QUOD ORBIS

CCM & GRC

Beyond Compliance: How Unified GRC and CCM Drive Real-Time Risk Management

Contents

From Reactive to Proactive: Smarter Risk Management with Unified GRC & CCM 03

GRC vs. CCM: Clearing Up the Confusion 04

The Value of Integrating CCM with GRC 10

What are the Business Outcomes of a GRC & CCM Integration? 15

The Future of GRC & CCM 19

OPERATIONAL RESILIENCE

From Reactive to Proactive: Smarter Risk Management with Unified GRC & CCM

Think CCM is just another GRC module? Think again.

GRC platforms have been the go-to for governance, risk, and compliance — helping organisations track status, report, and adjust. But there's a catch: they rely on static, manually collected data. That means decisions are only as good as the last update.

CCM changes the game. It connects directly to your ecosystem, pulling real-time data to give you a live, accurate view of your security, risk, and compliance posture. No delays. No blind spots. Just continuous assurance.

CCM isn't GRC — but when the two work together, GRC stops being a passive dashboard and becomes an active, always-on risk management engine.

Stop reacting. Start knowing

CCM transforms GRC from a static dashboard into a live, always-on risk management engine.

\\ GRC vs. CCM
Clearing Up the Confusion

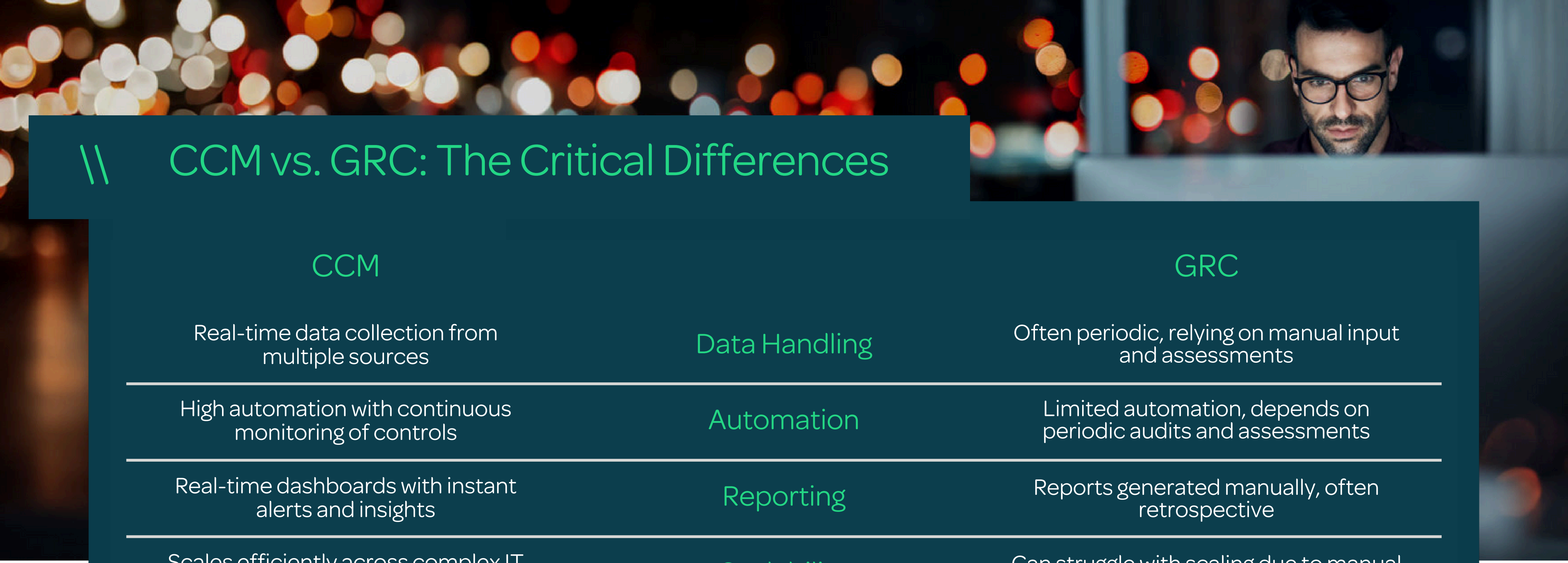
Many organisations assume that Continuous Controls Monitoring is just another GRC module, but this couldn't be further from the truth.

The confusion comes from their shared goal — helping businesses manage risk and compliance. However, while GRC platforms provide a structured framework for governance, risk, and compliance, they rely on manually collected, point-in-time data.

> CCM isn't a GRC add-on—it's the engine that keeps risk under control in real time.

In contrast, CCM operates in real-time, continuously pulling data from across the organisation's ecosystem to provide instant visibility and assurance. A direct comparison of GRC and CCM across key areas like data handling, automation, reporting, and scalability highlights their fundamental differences.

The overlap lies in their ability to support compliance efforts, but the key distinction is this: GRC helps organisations document and respond to risk, whereas CCM actively monitors and prevents issues before they escalate. When used together, they create a powerful, proactive risk management approach.



\\ CCM vs. GRC: The Critical Differences

CCM		GRC
Real-time data collection from multiple sources	Data Handling	Often periodic, relying on manual input and assessments
High automation with continuous monitoring of controls	Automation	Limited automation, depends on periodic audits and assessments
Real-time dashboards with instant alerts and insights	Reporting	Reports generated manually, often retrospective
Scales efficiently across complex IT landscapes	Scalability	Can struggle with scaling due to manual processes
Goes beyond compliance by actively reducing risk exposure	Compliance	Compliance-driven, focused on frameworks and policies
Dynamic risk detection with proactive mitigation	Risk Management	Risk assessment based on predefined intervals
Seamless integration with IT, security, and business systems	Integration	Often siloed, requiring manual reconciliation of data sources
Immediate response to deviations and threats	Response Time	Delayed due to assessment cycles
Cost-effective by reducing manual effort and audit fatigue	Cost Efficiency	High long-term costs due to manual labor and audits

\\ Why do organisations confuse GRC & CCM?

It’s true to state that CCM and GRC have overlapping goals in managing risk, ensuring compliance, and maintaining security.

However, while they share some similarities, they serve different purposes.

Here’s why the confusion happens:

1. GRC and CCM Both Aim to Reduce Risk and Ensure Compliance

GRC

GRC establishes policies, frameworks, and governance models to manage risks and compliance obligations.

CCM

CCM actively monitors whether these policies and controls are functioning as expected.

Since both help organisations stay compliant and manage risks, they’re often seen as interchangeable, but GRC is more about the “what” and “why,” whereas CCM is about the “how” and “now.”

\\ 2. Both Rely on Controls, but at Different Speeds

GRC

GRC defines and documents what controls should exist.

CCM

CCM continuously monitors and validates whether those controls are working in real-time.

Since GRC includes control management, people assume that means real-time monitoring too – but it doesn't. Traditional GRC tools rely on periodic assessments, whereas CCM offers continuous oversight.

3. GRC Tools Are Evolving to Include Monitoring Features

GRC

Some GRC platforms now offer some automation, such as risk dashboards and audit trails.

CCM

CCM automates the entire process providing a live asset repository and monitoring continuously in real-time.

This makes it seem like GRC tools are doing CCM's job, but these features are usually not truly continuous – they still rely on scheduled reports and periodic checks.

4. Audit and Compliance Cycles Create a False Sense of Security

GRC

GRC tools help with annual audits, regulatory filings, and risk assessments.

CCM

CCM provides real-time assurance that controls are working every day — not just before an audit.

Because organisations use GRC for compliance, they often assume it's enough for security and risk management. But compliance is just a snapshot in time – without CCM, businesses may be blind to ongoing security gaps.

\\ 5. Organisations Think CCM Is Just an Add-On to GRC

GRC

Many assume CCM is a “nice to have” feature within GRC rather than a separate discipline.

CCM

CCM isn’t just about compliance — it’s about ensuring that controls are always effective, reducing the risk of security failures and compliance breaches before they happen.

While GRC and CCM complement each other, they are not the same. GRC is the strategy; CCM is the execution.

Without CCM, GRC becomes reactive focused on documenting compliance rather than actively ensuring security. Organisations that rely only on GRC are often caught off guard by security failures between audit cycles – which is exactly what CCM helps prevent.

\\ The Value of Integrating CCM with GRC

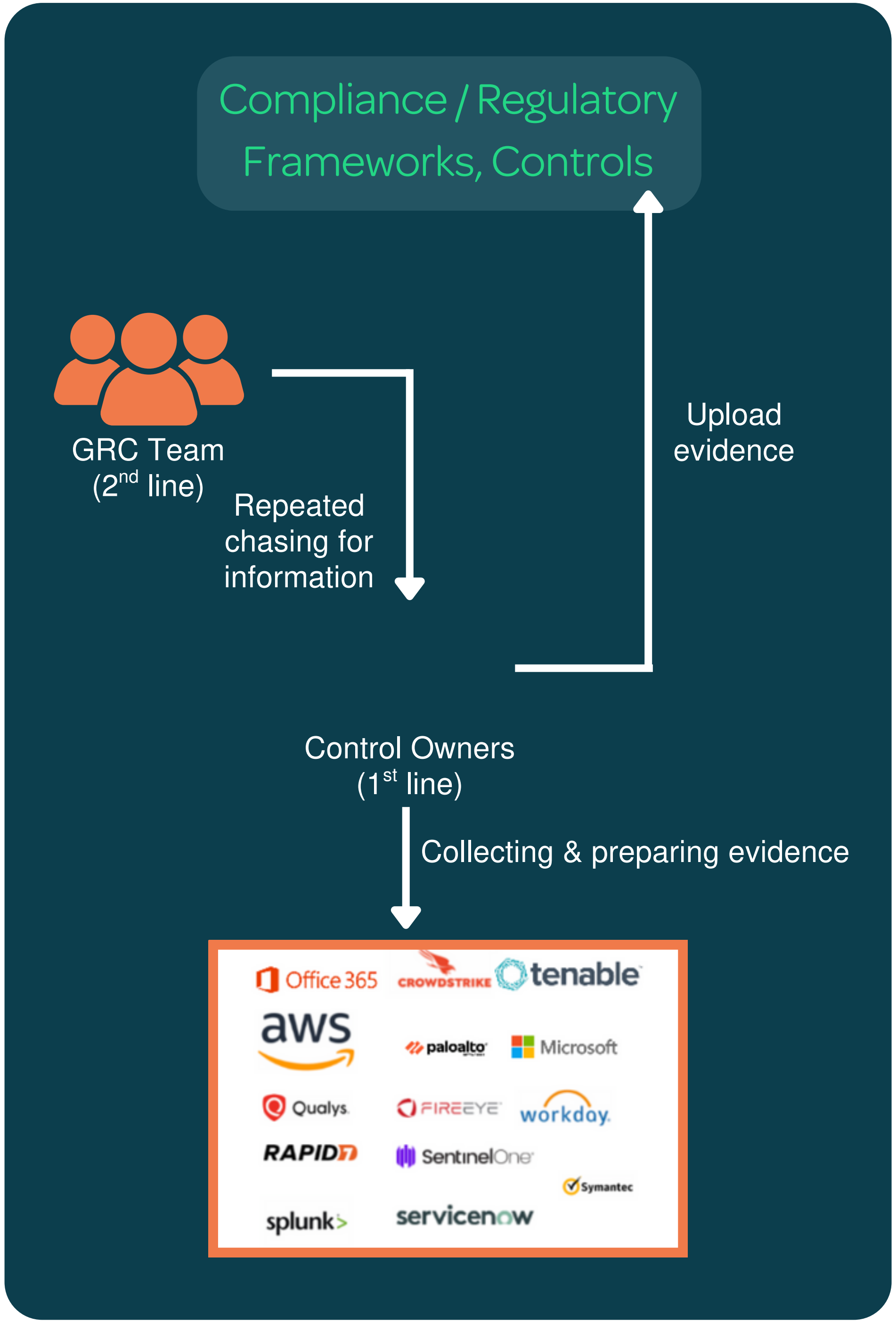
Standalone GRC products rely on point-in-time data uploads, which can be time-consuming and outdated.

The process was labour-intensive, manual, and perpetually outdated. Teams found it unrewarding and a significant drain on resources. In reality, GRC professionals lack the time to focus on critical risk reduction because they are consumed with chasing evidence and verifying its validity.

This raises a fundamental concern — how can GRC teams truly trust the integrity of the evidence they review? Without a reliable system, there's always the risk that control owners may manipulate data to present a more favourable picture.

> Integrating GRC with CCM solves this, allowing teams to focus on addressing risks. Unifying offers seamless integration, delivering valuable insights effortlessly.

How GRC Used to Operate



Compliance / Regulatory Frameworks, Controls

GRC Team (2nd line)

Repeated chasing for information

Upload evidence

Control Owners (1st line)

Collecting & preparing evidence

\\ Unified CCM & GRC: Powering Smarter Risk Management

With CCM, GRC is no longer just a compliance exercise—it becomes a proactive, security-enhancing function.

CCM transforms GRC from a check-the-box process to a security-first strategy:

- Prevents security gaps instead of just documenting them.
- Provides real-time assurance instead of periodic checks.
- Reduces audit fatigue with automated evidence collection.
- Aligns cyber security, IT risk, and compliance in one framework.

\\ CCM + GRC: Where Continuous Assurance Meets Governance

Fully Automated and Real-Time Insights

Leverage CCM for seamless integration and complete operational oversight.

Unified connectivity and visibility: Connect to every technology for a fully visible, streamlined ecosystem.

Simplified, real-time compliance: Centralise control requirements and monitor cyber metrics live, eliminating manual attestations.

Automation for accuracy: Replace manual processes to reduce errors and inefficiencies.

Resource optimisation: Free up teams to focus on mitigating risks, not chasing data.

Accelerated Efficiency & Assurance

Unlock faster compliance and improved assurance with near real-time data accuracy.

Effortless compliance: Automate evidence collection and optimise workflows to save time and reduce costs.

Real-time accuracy: Depend on trustworthy data for reporting and decision-making.

Maximised impact: Free your team from admin tasks to focus on strengthening internal controls.

\\ CCM + GRC: Where Continuous Assurance Meets Governance

Constant Compliance Status - Tailored Reporting

Effective compliance management combines data-driven reporting, real-time dashboards, actionable insights, and transparency to support proactive risk management and regulatory adaptability.

Quantitative compliance and risk: Use data-driven reporting to track progress and measure compliance readiness.

Tailored dashboards: Visualise real-time performance against regulatory benchmarks.

Actionable insights: Gain live metrics on risk levels, control gaps, and compliance status for swift, proactive decision-making.

Effective Risk Management

Effective risk management begins with enhanced visibility, providing organisations with a clearer understanding of their risk landscape.

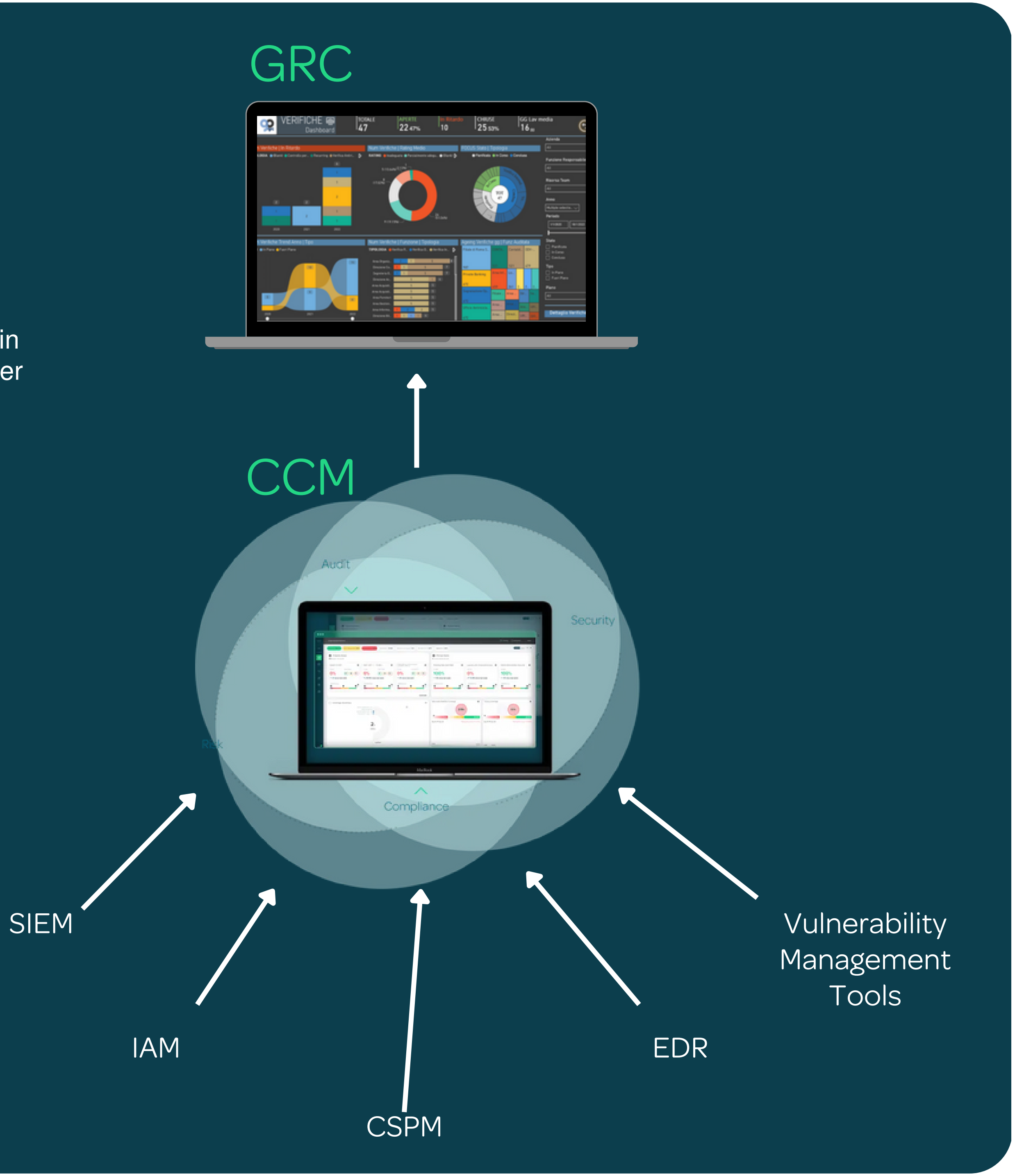
Enhanced transparency: Simplify risk assessments with accessible, analysable data.

Proactive risk management: Anticipate and mitigate issues to prioritise critical areas effectively.

Strengthened resilience: Support better decision-making for a streamlined, resource-focused approach.

How the CCM & GRC Intergration Works

CCM plugs into your GRC system and does the heavy lifting for you—automatically collecting evidence that usually takes hours to gather. You can let it run quietly in the background or check real-time dashboards whenever you like. For teams struggling with manual evidence collection, it's a huge time saver that quickly pays for itself.



ONBOARDING

\\ What are the Business Outcomes of a GRC & CCM Integration?

Real-Time Risk Visibility

Make faster, proactive decisions.
Gain live insights into control status and surface risks before they escalate.

Quantifiable Risk & Compliance Metrics

From guesswork to data-driven.
Turn subjective assessments into measurable KPIs and KRIs to report with confidence.

Automated Evidence Collection

Streamline audits and free up teams.
Auto-collect evidence and map it to frameworks—reducing manual effort and audit fatigue.

Reduced Operational Costs

Less firefighting, more foresight.
Eliminate redundant checks and expensive, last-minute compliance sprints.

Scalable Compliance

Stay ahead of changing regulations.

Adapt quickly to new frameworks like DORA, ISO 27001, and NIST without rework.

Stronger Security Posture

Prove your controls work continuously.

Catch control failures and security gaps in real-time, not during the next audit.

Increased Stakeholder Confidence

Win trust through transparency.

Show continuous assurance to customers, regulators, and your board.

Cyber Risk Quantification (CRQ) Foundation

Link cyber risk to business impact.

Use validated control data to model financial risk and make better strategic decisions.

CONFIGURATION

\\ How it supports the 3 Lines of Defence

First Line of Defence

Business & Operational Owners

- Real-time visibility
- Automated evidence
- Proactive alerts

SECURITY

AUDIT

Second Line of Defence

Risk & Compliance Functions

- Continuous Assurance
- Enhanced risk monitoring
- Framework alignment

COMPLIANCE

RISK

Third Line of Defence

Internal Audit

- Continuous audit readiness
- Focused audits
- Evidence-based assurance

\\ Implementing CCM Alongside Your GRC Platform

1. Align technical controls with your risk register and compliance obligations. Most GRC platforms include frameworks like ISO 27001, NIST, and DORA.

Identify key controls: Prioritise those tied to critical risks or regulatory needs.
Tag controls: Include metadata such as owner, frequency, system, risk area, and framework.

2. Connect to data Sources

CCM relies on real-time or scheduled data feeds from systems like SIEM, IAM, cloud, and endpoint tools.
Use APIs or log ingestion to capture control data (e.g., MFA in AD, firewall rules, S3 configs).
The goal: automate evidence collection, not manual attestation.

3. Set Monitoring Logic

Define what a healthy control looks like (e.g., “MFA enabled for all privileged users”).
Configure logic to continuously assess compliance against these criteria.
Set thresholds and exceptions—minor deviations don’t always mean failure

4. Push Insights Back Into the GRC Platform

Feed CCM results into the GRC dashboard as control health indicators.
Flag failing controls to trigger risk treatments, compliance alerts, or escalations.
Use insights to update risk scores, compliance status, and policies.

5. Enable Real-Time Assurance and Audit Readiness

GRC now proves controls exist and function effectively.
Use real-time dashboards to show compliance by regulation.
Replace static spreadsheets and sample audits with continuous evidence.

\\ The Future of GRC & CCM

Evolving Regulatory Landscapes & the Rising Demand for Continuous Monitoring

As regulations like DORA, NIS2, and SEC cybersecurity rules become more granular and real-time in nature, the expectations around how organisations monitor and report controls are shifting. Traditional point-in-time audits and attestations can no longer keep up.

Regulators don’t just want to know if you have controls—they want proof that they are working, continuously.

CCM answers this call, delivering live control performance data that ensures organisations are:

- Always audit-ready
- Proactively identifying issues
- Mapping control health directly to compliance requirements

How AI and Machine Learning Enhance CCM

The next evolution of CCM is not just automation, it's intelligence. AI and ML technologies are enabling platforms to:

- Detect anomalies and control drift automatically
- Predict control failures before they happen
- Prioritise remediation based on business risk and control criticality
- Learn from historical control data to optimise compliance efforts

This transforms monitoring from a reactive checklist to a proactive defence strategy.

Predictions: The Next Generation of GRC-CCM Integration

The future of GRC and CCM is a real-time, risk-aware nervous system for the business. Here's what we expect:

- Tighter, bidirectional integration: GRC platforms won't just collect data—they'll adapt policies and risk ratings based on real-time CCM insights.
- Framework-agnostic control libraries: Controls will be automatically mapped to multiple frameworks (e.g., ISO, DORA, NIST) via AI.
- Self-healing controls: Integration with orchestration tools will allow some systems to automatically correct control failures.
- Board-level dashboards: Live assurance will become part of executive-level reporting, not just compliance silos.

The endgame? A unified GRC-CCM ecosystem where policy, risk, control, and assurance all speak the same language—automated, continuous, and contextual.

QUOD
ORBIS

GLOBAL INFOSEC AWARDS WINNER
CYBER DEFENSE MAGAZINE
2025

Winner
Market Leader in Continuous Controls Monitoring!

Contact Us

www.quodorbis.com

contact@quodorbis.com

+44(0)203 9622206

Quod-Orbis