



WHY CCM SHOULD BE A BUDGET PRIORITY FOR 2025



www.quodorbis.com

THE CONSTANT CYBER RISKS



Ransomware Evolution

Ransomware exploits like RaaS and "double extortion" increasingly target critical infrastructure.



AI-Powered Threats

Cybercriminals use AI for deepfakes, personalised phishing, and automated vulnerability exploits.



IoT Security Risks

The rise of IoT devices expands attack surfaces, with many lacking strong security, making them easy targets.



Sophisticated Social Engineering

Attackers use refined techniques like phishing to exploit human vulnerabilities.

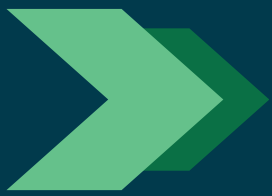


Supply Chain & Third-Party Risks

Cyberattacks target weak supply chains and third-party systems, causing disruptions and data breaches.



REGULATORY PRESSURES



Upcoming Compliance Deadlines

Financial institutions face challenges meeting DORA and the UK's Operational Resilience Act by January and PCI DSS V4.0 by March 2025.



Continuous Monitoring Required by Regulations

Regulations like NIST, ISO, DORA, CMMC 2.0, and SEC now require continuous cyber ecosystem monitoring.





www.quodorbis.com

FINANCIAL IMPACT



Non-compliance can be costly, with an average global cost of \$14.82 million, including fines, legal fees, downtime, and reputational damage. A breach alone averages \$4.93 million.



Proactive Compliance Investment: The average annual investment in proactive security and monitoring.



The average annual investment in proactive security and monitoring for medium to large organisations is \$3–\$5 million, about one-third of potential penalties and recovery costs. (Source: IBM Newsroom)



QO's research found C-suite leaders spend an average of 60 hours annually on regulatory compliance, not including team time, with CCM helping reduce operational costs.



OPERATIONAL EFFICIENCY



Streamlines Workflows

Automates manual tasks, reducing IT and security team workloads.



Boosts Collaboration

Provides simultaneous access to shared insights for IT and security teams.



Enhances Incident Response

Enables faster decision-making and immediate threat mitigation during incidents.



Improves Resilience

Bridges team gaps, reduces response times, and strengthens overall organisational security posture.



STRATEGIC ADVANTAGE



Builds Trust & Confidence

Demonstrates a commitment to protecting sensitive data, fostering trust with clients and stakeholders.



Enhances Reputation

Positions the organisation as a security-conscious industry leader, distinguishing it from competitors.



Drives Business Growth

Strengthens relationships with security-minded clients, supporting long-term partnerships.

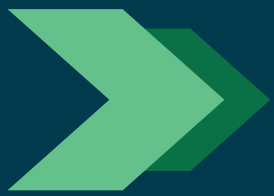


Supports Market Positioning

Proactively managing risks and threats reinforces the organisation's standing in the marketplace.

DEBUNKING CCM BUDGETING MYTHS

"We can't afford it"



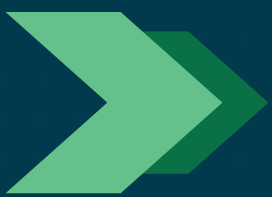
Investing in Continuous Controls Monitoring (CCM) prevents costly data breaches, fines, and reputational damage, making it more cost-effective than dealing with the fallout of cyber incidents.

"We're already compliant"



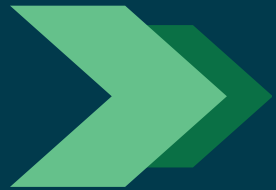
Compliance doesn't ensure resilience. CCM addresses evolving cyber threats beyond basic regulatory requirements.

"It's too complex to implement"



Modern CCM tools are scalable, user-friendly, and integrate easily with existing systems, making them practical for any organisation.

BUILDING A BUSINESS CASE FOR CCM



KPIs & KRIs

Highlight reduced response times, real-time risk detection, fewer audit findings, and cost savings through enhanced efficiency and compliance.



Budget-Friendly Approach

Start small with critical controls, leveraging scalable CCM solutions to grow as needed, ensuring visible improvements before expanding.



Enhances Risk Management

CCM enhances risk management, drives efficiency, and delivers long-term cost savings.

Plan now to integrate CCM into your 2025 budget—it's not just a tool but a vital shield against evolving threats.