meaning they can only analyse what is sent to them—essentially looking for the needle in the haystack.

In contrast, CCM takes a proactive approach by pulling any type of data—not just logs, which typically make up a small portion of what it collects. This approach ensures pinpoint accuracy in proving that controls are effective, rather than waiting for an incident to occur.

Automated and continuous

SIEM reacts to events by analysing logs, while CCM continuously monitors security controls across multiple data sources, alerting in real-time to prevent issues. SIEM reduces response time—CCM reduces the likelihood of incidents altogether.

Beyond Compliance Limitations

SIEM’s compliance features cover limited frameworks like PCI or GDPR. CCM delivers broader, adaptive compliance by assessing control effectiveness across multiple frameworks and operational domains.

2. GRC platforms

GRC platforms often market themselves as being able to continuously monitor organisations' governance and risk. However, the reality is vastly different.

GRC platforms rely on periodic data uploads from assessments, manual audits, or static reports. This data quickly becomes outdated, failing to reflect real-time changes.Updates often depend on human intervention, such as entering audit results or manually flagging issues. This makes continuous monitoring more of a scheduled activity than an ongoing process.

Static versus dynamic

GRC platforms rely on periodic assessments which means static out-of-date data.

CCM platforms provide near real-time continuous controls status updates on cyber security, risk and compliance posture.

Automation versus workflow

CCM is automated, meaning that teams have assurance in the accuracy of the data—there is no opportunity for human error and the focus can be on proactivity rather than reactivity.

Limited integration versus holistic capability

GRC has limited real-time integration with operational systems, whereas CCM tools connects to your entire business ecosystem, providing a holistic viewpoint of your cyber security risk and compliance posture.

CCM is the magic ingredient for GRC

CCM brings GRC to life when integrated together, making it more effective and efficient in managing risk and compliance to deliver strategic and operational benefits:

- Real-time visibility
- Proactive response
- Automated evidence collection
- Actionable insights
- Continuous assurance

3. Power BI

Power BI is a powerful enterprise-wide reporting tool designed for visualising and analysing fixed data from multiple sources. It excels at generating dashboards and reports that help organisations track key performance indicators and business metrics.

However, Power BI is fundamentally a reporting solution—it pulls in static data for analysis but lacks the ability to continuously monitor, validate, and correlate data in real-time. It's great for retrospective insights but falls short when it comes to proactive security and compliance monitoring.

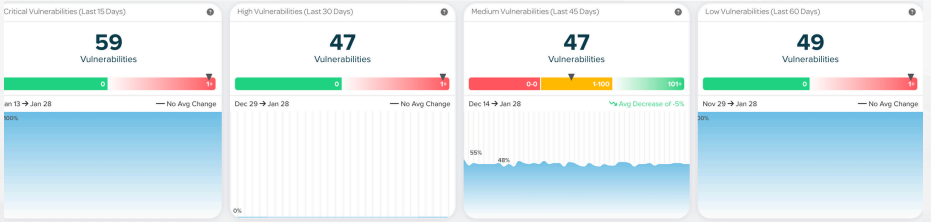
The CCM Difference

Unlike Power BI, which is limited to fixed data sets and predefined connectors, CCM is purpose-built for continuous control monitoring. It provides real-time data feeds from thousands of sources with no limitations, thanks to its low-code/no-code backend.

CCM doesn't just report on what's already happened—it actively monitors controls, identifies coverage gaps, and ensures that no critical asset is left unchecked. Power BI's inability to perform complex control calculations or provide comprehensive visibility makes it an incomplete solution for organisations seeking true operational resilience.

Compliance isn't just an add-on for CCM—it's a core feature. While Power BI wasn't designed for audit-ready compliance, CCM delivers immutable evidence to satisfy regulatory requirements and audits effortlessly.

Businesses can monitor their controls continuously, identify weaknesses instantly, and remain compliant without disruption. In short, Power BI tells you what happened, while CCM ensures you're always in control of what's happening now.

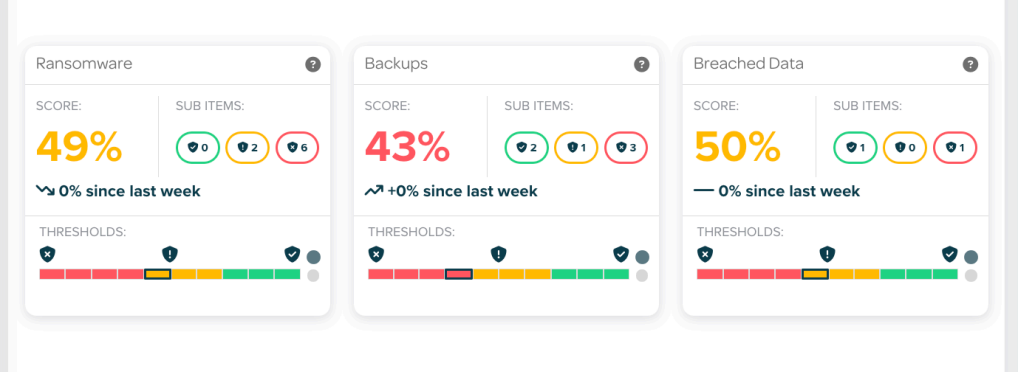


\\ Myth No. 3
It Is Just a Compliance Tool

It's true, Continuous Controls Monitoring is an incredible solution for compliance and an increasing number of regulations now demand continual monitoring as standard – ISO 27001, PCI V 4 and DORA are just two examples. Now this is what organisations think of when they think of CCM.

However, limiting this tool to compliance alone is like making the Swiss army knife just to use it as a bottle opener.

CCM in reality, is a far more powerful tool that goes beyond audit requirements. It strengthens an organisation's cyber security posture, reduces operational inefficacies, boosts operational resilience, and provides far greater insights on operational risk. So not realising the full potential off this tool is merely overshadowing what it can accomplish for organisations.



The cost of manually monitoring controls can add up significantly for enterprise businesses. The average cost to manually monitor each control for an enterprise-level business is £1.5K* per control test.

However, this does not account for the time the second line of defence has to chase for information, analyse the results, provide feedback, and ask why controls are failing. Nor does it consider the time the first line of defence spends collecting the necessary information, formatting it correctly, and reporting it to all relevant stakeholders.

But that aside, let's break down the potential total costs based on typical enterprise needs:

1. Number of Controls:
   - Large enterprises often have 500 to 5,000+ controls across their cybersecurity, compliance, and risk management frameworks.
   - Assuming an average of 1,000 controls, this already becomes a substantial figure.

2. Testing Frequency:
   - Manual control tests are often conducted quarterly or annually, depending on regulatory requirements and business risk tolerance.
   - Quarterly testing (4 times a year) means the cost multiplies rapidly.

Estimated Cost Calculation:
   - 1,000 controls x £1,500 per test = £1.5M per round of testing.
   - Quarterly testing = £6M per year.

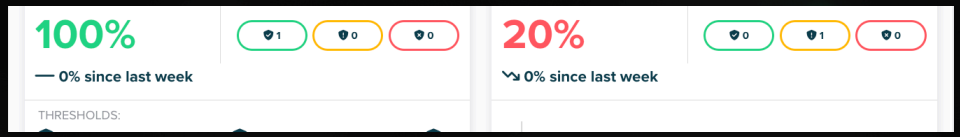
And this is purely the cost of executing the tests—not the hidden costs of inefficiencies, delays, and resource drain across multiple teams.

*This cost of monitoring each control manually was aquired by an enterprise client of QO.

The Broader Impact of Continuous Controls Monitoring

Automation that validates controls and delivers real-time actionable insights beyond regulatory frameworks.

- Automation that connects and empowers: CCM connects to your entire ecosystem providing near-real-time insights in your cyber security and risk posture.
- Beyond Compliance to Resilience: CCM takes cyber security to the next level by continuously tracking control failures—such as unpatched systems or unauthorised access—and delivering early warnings before incidents escalate.
- By integrating Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs), CCM empowers organisations with actionable insights, enabling them to measure security effectiveness, anticipate potential threats, and respond proactively. This data-driven approach not only enhances compliance but also strengthens overall resilience against evolving cyber threats.
- Operational Efficiency: Automation reduces the manual burden of evidence collection, control testing, and reporting. Teams can focus on strategic initiatives instead of getting bogged down in repetitive tasks.



- Risk Management: By offering real-time visibility into risks, CCM enables organisations to act quickly on emerging issues. For example, identifying a misconfigured firewall in minutes rather than weeks could prevent a potential breach.
- Stakeholder Confidence: A robust CCM program signals to customers, partners, and regulators that an organisation is committed to proactive security and governance, bolstering trust and competitive advantage.

Customers of our CCM platform are typically seeing a 75% increase in their cyber risk visibility.

The Cost of the Compliance-Only Mindset

Cost is not always a black and white number.

There are sometimes far greater costs to having a particular mindset rather than embracing the full potential of something.

So, whilst you can focus your CCM platform on regulatory compliance, you will be overlooking the full potential of what you could achieve with CCM and any operational blind spots that don't fall within the scope of specific regulatory frameworks.

Our latest research identified that the average large enterprise are managing 19 security solutions at any one time with a quarter citing a lack of visibility being as a significant challenge.

Our latest research identified that the average large enterprise are managing 19 security solutions at any one time, with a quarter citing a lack of visibility being a significant challenge. Access the full research here.

Here Is the Cost Broken Down:

- Critical issues, such as misconfigurations or unmonitored third-party risks, may go unnoticed simply because they aren't mandated by an audit. The average cost of a data breach globally was $4.88 million in 2024, so can organisations afford to ignore what oversight technology they need?
- Focusing solely on compliance also means missing out on the cost-saving potential of automation and optimisation. CCM can reduce manual effort, streamline processes, and free up resources—benefits that extend far beyond compliance, identifying risk exposures by up to 40% by enabling real-time adjustments and proactive management. This contributes to both direct financial savings and improved operational efficiency across compliance and risk management.
- Perhaps most importantly, focusing solely on compliance can erode your competitive edge. Customers and stakeholders increasingly expect organisations to demonstrate robust resilience and proactive risk management.
- Limiting CCM to compliance could make your business appear reactive, rather than innovative and forward-thinking.

Ask yourself: are you limiting your organisation's potential by viewing CCM merely as a compliance tool? If so, it's time to rethink what CCM can do.
Compliance may be the starting point, but it's far from the end goal. By focusing solely on meeting regulatory requirements, organisations miss out on CCM's broader potential to enhance resilience, drive operational efficiency, and support long-term growth.

To unlock the full value of CCM, organisations must view it as a strategic tool, not just a compliance necessity. Embracing CCM as a holistic approach can transform how you manage risk and deliver value to stakeholders.

\\ Myth No. 4
CCM Is Expensive to Implement

Organisations are expected to have spent approximately $213 billion globally on cyber security software in 2024, with overall annual spending on products and services projected to reach $459 billion by 2025. These investments reflect the increasing sophistication of cyber threats and the critical need for robust security measures.

Despite this, many Boards remain hesitant to allocate bigger budgets to digital security.

Reasons include financial pressures like inflation and recession fears, as well as uncertainty about the tangible returns on these investments. Some leaders also believe their existing tools are sufficient or struggle with prioritising cyber security amidst competing business needs.

> Organisations often focus more on prevention rather than resilience, underestimating the inevitability of breaches and the importance of mitigating their impact.

So, there are an array of challenges when deliberating over new tech implementations, like Continuous Controls Monitoring. Leaders question the necessity behind investing in new technology to fill security gaps, and the myth that CCM is expensive and takes too long to implement has now become a reoccurring theme in the board room.

1. Origins of the Myth

The belief that Continuous Controls Monitoring is costly stems from outdated perceptions of traditional security and compliance processes. Historically, audits and control assessments have been manual, time-intensive, and resource-heavy, making it easy to assume that implementing CCM would require a similar investment.

Many leaders also fear that customisation and integration demand significant upfront costs and specialised personnel, making the transition seem daunting.

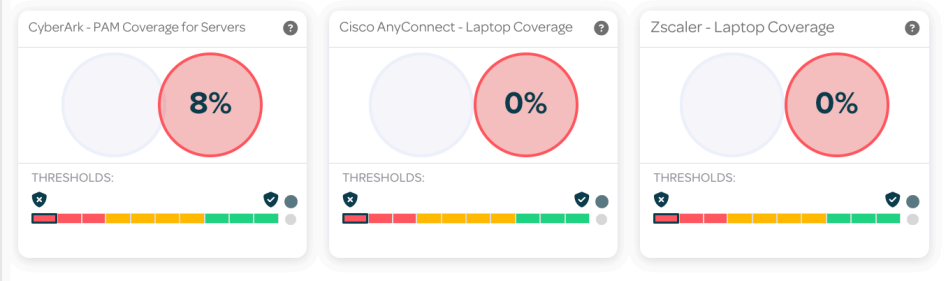
Adding to this, some organisations adopt the "if it ain't broke, don't fix it" mentality. Because they believe their current security measures are adequate, they resist automation, failing to account for long-term savings and improved risk management.

2. Breaking Down the Reality - CCM Is Cost-Effective & Scalable

Modern CCM solutions eliminate these cost concerns by providing:

- Flexible, scalable pricing – Organisations can focus on what they need, avoiding large upfront costs.
- Automation that cuts costs – By replacing manual audits, CCM reduces labor expenses, eliminates redundancies, and minimises compliance-related penalties.
- Seamless integration – Pre-built API connectors allow CCM to fit within existing security infrastructures, reducing time and expense.

CCM platforms leverage automation and APIs to integrate quickly with existing systems with key vendors offering tailored platforms so that each customer can leverage the platform for their unique requirements.



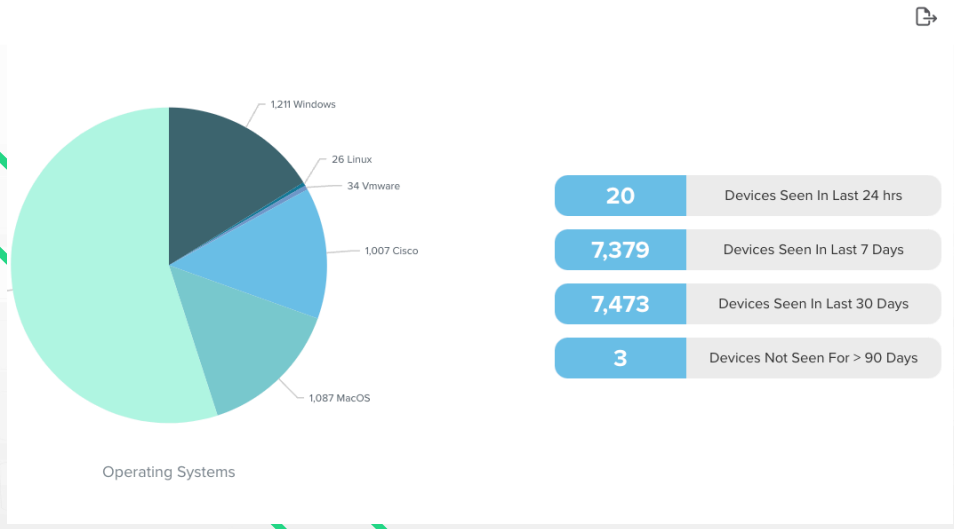
3. Real-World Benefits of CCM

Implementing Continuous Controls Monitoring delivers value, fast:

- Quicker detection of control failures.
- Reduced cost of periodic audits and greater proactivity rather than reactivity.
- Enhanced resilience, reducing financial impact of breaches.

Our client, a global leader in aircraft manufacturing for 79+ years, has achieved this ROI:

- 2-3X more visibility (stood by the 75%)
- 50% more vulnerabilities discovered
- 1,000 more devices unearthed



The Cost of Doing Nothing: The Hidden Risks of Avoiding Continuous Controls Monitoring (CCM)

While adopting CCM might seem like a significant investment, the cost of inaction often far outweighs the price of implementation. Below, we delve into the hidden costs of not integrating CCM into your cybersecurity and operational strategy:

1. Higher Cyber Risks

Without CCM, blind spots in controls leave organisations vulnerable to attacks.

IBM reports the average cost of a data breach reached $4.45M in 2023, with delayed detection driving up losses.

*Access the report here.

2. Regulatory Non-Compliance Fines

Manual processes increase the risk of compliance failures and penalties.

GDPR fines for organisations like British Airways and Marriott have surpassed $900M, often due to poor visibility of controls.

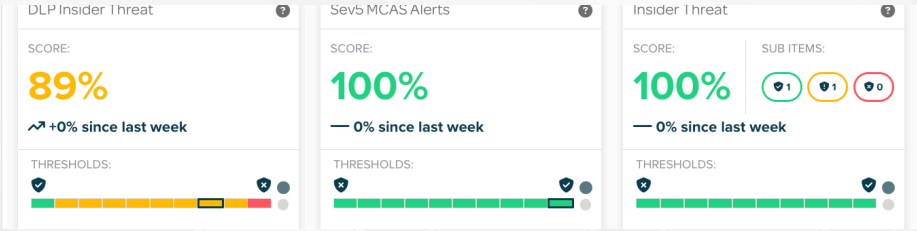
3. Operational Inefficiencies

Manual monitoring is slow, error-prone, and resource-intensive.

Ponemon Institute shows breach detection via manual processes can take 200+ days, leading to prolonged downtime and escalating recovery costs. Access the report here.

CCM: A Strategic Investment

CCM isn't just a tool—it's a critical strategy for real-time risk mitigation, regulatory compliance, and operational efficiency. The cost of doing nothing isn't just financial; it's a risk to your organisation's survival in an increasingly demanding digital world.



\\ Myth No. 5
Too Complex and Time-Consuming

Many organisations hesitate to adopt CCM due to fears of lengthy implementation timelines and resource-intensive onboarding.

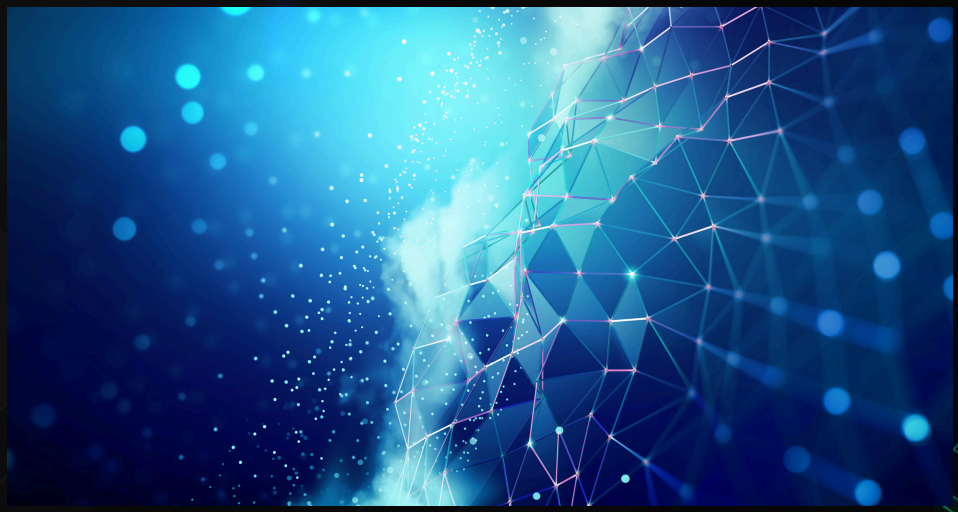
Some believe that CCM requires a complete infrastructure overhaul, while others worry that it will divert cyber security teams from mission-critical tasks.

The assumption that CCM needs heavy customisation and consultant-driven deployments further discourages adoption, making it seem out of reach for lean security teams.

Where the myth comes from

The misconception about CCM's complexity likely stems from its ambitious scope.

- CCM integrates data from diverse systems,
- Continuously monitors compliance against frameworks,
- Delivers actionable insights in real-time.



At first glance, this can seem daunting—especially to organisations already stretched thin with resource-intensive cyber security tasks.

There's also a lingering perception that implementing CCM requires wholesale infrastructure changes or lengthy, consultant-heavy projects. In truth, many of today's CCM solutions are designed to integrate seamlessly into existing environments, offering a low-friction path to adoption.

The Simplicity of CCM solutions

Thanks to innovations in cloud computing, APIs, and machine learning, implementing CCM is no longer the monumental task it's imagined to be.

1. Plug-and-Play Integrations

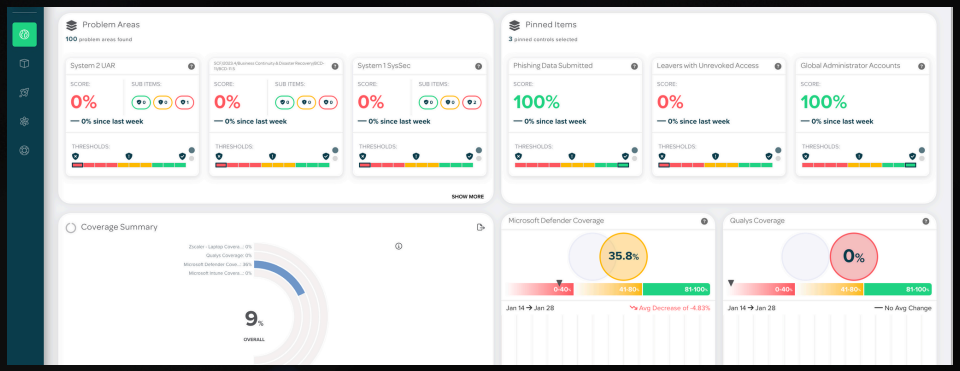
Modern CCM platforms come with pre-built integrations for commonly used tools—think Microsoft 365, AWS, and ServiceNow. These integrations make it easy to connect your existing systems without extensive customisation.

2. Cloud-Native Architectures

Gone are the days of on-premises infrastructure overhauls. Cloud-native CCM solutions can be deployed quickly and scale with your organisation, minimising upfront costs and implementation timelines.

3. Disparate Environments

If you have a mixture of cloud and on-premise, CCM's should be able to connect to all environments and pull the information into one cohesive view.



4. User-Friendly Interfaces

Intuitive dashboards and straightforward workflows eliminate the need for specialized expertise. Teams can quickly learn how to configure, monitor, and act on CCM insights.

5. Automated Processes

One of CCM's core strengths is automation. Rather than relying on manual, error-prone processes, CCM automatically collects data, evaluates control performance, and generates reports. This reduces administrative overhead and speeds up adoption.

CCM Evolves as Your Organisation Does

For many organisations, the fear of disruption is a significant deterrent. Teams worry that implementing CCM will pull resources away from critical projects. However, the right approach can ensure a smooth transition:

Pilot Programs

Start small by focusing on a high-impact use case or a specific compliance framework. Demonstrating quick wins builds momentum and confidence for broader rollouts.

Incremental Rollouts

Rather than trying to do everything at once, organisations can adopt CCM in phases. This approach allows for continuous learning and refinement without overwhelming your resources.

The Value of a Service Wrap: Saving Time and Costs

One of the biggest misconceptions about Continuous Controls Monitoring is that implementing it requires a significant internal effort in terms of time, money, and resources. However, working with a vendor that provides a comprehensive service wrap can significantly alleviate these challenges. By leveraging expert onboarding support, organisations can bypass the steep learning curve and get up and running faster than they would with an in-house approach.

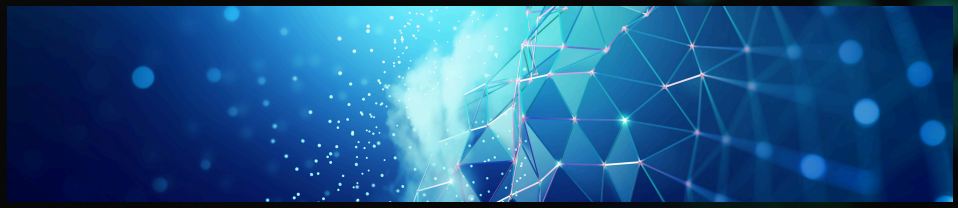
Vendors offer tailored guidance, pre-configured integrations, and ongoing support to ensure that CCM aligns seamlessly with business objectives without burdening internal teams.

A service wrap eliminates the need to allocate extensive internal resources to deployment and maintenance, freeing up valuable time for security teams to focus on strategic initiatives.

The result?

- Faster time to value,
- Reduced operational overheads,
- Lower total cost of ownership over time.

Ultimately, the right vendor partnership transforms CCM implementation from a complex endeavour into a streamlined process that delivers immediate and ongoing benefits.



The ROI of Quick Implementation

Organisations that embrace CCM often find that its implementation pays off faster than expected. By automating compliance checks and improving control visibility, CCM reduces audit preparation time, identifies vulnerabilities earlier, and streamlines reporting processes. The time and effort saved far outweigh the initial investment.

For example, consider an organisation grappling with manual compliance checks across multiple frameworks like ISO 27001 and NIST CSF. Transitioning to CCM might initially seem complex, but within weeks, they're saving hundreds of hours on compliance tasks and gaining real-time insights into their risk posture.

Each compliance team member spends 70–90% of their workweek on repetitive tasks like control testing, evidence gathering, and audit prep.

This is an annual Commitment: 1,500–2,000+ hours per person.

Average person works a 37.6 hr week: 2000/37.5 = 53 weeks which means they are spending more weeks than in a year to complete this.

Overcoming the Myth

To dispel the myth of complexity and time intensity, organisations should:

Evaluate Vendors Carefully

Choose a CCM solution tailored to your needs, with proven ease of implementation and robust support.

Leverage Existing Tools

Modern CCM platforms excel at working with what you already have, eliminating the need for costly overhauls. The platform connects to your entire ecosystem.

Embrace Automation

The beauty of CCM is in its ability to automate repetitive tasks. Trust the technology to lighten the load for your team.

Celebrate Milestones

Track and celebrate the efficiency gains from your CCM deployment to keep stakeholders engaged and supportive.

The Bottom Line

CCM need not be the formidable challenge it is often portrayed as. With the right tools, expert support, and a strategic approach, organisations can seamlessly implement CCM, unlocking powerful capabilities that enhance security, ensure compliance, and strengthen operational resilience.

\\ One Added Extra

CCM is Only for One Industry

Continuous Controls Monitoring isn't just for financial services or highly regulated industries.

It's essential for every organisation, regardless of size or sector. The threat landscape is constantly evolving, with cyberattacks becoming more sophisticated and indiscriminate.

Ransomware continues to rise, targeting businesses of all types, from healthcare to manufacturing, while regulatory scrutiny is tightening across industries, demanding stronger security and compliance measures.

At the same time, accountability is increasing, with executives and boards expected to prove that risks are being actively managed. Without real-time visibility into security controls, organisations risk blind spots that could lead to costly breaches, fines, and reputational damage.

CCM provides the proactive monitoring needed to stay ahead of threats, meet compliance obligations, and demonstrate resilience in an era where cybersecurity is a business-critical issue.

\\ Note to reader

We have not made this a myth by itself because whilst we feel this is important to note, we don't think it's a primary myth

Contact Us

www.quodorbis.com

contact@quodorbis.com

+44 (0)203 9622206

Quod-Orbis