AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

# Continuous Controls Monitoring:

## The End of Spreadsheet Compliance

# 01 Executive Summary

Compliance has long been treated as a calendar event rather than a continuous business function. For decades, organizations prepared for audits with sprint-like bursts of spreadsheet updates, screenshot captures, and manual evidence assembly, then exhaled in relief once the auditor left the building and carried on until the next cycle began. That model is now genuinely broken, not merely inconvenient, and the data from across the industry confirms it with uncomfortable clarity.

Research conducted by Swimlane in March 2025, drawing on 500 IT and cybersecurity decision-makers across the United States and United Kingdom, found that only 29 percent of organizations report their compliance programs consistently meet internal and external standards.[1] A companion study by RegScale found that while 94 percent of information security leaders believe Continuous Controls Monitoring (CCM) would improve both their compliance posture and their security, only 28 percent were actually monitoring controls continuously in real time.[2] That gap between belief and execution is precisely where risk lives.

The regulatory landscape has simultaneously transformed beyond what manual approaches can reasonably absorb. The Digital Operational Resilience Act (DORA), enforced across EU financial institutions since January 2025, demands continuous ICT risk management as an ongoing legal obligation.[9] PCI DSS 4.0 and 4.0.1, with heightened logging, authentication, and monitoring requirements fully enforced from March 2025, require demonstrable evidence of control effectiveness far beyond quarterly screenshots.[10] The U.S. Securities and Exchange Commission now mandates disclosure of material cybersecurity incidents within four business days.11 These frameworks share a single expectation: that organizations can demonstrate their controls are working, not merely that they exist on paper.

This whitepaper examines how Continuous Controls Monitoring closes that gap. It explores why spreadsheets became the default compliance tool, why that default now constitutes a governance liability, and how GRACE, an intelligent Orchestrated Compliance Platform, transforms compliance from a reactive scramble into a continuous, data-driven function embedded in the organization's daily operations.[22] Through industry data, regulatory context, real-world risk scenarios, and a structured implementation framework, this paper offers security leaders, GRC professionals, and board members a clear view of what modern compliance assurance looks like and what it takes to get there.

# 02 The Spreadsheet Compliance Era: How We Got Here

To understand why Continuous Controls Monitoring matters, it helps to understand why spreadsheets took hold in the first place. When organizations began formalizing their governance, risk, and compliance programs in the early 2000s, spreadsheets were the most accessible structured-data tool available to most compliance teams. They required no procurement approval, no vendor relationship, and no integration with existing systems. A compliance analyst could build a risk register in a morning and share it with leadership before lunch. For a small organization managing a handful of controls against a single framework, this approach worked reasonably well.

The problem is that the environment those early GRC spreadsheets were designed for no longer exists. The number of active regulatory frameworks that organizations must navigate has multiplied dramatically. A midsize financial services firm today might simultaneously maintain compliance with DORA, PCI DSS, GDPR, ISO 27001, SOC 2, and one or more national-level cybersecurity requirements depending on the jurisdictions in which it operates. Each framework carries its own control vocabulary, evidence requirements, testing cadences, and reporting obligations. Mapping those requirements manually across a collection of spreadsheets is not a scalable process; it is an ongoing source of duplication, inconsistency, and hidden risk.

Dartmouth College research found that 94 percent of operational spreadsheets contain errors, and that nearly 2 percent of all formula cells produce incorrect results. KPMG and Ernst and Young have reached similar conclusions, observing that virtually every complex spreadsheet contains material mistakes that go undetected until they cause a consequence.[4] When the spreadsheets in question are feeding compliance assessments, risk registers, and audit evidence packages, those mistakes do not stay inside the file. They become governance failures with financial, legal, and reputational dimensions.

The 2024 UK court ruling in the Thyssenkrupp tax dispute illustrated this dynamic with unusual clarity. An unauthorized modification to a formula in a tax-return spreadsheet resulted in an incorrect calculation that the court ruled invalid, producing an additional GBP 10 million tax liability.[4] The organization argued it was a simple error. The court confirmed that in a compliance context, a simple error in a spreadsheet is not a mitigating factor; it is the failure itself. The lesson extends beyond tax to every domain where spreadsheet-based evidence underpins a regulatory obligation.

## The Structural Failures Hiding in Plain Sight

The deficiencies of spreadsheet-based compliance are not merely anecdotal. They are structural, meaning they arise not from poor practice but from the inherent characteristics of spreadsheets as a tool for managing dynamic, multi-stakeholder, multi-framework compliance programs. The following failure modes recur predictably across every sector and organization size.

- **Version control collapses under scale.** When multiple team members contribute evidence or update control statuses across separate files, there is no authoritative record of which version is current, who changed what, or whether a given snapshot reflects the state of controls at the moment the auditor needs to see. Auditors who encounter inconsistent evidence across documents frequently raise findings not because controls are absent but because traceability cannot be established.[6]

- **Audit trails are either absent or reconstructed after the fact.** Most compliance spreadsheets do not natively log who made a change, when they made it, or what the previous value was. When investigators, auditors, or regulators request a verifiable chain of custody for control evidence, organizations relying on spreadsheets either cannot produce one or must reconstruct it from memory and email threads which is itself a red flag.[5]

- **Manual data entry introduces systematic inaccuracy.** When control owners update a spreadsheet based on their own observation of system state, they are making a judgment call about what they saw, when they saw it, and whether it matches the control requirement. Two people looking at the same system configuration can document it differently. Neither entry is independently verifiable without returning to the source system.

- **Siloed data prevents organizational visibility.** Research by Onspring found that when GRC data is fragmented across departmental spreadsheets, risk teams and compliance teams frequently reach conflicting conclusions about the same vendor, system, or control a conflict that auditors discover and treat as a program integrity issue.[5]

- **Real-time awareness is impossible by design.** A spreadsheet reflects the state of controls at the moment it was last updated. In an environment where system configurations change, access rights are modified, and new endpoints join the network daily, a compliance posture captured in a spreadsheet begins drifting from reality the moment it is saved. By the next audit cycle, the gap between documented and actual control state can be substantial.[6]

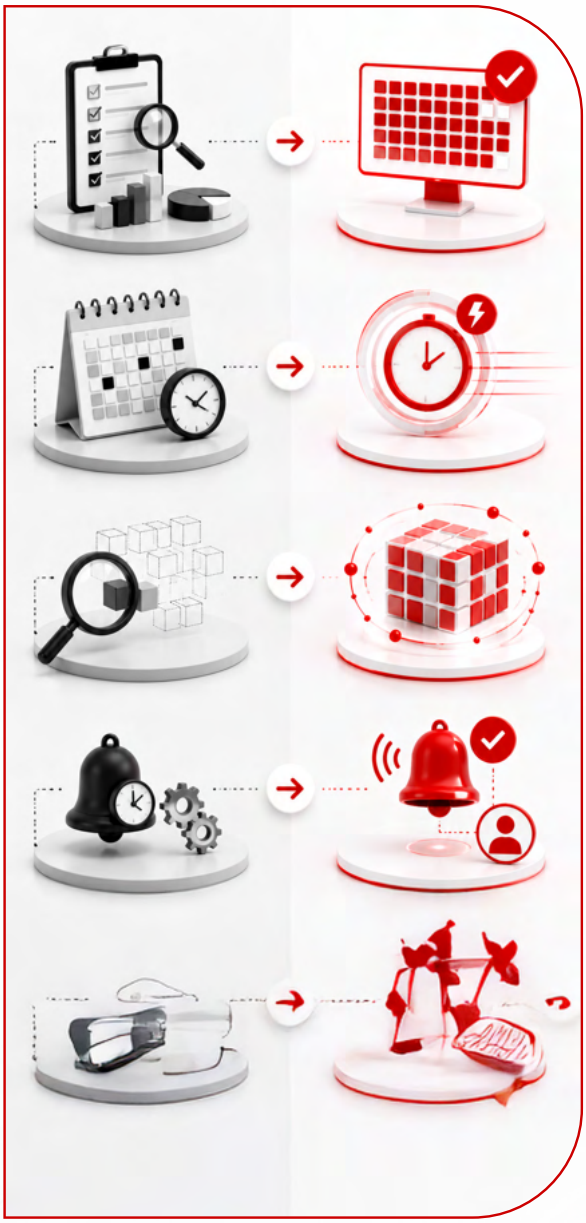
# 03 What Continuous Controls Monitoring Actually Is

Continuous Controls Monitoring is the automated, real-time process of validating whether an organization's internal controls are operating as intended, documenting that validation with machine-generated evidence, and surfacing failures or deviations immediately so they can be addressed before they become audit findings, regulatory violations, or security incidents.[7] The definition sounds straightforward, but the operational implications are significant.

CCM is not a dashboard bolted onto an existing compliance program. It is a fundamental change in the operating model for compliance, shifting the function from a periodic, human-intensive exercise to a continuous, automated process that runs as part of the organization's standard technology operations. In practical terms, CCM platforms ingest telemetry from the organization's existing technology stack including SIEM tools, endpoint detection systems, cloud security posture management platforms, identity governance tools, vulnerability scanners, and configuration management databases and use that telemetry to continuously test whether controls meet the defined requirements of the applicable frameworks.[8]

When a CCM system detects that a control is drifting from its required state, it generates an alert, creates a record of the deviation, and routes it to the appropriate owner for remediation. The evidence of that detection, the deviation record, the alert, and the remediation action are all captured automatically and stored in a way that is immediately retrievable, attributable to a specific system state at a specific moment in time, and defensible under audit scrutiny. This means that when an external auditor arrives and asks for evidence that patch management controls were operating effectively over the past twelve months, the organization does not need to assemble a package of screenshots from memory, it can produce a continuous, timestamped record of control performance across the entire period.

## How CCM Differs from Traditional Monitoring



Research from MetricStream and Sprinto identifies four defining characteristics that distinguish CCM from traditional compliance monitoring approaches.[7] First, where traditional monitoring relies on manual sampling of a subset of controls on a periodic schedule, CCM applies automated testing to the full population of controls on a continuous basis. Second, where traditional monitoring detects failures days or weeks after they occur, CCM surfaces deviations in real time. Third, where traditional monitoring covers a limited sample, CCM provides comprehensive oversight of the entire control environment. Fourth, where traditional monitoring produces delayed alerts that require manual triage, CCM generates immediate, context-rich notifications routed directly to the responsible owner. These differences are not incremental improvements, they represent a qualitative change in what compliance programs can see, how quickly they can respond, and how credibly they can demonstrate control effectiveness to regulators, auditors, customers, and boards.

## The Regulatory Imperative Behind CCM

The shift toward CCM is not purely a matter of operational preference. It is being driven, with increasing urgency, by regulatory frameworks that explicitly require continuous monitoring of controls rather than point-in-time demonstrations of compliance.

DORA, which has been fully enforceable since January 2025 across more than twenty categories of EU financial entities including banks, insurers, and asset managers, requires organizations to maintain continuous ICT risk management frameworks, conduct ongoing resilience testing, and demonstrate that their monitoring capabilities can detect and respond to incidents in real time. Supervisory reviews that began in 2026 carry penalty exposure of up to two percent of global annual turnover for non-compliant entities.[9]

PCI DSS 4.0, whose future-dated requirements became fully mandatory as of March 2025, substantially increases expectations for logging continuity, authentication controls, and the ability to reconstruct access events over time. The standard does not merely ask whether logging is enabled; it asks whether logs capture the right events, whether they are protected from tampering, and whether they can support a forensic reconstruction of what happened and when. Continuous, automated evidence collection is the only operationally viable path to meeting these requirements at scale.[10]

The SEC's cybersecurity disclosure rules require public companies to disclose material cybersecurity incidents on Form 8-K within four business days of determining that a material incident has occurred. An organization cannot meet a four-day disclosure window if it does not have continuous visibility into its security posture. The rule does not mandate CCM by name, but it creates conditions under which the absence of continuous monitoring becomes a direct liability.[11]

NIST's Cybersecurity Framework 2.0, released in February 2024 and increasingly referenced across sectors as a governance baseline, strengthens the emphasis on continuous monitoring and measurement as core components of an effective cybersecurity program. The framework explicitly distinguishes between organizations that identify and assess risks periodically and those that monitor and manage them continuously, treating the latter as the more mature posture.[12]

# 04 The Cost Of Not Acting: Quantifying Compliance Risk

Compliance professionals have long struggled to translate the risks of inadequate controls into language that moves decision-makers to act. The language of audit findings and regulatory citations rarely generates the same urgency as a revenue shortfall or a customer loss. What has changed in the past two years is the availability of data that quantifies compliance failure in business terms that boards and finance committees understand.

NAVEX Global and IBM's Cost of a Data Breach Report 2025 found that data breaches where non-compliance was a contributing factor cost organizations an average of USD 4.61 million, approximately four percent higher than the global average breach cost, with breaches involving regulatory non-compliance carrying an additional USD 174,000 in costs over and above direct breach-related expenses.[13]

Research by Hyperproof published in mid-2026 revealed that 50 percent of organizations managing risk in an ad hoc, manual fashion experienced a data breach in 2025. Among organizations using an integrated, automated approach to risk and compliance management, that figure dropped to 27 percent.[14] The relationship between operational maturity in GRC programs and security outcomes has become statistically visible and measurable, and organizations that invest in automation are experiencing materially better security results, not just more efficient compliance workflows.

Beyond breach costs, the financial impact of compliance failure manifests in regulatory fines, elevated cyber insurance premiums, and lost commercial opportunities. Forty-seven percent of organizations surveyed in 2025 reported that inadequate security assurance had delayed a sales cycle, and 38 percent had lost a deal outright because they could not produce the compliance evidence a customer or partner required.[15]

The same Swimlane research that found only 29 percent of organizations consistently meeting compliance standards also revealed that 96 percent of organizations find it challenging to keep up with the growing number of industry regulations.[1] Hyperproof's 2026 benchmark data showed that 76 percent of GRC professionals still spend 30 percent or more of their working hours on repetitive, manual administrative tasks.[14] That is not a compliance team functioning at its potential; it is a compliance team trapped in the mechanics of evidence gathering, unable to apply its judgment to the higher-value activities that actually reduce risk.

## The Audit-Season Fire Drill

Perhaps the most familiar cost of spreadsheet-based compliance is the audit-season fire drill: the weeks of compressed activity preceding a scheduled audit during which teams chase down evidence, reconcile conflicting versions of control documentation, reconstruct timelines from email threads, and prepare narrative explanations for gaps that should not exist in a well-managed program. This is not a sign of poor intent. It is the predictable output of a compliance model built around periodic events rather than continuous operations.

Organizations that have adopted CCM consistently report that audit preparation time drops dramatically once continuous evidence collection is in place. Hyperproof's case study data includes one organization that achieved a 75 percent reduction in audit preparation time and a 50 percent reduction in time spent on evidence collection after implementing an automated compliance platform.[14] RegScale's research found that 23 percent of organizations that have adopted GRC automation cut their time spent on compliance tasks by more than half.[3]

# 05 Continuous Controls Monitoring In Practice

Understanding what CCM is and why it matters is necessary but not sufficient. The more actionable question for organizations evaluating a transition from spreadsheet-based compliance is what CCM actually looks like in operation, how it integrates with existing technology investments, and what the realistic implementation path looks like.

## The Technical Architecture of CCM

A mature CCM implementation rests on four interconnected technical capabilities that work together to provide continuous, evidence-backed assurance across the organization's control environment.

The first capability is data ingestion and normalization. A CCM platform must connect to the organization's existing technology stack and pull structured telemetry from the systems where controls are actually operating. This includes SIEM platforms, cloud security posture management tools, identity governance systems, endpoint detection and response tools, vulnerability management scanners, and configuration management databases. The richness of CCM output is directly proportional to the breadth and fidelity of the data sources feeding the platform.[8]

The second capability is control mapping and framework crosswalk. A control that is tested once and mapped to multiple frameworks simultaneously is fundamentally more efficient than the same control tested separately for each framework it touches. Modern CCM platforms use AI-assisted semantic mapping to normalize controls across frameworks such as NIST CSF 2.0, ISO 27001, SOC 2, CMMC, DORA, and PCI DSS, ensuring that evidence collected for one compliance obligation is automatically attributed to overlapping requirements in other frameworks. Hyperproof's data indicates that a centralized common controls framework reduces manual administrative burden by up to 33 percent compared to siloed, framework-by-framework approaches.[14]

The third capability is automated testing and evidence generation. Rather than relying on a control owner to observe system state, document it in a spreadsheet, and submit a screenshot, a CCM platform runs automated tests against defined control requirements on a continuous or scheduled basis. The test results including timestamps, source data, pass/fail status, and contextual metadata are captured as machine-generated evidence that requires no manual assembly. This evidence is stored in a format that is immediately retrievable, attributable to a specific system state at a specific moment in time, and defensible under audit scrutiny.[7]

The fourth capability is exception alerting and workflow routing. When a control test fails or a control status drifts from its required state, the CCM platform generates an alert that is routed to the appropriate owner with context about what failed, what the expected state was, and what remediation is required. This transforms compliance from a retrospective function, discovering failures weeks after they occurred, into a prospective one that addresses deviations before they accumulate into audit findings or security incidents.[18]

## Multi-Framework Compliance and the Crosswalk Problem

One of the most consistent pain points reported by GRC practitioners managing mature compliance programs is the crosswalk problem: the labor-intensive process of manually mapping overlapping requirements across multiple frameworks, duplicating evidence collection efforts, and reconciling inconsistencies when two frameworks describe similar requirements using different language. A CISO managing simultaneous compliance with SOC 2, ISO 27001, DORA, and PCI DSS is not facing four independent compliance programs; they are managing a complex web of overlapping obligations where many controls satisfy requirements across multiple frameworks simultaneously, but only if the mapping has been done correctly and maintained as frameworks evolve.[19]

CCM platforms address this through centralized control libraries that maintain canonical mappings between frameworks. When a control is tested and evidence is generated, the platform attributes that evidence to every framework requirement the control satisfies, eliminating the need for parallel evidence collection. Cyber Sierra, recognized as a sample vendor in the Gartner Hype Cycle for Cyber-Risk Management in 2024, describes this capability as allowing teams to define controls once and have them mapped across all relevant frameworks automatically.[20]

## AI and Machine Learning in CCM


The integration of artificial intelligence into CCM platforms represents the next significant evolution in what continuous monitoring can deliver. Traditional rule-based monitoring systems apply fixed criteria to telemetry data and flag deviations when those criteria are met. This works well for known, well-defined control requirements but generates substantial false-positive noise in complex environments where normal operational variation can resemble a control failure to a rule without context.[17]

AI-powered CCM systems address this by learning from historical compliance data to distinguish genuine deviations from operational noise, reducing false positives and improving the signal quality of alerts that reach compliance and security teams. Beyond noise reduction, AI capabilities are increasingly being applied to predictive compliance monitoring, in which the system analyzes patterns in control performance data to forecast where failures are likely to occur before they actually do. RegScale's 2026 State of CCM Report found that 100 percent of AI adopters in their survey reported positive outcomes in their Cyber GRC programs, with 64 percent describing the benefits as significant or transformational.[2]

# 06 From Point-In-Time To Continuous: The Compliance Maturity Progression

Organizations do not typically move from manual spreadsheet compliance to fully automated CCM in a single step. The transition follows a recognizable progression that corresponds to increasing operational maturity in the GRC function, and understanding where an organization sits on that progression is a prerequisite for planning an effective path forward.

## Stage One: Ad Hoc Compliance

At this stage, compliance is managed reactively, primarily through periodic audit preparation exercises. Control documentation lives in spreadsheets and shared drives. Evidence collection is manual and episodic, occurring in concentrated bursts before scheduled assessments. Risk visibility is limited to what was documented in the most recent review cycle. Control failures go undetected between cycles. Most organizations at this stage are aware that their approach is insufficient but have not yet made the structural investment required to change it. Hyperproof's benchmark data found that organizations at this stage experienced a data breach rate of 50 percent in 2025.[14]

## Stage Two: Structured but Static

Organizations at this stage have formalized their compliance programs with defined control inventories, assigned control owners, and documented testing procedures. Compliance activity is more regular and better organized than at Stage One, but it remains fundamentally periodic and manual. The improvements at this stage are real but limited: structured compliance programs still miss failures that occur between assessment cycles, still generate evidence through manual observation rather than automated testing, and still struggle with the consistency and completeness problems inherent in human-mediated documentation at scale.[16]

## Stage Three: Integrated and Automated

At Stage Three, organizations have connected their compliance programs to their technology stacks through CCM platforms or GRC automation tools that pull live telemetry and generate continuous evidence. Control testing runs automatically. Exceptions alert immediately to the appropriate owners. Evidence packages are built continuously rather than assembled in audit sprints. Multi-framework mapping reduces duplication. Board and leadership reporting draws on real-time posture data rather than point-in-time snapshots. Apptega's 2026 State of Continuous Compliance Report found that 86 percent of security service providers are now interested in offering ongoing continuous compliance as a service, and 70 percent of their clients are actively requesting real-time compliance scoring and visibility.[16]

## Stage Four: Predictive and Intelligence-Driven

The most mature organizations are extending CCM beyond reactive detection of control failures to predictive identification of compliance risk before it materializes. At this stage, AI-powered analytics examine patterns in control performance data, environmental changes, and external threat intelligence to forecast where compliance gaps are likely to emerge and prompt preventive action. This stage represents the convergence of security and compliance into a unified, continuous assurance function that is genuinely embedded in operational workflows rather than layered on top of them.[17]

# 07 Real-World Risk Scenario: When Controls Drift Undetected

To illustrate the practical consequences of the gap between documented and actual control state, consider a scenario that compliance and security teams encounter with regularity in environments that rely on periodic, manual monitoring.

A financial services organization is preparing for its annual SOC 2 Type II audit, covering a twelve-month period that ended three weeks ago. The compliance team assembles evidence from the control spreadsheet maintained throughout the year, which reflects the state of controls at the time each entry was made. The spreadsheet shows that multi-factor authentication was enabled for all privileged access accounts throughout the review period.

During the audit, the external assessor pulls access logs directly from the organization's identity management system and discovers that for a period of six weeks, beginning five months ago, MFA enforcement was inadvertently disabled for a service account category during a system migration. The migration team corrected the issue before the next quarterly review, updated the relevant documentation in the spreadsheet to reflect the current state, and moved on. The spreadsheet never captured the six-week gap because no one was monitoring continuously.

The auditor's finding is not that MFA is absent now. It is that there is a documented period within the audit window during which the control was not operating as required, and the organization's compliance program did not detect it. The finding results in a qualified opinion on the SOC 2 report. Two enterprise customers, both of whom have contractual requirements for clean SOC 2 opinions from their service providers, initiate vendor review processes. The financial and reputational consequences of a gap that existed for six weeks, went undetected for months, and was never remediation-tracked are now unfolding at a scale entirely disproportionate to the original technical issue.[5]

In a CCM-enabled environment, this scenario does not play out this way. The MFA configuration change is detected by the CCM platform within hours of occurring because continuous monitoring of identity management system telemetry is part of the standard control testing regimen. An alert routes to the IT security owner, who investigates, discovers the misconfiguration, and opens a remediation ticket. The ticket is resolved within 48 hours. The entire sequence detection, alert, investigation, remediation is captured in the CCM evidence log. When the auditor reviews the same control, they see not a gap but a demonstration of exactly the control assurance process the framework requires: a deviation was detected quickly, attributed to a root cause, remediated, and documented. The same misconfiguration happened in both versions of this scenario. The difference in outcome is entirely a function of whether the organization could see it when it happened.

# 08 Grace: From Compliance Burden To Continuous Assurance

GRACE is designed for organizations that have outgrown spreadsheet-based compliance but are looking for a practical, intelligence-driven path to continuous assurance, GRACE operationalizes every principle discussed in this whitepaper through a unified, audit-ready interface.[22]

Where spreadsheets scatter evidence across dozens of files maintained by different stakeholders, GRACE consolidates the entire compliance lifecycle from control definition and framework mapping through continuous testing, exception management, evidence storage, and board-level reporting into a single, authoritative system of record. The platform is built on the conviction that audit readiness should not be a sprint; it should be a permanent state of the organization.


## Intelligent, Continuous Control Monitoring

GRACE connects to an organization's existing technology stack and continuously ingests security telemetry from SIEM platforms, identity management systems, endpoint detection tools, cloud security posture management solutions, and vulnerability scanners. Rather than relying on control owners to periodically document what they believe to be true about system state, GRACE validates control performance against defined requirements in real time, generating machine-produced evidence that is timestamped, attributed, and immediately auditor-ready.[22]

When a control deviation is detected, GRACE routes an alert to the responsible owner with full context about the failure, the affected system or process, the applicable framework requirement, and the remediation steps required. This means that by the time an external auditor asks for evidence, the organization is not assembling a package it is presenting a continuous record of control performance that the system has been building automatically throughout the audit period.

## Cross-Framework Mapping and Unified Evidence

One of the most significant sources of compliance inefficiency in organizations managing multiple frameworks simultaneously is the duplication of evidence collection effort. GRACE addresses this through a centralized controls library that maps each control to every framework requirement it satisfies across PCI DSS, SOC 2, ISO 27001, NIST CSF, CMMC, HIPAA, DORA, and other applicable standards. When a control is tested and evidence is generated, that evidence is automatically attributed to all relevant framework requirements, eliminating the parallel workstreams that currently consume compliance team capacity.[22]

This map-once-comply-many approach means that organizations adding a new regulatory framework to their compliance program do not need to build a parallel evidence collection process. They need only to map their existing controls to the new framework's requirements, and GRACE's continuous monitoring populates the evidence automatically.

## Risk Quantification and Board-Ready Reporting

GRACE goes beyond control monitoring to provide integrated risk quantification that connects control performance to financial exposure. When a control fails or degrades, GRACE does not merely surface the technical deviation it quantifies the risk impact in terms that boards and leadership committees can act on, connecting the technical finding to the business consequence and enabling informed prioritization of remediation investment.

Board-level dashboards in GRACE display real-time compliance posture across all applicable frameworks, current control effectiveness rates, exception trends, and audit readiness scores. These are not static reports assembled by the compliance team before a quarterly presentation; they are live views of the organization's compliance state that can be accessed at any moment by any authorized stakeholder, providing the kind of continuous visibility that modern regulatory expectations require.[22]

## Eliminating the Audit Sprint

The most immediate operational benefit organizations experience when deploying GRACE is the elimination of the audit-season fire drill. Because GRACE generates and organizes audit evidence continuously throughout the year, audit preparation becomes a matter of reviewing what the system has already documented rather than assembling evidence from scratch. External auditors work directly with GRACE's evidence repository, reducing the back-and-forth that extends audit timelines and consumes compliance team bandwidth.

GRACE is purpose-built for the reality that compliance is not a once-a-year activity, it is an ongoing operational discipline that protects the organization every day, not only in the weeks before an assessment. For organizations ready to move from the spreadsheet era to continuous assurance, GRACE provides the platform, the intelligence, and the operational framework to make that transition practical, measurable, and durable.

# 09 Implementing Continuous Controls Monitoring: A Practical Framework

Organizations that have successfully transitioned to CCM share a common observation: the technology is rarely the hardest part. The harder work involves defining the scope of monitoring, aligning stakeholders across IT, security, compliance, and leadership, establishing the data foundations that CCM relies on, and building the operational processes that convert CCM output into consistent action. The following framework reflects the implementation patterns that produce durable results.

## 01 Step One: Establish a Control Inventoryand Framework Map

CCM requires a clear, authoritative definition of what controls exist, what they are supposed to do, and which regulatory requirements they satisfy. Many organizations discover during this step that their control inventories are less complete than they assumed. Controls exist in different versions across different teams, framework mappings are inconsistent, and ownership is unclear for a meaningful fraction of the control population. Completing this foundational work before deploying CCM technology is essential because an automated monitoring platform cannot monitor controls that have not been defined. This step should produce a single, canonical controls library that maps each control to the frameworks it satisfies, assigns a clear owner, defines the technical test that will be used to validate the control's operation, and specifies the evidence that test will produce.

## 02 Step Two: Assess Data Source Availability and Quality

CCM derives its value from the quality and completeness of the telemetry it ingests. Before deploying a CCM platform, organizations should audit the data sources that will feed it. Are the relevant systems producing structured, machine-readable logs? Are those logs centralized in a way that the CCM platform can access? Are there gaps in coverage, classes of systems or applications that do not produce the kind of telemetry required to validate the controls they host? These questions surface the gaps that would otherwise limit CCM effectiveness, and addressing them before deployment significantly improves the quality of monitoring output from day one.

## 03 Step Three: Prioritize Controls by Risk and Regulatory Weight

Not all controls carry equal weight in terms of risk impact or regulatory consequence. Organizations with large control populations should prioritize implementation of continuous monitoring for the controls that, if they failed undetected, would produce the most severe consequences. These are typically controls that satisfy high-impact regulatory requirements, controls that protect the most sensitive data categories, and controls that have historically been sources of audit findings. Starting with high-priority controls allows the organization to demonstrate early value from CCM investments and build operational confidence in the monitoring process before extending coverage across the full control environment.[21]

## 04 Step Four: Deploy and Integrate

With a defined control inventory, clear data source availability, and a prioritized implementation scope, the organization is ready to deploy CCM tooling and build the integrations that connect the platform to the relevant data sources. This phase should be approached iteratively, beginning with the highest-priority controls and the data sources that support them, validating that the platform is producing accurate, complete evidence before expanding coverage. The integration work at this stage often uncovers data quality issues, access permission gaps, or system configuration problems that need to be resolved before monitoring can operate effectively, and these discoveries are valuable, representing control gaps that the previous manual approach was not surfacing.

## 05 Step Five: Build Operational Processes Around CCM Output

CCM technology generates value only if the alerts and evidence it produces are connected to operational processes that act on them. Organizations should define explicit workflows for how exceptions are triaged, who is responsible for investigating alerts within what timeframe, how remediation is tracked, and how evidence is organized for audit retrieval. Without these processes, CCM output accumulates without generating the control improvements and compliance assurance it is designed to produce. This step also includes calibrating alert thresholds to reduce false positives, early in a CCM deployment, alert volumes can be high as the system learns the baseline behavior of the monitored environment.[18]

# 10 Board-Level Metrics For A CCM-Enabled Compliance Program

One of the most significant benefits of CCM for senior leadership and boards is the transformation of compliance reporting from backward-looking narrative summaries to real-time, data-driven metrics that reflect the current state of the organization's control environment. The following KPIs represent the kind of metrics that CCM enables and that boards should expect from a mature compliance program.[21]

**Control Coverage Rate:** Measures the percentage of in-scope controls subject to automated, continuous testing. An organization targeting high compliance maturity should be working toward 90 percent or greater automated coverage of its critical controls, with a clear plan for the remainder.

**Mean Time to Remediate (MTTR):** Measures the average elapsed time between a control failure being detected and the failure being resolved. MTTR is a measure of operational response capability rather than monitoring capability, but it is directly enabled by the early detection that CCM provides.

**Framework Coverage Integrity:** Measures the degree to which the organization's control testing provides coverage across all requirements of its applicable frameworks without gaps or orphaned requirements. This metric surfaces the framework crosswalk problems that manual approaches tend to hide until an

**Mean Time to Detect (MTTD):** Measures the average elapsed time between a control failure occurring and the organization becoming aware of it. In a manual compliance environment, MTTD can be weeks or months. A well-configured CCM environment should produce MTTD measured in hours for high-priority controls.

**Audit Readiness Score:** Measures the completeness and recency of evidence available to support an audit at any given moment. A CCM-enabled compliance program should be able to produce audit-ready evidence on demand rather than requiring weeks of preparation.

**Framework Coverage Integrity:** Measures the degree to which the organization's control testing provides coverage across all requirements of its applicable frameworks without gaps or orphaned requirements. This metric surfaces the framework crosswalk problems that manual approaches tend to hide until an auditor discovers them.

# 11 The Path Forward: Compliance As A Continuous Capability

The question facing most organizations today is not whether they need to move beyond spreadsheet compliance. The regulatory environment, the security threat landscape, and the organizational cost of manual evidence management have collectively made that question redundant. The genuine question is how to make the transition in a way that is operationally realistic, financially defensible, and durable enough to keep pace with the continuing evolution of both the regulatory landscape and the technology environment.

The answer begins with recognizing that CCM is not a technology replacement project. It is an operating model transformation. The spreadsheet did not fail because it was the wrong software; it failed because the operating model it supported, periodic, manual, event-driven compliance, is no longer adequate for the scale and dynamism of modern regulatory requirements. Replacing the spreadsheet with a CCM platform while retaining the periodic, manual operating model produces better reporting but not better compliance. The transformation requires both the technology and the process and governance changes that make the technology meaningful.

Organizations that have made this transformation successfully defined their control environment clearly before automating it. They built cross-functional ownership of the CCM program, involving IT, security, compliance, legal, and leadership stakeholders rather than treating it as a compliance team project. They invested in data quality across the systems feeding their CCM platform, recognizing that the reliability of vmonitoring output depends on the reliability of the telemetry beneath it. And they communicated CCM outcomes to boards and leadership in business terms, connecting control performance to financial risk, regulatory exposure, and customer confidence rather than presenting technical metrics in isolation.[3]

The GRC automation market, valued at USD 48.7 billion in 2023, is projected to reach USD 179.5 billion by 2032, reflecting the scale of organizational investment flowing toward the tools and platforms that make continuous compliance operationally real. Organizations with automated, integrated GRC programs breach at half the rate of those managing compliance ad hoc, spend dramatically less time on audit preparation, and are better positioned to respond to the rapid regulatory changes that show no sign of slowing.[14]

The spreadsheet served its purpose in an era when compliance was simpler, slower, and less consequential than it is today. That era is long gone. The organizations that recognize this now and act on it with the deliberateness the transformation requires will enter the next cycle of regulatory enforcement with the assurance that comes from genuinely knowing whether their controls are working. Those that do not will continue to find out at the worst possible moment in the middle of an audit, or after a breach, that the compliance posture they thought they had was not the one they actually had.

# 12 References

All sources cited in this whitepaper are listed below. Reference numbers correspond to superscript citations used throughout the document

**1. Swimlane:** GRC Chaos: The High Price of Audits and Non-Compliance (2025)
https://swimlane.com/news/grc-audit-research/

**2. RegScale:** 2026 State of Continuous Controls Monitoring Report
https://regscale.com/resource-center/state-of-continuous-controls-monitoring-report/

**3. RegScale:** Why Spreadsheets Still Dominate GRC (2026)
https://regscale.com/blog/grc-spreadsheets-problem-symptom/

**4. Symbiant:** Spreadsheet Horror Stories and Real Compliance Disasters (2026)
https://www.symbiant.co.uk/spreadsheet-horror-stories-real-compliance-disasters-and-how-modern-grc-software-prevents-them/

**5. Onspring:** The Hidden Compliance Risks of Siloed GRC Data (2025)
https://onspring.com/resources/blog/hidden-compliance-risks-siloed-grc-data/

**6. Granite GRC:** Avoiding Spreadsheet Drift (2026)
https://granitegrc.com/archive/avoiding-spreadsheet-drift-signals-its-time-for-a-dedicated-grc-platform/

**7. Sprinto:** Continuous Control Monitoring Guide (2026)
https://sprinto.com/blog/continuous-control-monitoring/

**8. Databee:** Continuous Controls Monitoring Explained
https://www.databee.ai/cybersecurity-data-education-hub/what-is-continuous-controls-monitoring-ccm

**9. European Banking Authority:** DORA Regulatory Technical Standards
https://www.eba.europa.eu/regulation-and-policy/dora

**10. PCI Security Standards Council:** PCI DSS 4.0 Documentation
https://www.pcisecuritystandards.org

**11. U.S. Securities and Exchange Commission:** Cybersecurity Disclosure Guidance
https://www.sec.gov/corpfin/secg-cybersecurity

**12. NIST:** Cybersecurity Framework 2.0
https://www.nist.gov/cyberframework

**13. NAVEX Global / IBM:** Cost of a Data Breach Report (2025)
https://www.ibm.com/reports/data-breach.

**14. Hyperproof:** Mid-2026 IT Risk and Compliance Benchmark Report
https://hyperproof.io/resource/mid-year-review-of-it-risk-and-compliance/

**15. Symbiant:** GRC in 2025 — A Year of Pressure, Proof, and Progress
https://www.symbiant.co.uk/grc-in-2025-a-year-of-pressure-proof-and-progress/

**16. Apptega:** 2026 State of Continuous Compliance Report
https://www.apptega.com/blog/continuous-monitoring

**17. Cyber Sierra:** The Future of CCM with AI Agents (2025)
https://cybersierra.co/blog/ai-continuous-control-monitoring/

**18. DigitalXForce:** Why CCM Is a Must-Have in 2025
https://digitalxforce.com/why-continuous-controls-monitoring-ccm-is-a-must-have-in-2025/

**19. Cyber Sierra:** 10 Continuous Compliance Tools for Multi-Framework Security (2026) https://cybersierra.co/blog/continuous-compliance-tools-2026/

**20. Gartner:** Hype Cycle for Cyber-Risk Management (2024)
https://www.gartner.com/en/documents/hype-cycle-for-cyber-risk-management

**21. CyberSaint:** Continuous Control Monitoring (CyberStrong Platform)
https://www.cybersaint.io/cybersecurity/continuous-control-monitoring

**22. Ampcus Cyber:** ComplyX GRACE — GRC Tool for Continuous Compliance
https://www.ampcuscyber.com/complyx/grace/

AMPCUS CYBER

INTELLIGENT CYBERSECURITY DELIVERED

**Ready to take the next step?**
**Connect with our cybersecurity experts today.**


+1 (703) 310-6237

letsconnect@ampcuscyber.com

www.ampcuscyber.com