November 2025

CoreStream GRC for ERM

Enabling ERM Amid Uncertainty in Business

SOLUTION***PERSPECTIVE***

Governance, Risk Management & Compliance Insight

Table of Contents

TALK TO US . . .

We look forward to hearing from you and learning what you think about GRC 20/20 research. GRC 20/20 is eager to answer inquiries from organizations looking to improve GRC related processes and utilize technology to drive GRC efficiency, effectiveness, and agility.

CoreStream GRC for ERM

Enabling ERM Amid Uncertainty in Business

Managing Uncertainty to Objectives in a World of Chaos

Modern business runs on objectives. Organizations exist to reliably achieve outcomes for customers, employees, investors, and society. Yet every objective lives in a world of uncertainty shaped by markets, geopolitics, regulation, technology, people, and partners. Enterprise Risk Management (ERM) is how the organization understands and navigates this uncertainty: connecting strategy with execution so that value is protected and created.

As expectations rise from boards, regulators, investors, and the public, leaders are accountable not only for what happens within the four walls of the enterprise but also for the ripple effects of decisions across operations, third parties, digital infrastructure, and the external risk environment. Cyber incidents, conduct failures, model risk, ESG controversies, geopolitical shocks, and operational disruptions all become board-level concerns because they threaten objectives and trust. The need to move beyond periodic, control-centric "risk lists" to a living, objective-centric ERM lifecycle has never been more urgent.

Governance is where ERM starts. Risk management is too often reactive, cataloguing threats and running assessments. Governance sets direction and context, it clarifies purpose, defines objectives and risk appetite, assigns accountability, and embeds integrity into decisions. Without governance, ERM fragments into siloed activities: busy, but not strategic.

Governing the ERM Lifecycle

ERM is not an annual workshop; it is a continuous, closed-loop lifecycle that connects strategy, performance, risk, and resilience. A mature ERM capability flows through several phases, each reinforcing the other.

1. **Strategy & Context.** The lifecycle begins with strategy and context, where the organization sets direction by establishing its business model, strategic objectives, and the internal and external contexts for uncertainty. This is where risk appetite and tolerance are defined, linked to measurable outcomes and stakeholder expectations. Objectives must have clear performance indicators — KPIs and KRIs — and be tied to the underlying architecture of the business: its value streams, processes, assets, services, locations, and third parties. Risk does not exist in abstraction; it attaches to the moving parts of the organization and the objectives they support.

2. **Risk Identification & Assessment.** From there, the organization moves into risk identification and assessment, continuously surfacing threats, opportunities, and scenarios across strategic, financial, operational, technology, compliance, and reputational domains. In this phase, qualitative and quantitative methods combine with enterprise risk intelligence (ERI) to provide situational awareness. ERI draws on risk intelligence and signals to separate noise from what truly matters. Near-misses and weak signals are captured from across the enterprise, giving the organization early warning before risks become realities.

3. **Risk Response, Controls, and Initiatives.** The next phase, risk response, controls, and initiatives, translates analysis into action. Here the organization decides whether to accept, avoid, reduce, or transfer each risk. Effective governance demands clarity: actions must have defined owners, budgets, timelines, and an understanding of their impact on objectives. Controls must be designed and tested for effectiveness, and where possible, automated to provide continuous evidence. Strategic initiatives that reduce exposure or enhance capability are tracked with milestones and dependencies, creating transparency and accountability. This phase is also where resilience is built through scenario playbooks, business continuity plans, and defined impact tolerances for critical services.

4. **Risk Monitoring, Indicators, and Reporting.** With response mechanisms in place, ERM moves into risk monitoring, indicators, and reporting: the heartbeat of an effective program. This involves continuous measurement of performance and risk through KRIs, KPIs, and early-warning indicators, supported by external intelligence feeds. The organization must maintain a living dashboard that adjusts forecasts as conditions change, triggering alerts when tolerances are breached. Contextual analytics replace static heatmaps, allowing leaders to understand cause-and-effect relationships and see how risk trajectories influence performance and strategy.

5. **Risk Incidents, Issues, and Decisions.** When reality deviates from plan, the next phase, incidents, issues, and decisions, ensures the organization learns and adapts. Events, near-misses, and losses are captured and triaged with clear root-cause analysis and ownership for corrective actions. Decision-making processes are documented and evidenced to strengthen accountability. Lessons learned feed back into appetite, scenarios, and control design, closing the learning loop and ensuring continuous improvement.

6. **Risk Assurance, Testing, and Challenge.** Assurance, testing, and challenge follow, providing confidence that the governance, risk, and control environment is designed and operating effectively. Risk, compliance, and audit functions coordinate under a "three lines" model, ensuring independent oversight without duplication. Assurance programs are risk-based, testing is continuous where feasible, and results are tied directly to risk appetite and board-level reporting. This disciplined challenge process strengthens — not duplicates — management's own insight.

7. **Risk Review and Refresh.** Finally, the review and refresh phase closes the loop. ERM must evolve alongside strategy, business change, and the external environment. Frameworks, appetites, methodologies, and models are revisited regularly to ensure relevance. A mature organization learns from its own performance and from the world around it, updating its assumptions and tolerances to remain agile and resilient. This should be handled as a continuous process and not a periodic.

Why Siloed Risk Approaches Fail

Despite this logical lifecycle, many organizations still run risk functions as parallel, disconnected efforts. Finance focuses on stress testing, operations on incidents, cybersecurity on vulnerabilities, compliance on obligations, and audit on assurance. Each does its job well, but no one sees the whole. Seemingly minor risks in one area can combine with others to form material exposures that surprise leadership. Spreadsheets, emails, and static reports only compound this fragmentation, failing to capture the interconnected relationships that define the enterprise. Annual assessments are outdated almost as soon as they are completed, leaving organizations reactive instead of prepared.

The Case for an ERM Platform

True ERM begins with modelling the business, connecting strategy to value streams, processes, assets, and obligations. Risk attaches to these moving parts and their objectives. Performance and objective management come next, as risk cannot be understood outside the context of the goals it may impact. Objectives define the frame for uncertainty, and by linking them with measurable indicators, scenarios, and initiatives, organizations can see risk-adjusted performance in real time. Strategic risk and resilience form the decision layer, where organizations not only protect strategy but shape it through informed choices. ERM becomes objective-centric when risks are owned where work happens, and performance indicators and risk indicators move in tandem. Near-misses and weak signals are captured and analyzed, creating an enterprise nervous system that senses and adapts. Finally, operational risk and resilience provide the rails on which strategy rides, ensuring that critical services, processes, and systems can continue through disruption.

Delivering this level of intelligence and governance at scale is impossible with manual processes and disconnected risk management tools. Organizations require an integrated platform that unifies enterprise risk and resilience management around the structure of the business itself. An integrated ERM platform becomes the single source of truth: linking objectives, risks, controls, indicators, issues, and decisions to the processes, services, assets, and third parties that comprise the enterprise.

Automation replaces manual effort, while external intelligence and internal telemetry combine to provide continuous situational awareness. Decision intelligence capabilities enable scenario simulations, stress testing, and risk-adjusted forecasting, empowering leadership to make informed choices with confidence. Collaboration across the first, second, and third lines ensures accountability, while defensible audit trails support regulatory assurance and board oversight. The outcome is an organization that operates not just with greater efficiency, but with enhanced effectiveness, agility, and resilience.

At the heart of this the ERM platform functions as the organization's central nervous system sensing, thinking, and orchestrating response across diverse sources of uncertainty. The ERM platform harmonizes governance, risk, and resilience within the context of objectives and risk appetite. Supported by modern technology, automation, and analytics, this transforms from reactive oversight to proactive orchestration of risk management, ensuring the enterprise can navigate uncertainty with confidence and foresight.

The Bottom Line: ERM does not work in silos. To thrive amid interconnected complexity, organizations must embrace an objective-centric ERM lifecycle, from strategy and appetite through assessment, response, monitoring, incidents, assurance, and review. This requires integrated strategies, processes, and technologies that deliver continuous visibility, accountability, and alignment with business objectives. The organizations that succeed will be those that treat risk not as a liability to avoid, but as uncertainty to be governed. By enabling an ERM platform to orchestrate governance, risk management, and resilience into the fabric of decision-making, the organization will gain the confidence to take the right risks, build trust, and enable sustainable performance in an unpredictable world.

CoreStream GRC for ERM

Enabling ERM Amid Uncertainty in Business

CoreStream GRC is a solution that GRC 20/20 has researched, evaluated, and reviewed with organizations using it to modernize enterprise risk management (ERM) in distributed, dynamic, and disrupted business environments across industries and geographies. It is an agile, next-generation GRC platform that supports a wide range of enterprise, operational, and compliance risk processes. CoreStream GRC delivers a no-code solution with a modern information architecture, intuitive interface, and high configurability, making it a powerful business management platform designed to embed governance, risk management, and compliance into everyday decision-making.

CoreStream GRC provides organizations with out-of-the-box ERM capabilities — risks, controls, actions, incidents, and indicators — alongside the ability to tailor and expand the solution to reflect unique frameworks, methodologies, and business models. GRC 20/20's evaluation finds that CoreStream GRC delivers a flexible, intuitive, and engaging ERM experience that transforms risk from a static exercise into a dynamic, intelligence-driven discipline. It enables organizations to collect, organize, link, report, and analyze enterprise risk data with greater control, collaboration, and accountability across the three lines of defense.

Before CoreStream GRC. Prior to adopting CoreStream GRC, organizations typically relied on fragmented, manual risk management approaches driven by spreadsheets, documents, emails, and disconnected systems. These methods were time-consuming, error-prone, and difficult to scale—especially when aggregating and reporting risk data across global operations or multiple business units. Some organizations had experimented with larger, traditional GRC platforms but found them overly complex, costly, and rigid, with customizations breaking during upgrades. Clients emphasized

frustration with inefficiency, outdated information, and lack of visibility prior to adopting CoreStream GRC.

GRC 20/20's evaluation, research, and interactions with CoreStream GRC clients have determined the following:

- **Before CoreStream GRC.** Clients typically arrive from fragmented, manual ERM ecosystems encumbered with spreadsheets, documents, emails, and legacy tools that are hard to scale and harder to trust. Annual risk registers compiled for the year-end report left leaders with stale insight and limited ability to drill into cause, trend, or ownership. Some had trialed heavyweight suites only to encounter cost, rigidity, and brittle customizations that complicated upgrades. The shared experience was inefficiency, missed signals, and a lack of consolidated visibility.

- **Why CoreStream GRC.** Organizations choose CoreStream GRC for its agility, configurability, and ease of use, providing a single, integrated environment for managing the full enterprise risk lifecycle. Clients consistently value the platform's flexibility to align with their frameworks, its adaptability to regulatory and governance requirements, and its ability to support both enterprise-wide and project-level risk programs in parallel. The decision is often reinforced by CoreStream GRC's lower total cost of ownership compared to larger competitors and by its strong reputation for responsiveness, partnership, and customer focus. Clients describe CoreStream GRC as an energetic, collaborative vendor that listens, adapts, and continually evolves its roadmap in line with user needs.

- **How CoreStream GRC is used.** CoreStream GRC is deployed as the foundation for enterprise and operational risk management. It enables risk identification, assessment, and treatment to be seamlessly linked to controls, incidents, and performance indicators. Leadership teams use CoreStream GRC dashboards to access real-time global, regional, and business unit views of top risks and mitigation actions. In some organizations, CoreStream GRC has replaced legacy databases and tools, unifying enterprise and project risk in a single platform. The no-code environment allows rapid adaptation, from implementing new workflows for declarations and maturity assessments to integrating risk data into external analytics and quantification engines.

- **Where CoreStream GRC has excelled.** Clients consistently highlight CoreStream GRC's flexibility, user-friendliness, and speed of delivery. Its ability to integrate enterprise and project risk, automate reporting, and improve visibility has helped organizations shift risk from a compliance-driven process to a living management discipline. Users praise CoreStream GRC's configurable dashboards that facilitate board-level discussions and provide a consolidated, real-time risk view across global operations. The platform's simplicity promotes broad engagement, driving consistency in how risks are identified, assessed, and acted upon. Clients particularly emphasize CoreStream GRC's strong implementation support, responsive service culture, and willingness to collaborate on new features. While acknowledging its smaller scale compared to major enterprise vendors, clients view its focused expertise, innovation roadmap, and practical delivery as key advantages in meeting complex ERM requirements.

CoreStream GRC enables organizations to embed risk thinking into the fabric of daily operations—delivering efficiency, effectiveness, agility, and resilience. It modernizes risk management from static spreadsheets to a living system of record and intelligence, empowering leadership with a clear, data-driven understanding of risk across the enterprise.

CoreStream GRC ERM Client Experiences

Organizations across industries and regions are leveraging CoreStream GRC to strengthen their ERM and broader GRC programs, achieving improvements in efficiency, automation, and adaptability to complex regulatory requirements. GRC 20/20 has engaged with CoreStream GRC clients globally, and in this evaluation conducted four specific client reference calls that found:

- **Global travel food services organization (~40 countries, ~50,000 employees).** ERM moved from an annual, report-driven exercise into a living discipline used daily and recognized at CEO level. "Group CEO has called this out to the company several times, risk management has gone from tick box exercise to something they live and breathe." CoreStream GRC provides a real-time consolidated view that can instantly pivot to region or country, enabling leadership to see top risks and mitigations on demand. Simplicity and usability drove engagement across leadership groups and created greater consistency in how risks are identified and understood. Reporting continues to be refined; ambitions include broader delegated action tracking and more automated board-pack output. Support has been highly responsive and pragmatic.

- **Global energy company (~100,000 employees).** Global enterprise and project/delivery risk now run in one platform, replacing multiple legacy tools and consolidating roughly a hundred disparate data stores. Costs dropped materially versus prior systems, while usage expanded to thousands of users. Governance checkpoints, exposure windows, and trend "flight paths" made the program more forward-looking, improving alignment of capital and contingency to risk timelines. APIs feed external quantification tools; CoreStream GRC serves as the risk data spine. Requests include faster delivery of certain advanced visualizations and simpler grid editing for high-volume users.

- **UK financial mutual (specialty re/insurance covering £2.2 trillion in assets).** After challenges with a previous tool, the organization adopted CoreStream GRC for risks, controls, KRIs, events, maturity, and actions, plus a declarations module. Adoption leapt from ~40% to ~95% within one cycle. Same-day capture-to-committee reporting is now routine; internal audit operates directly in the platform; and confidence in data quality has increased. Efficiency improved as "admin drag" disappeared, freeing time for analysis. Desired roadmap items include greater end-user self-service for dashboards and analytics, building on a strong standard set. They compare the level of support to their old tool stating "People and culture at CoreStream GRC are really really good, the team are keen to help, we've all become good friends. Never had that kind of engagement with a software solution!"

- **Big-Four perspective (implementation partner and internal user).** Praises a practitioner-built design, "Lego-block" configurability, and the right price point for organizations digitizing ERM or stepping up from first-generation tools. Executive and board meetings benefit from live, drillable dashboards that materially improve discussion quality versus static decks. Recommendations for roadmap emphasis include deeper self-service configuration, BI-grade visualization polish and integration.

Across these deployments we see a consistent pattern: efficiency through consolidation and automation; effectiveness via clearer appetite alignment and action follow-through; resilience as forward-looking indicators and exposure windows bring early warning; and agility as teams spend less time on pack preparation and more time on horizon scanning and decision support. CoreStream GRC's culture — enthusiastic, collaborative, and responsive — amplifies these results by meeting organizations where they are and moving them forward at pace.

CoreStream GRC is well-suited to organizations seeking a practical, configurable ERM core with strong UX and fast time-to-value. It modernizes risk from spreadsheets and static reports into a connected, objective-centric discipline embedded in daily management. While clients ask for more self-service analytics and automation — appropriate for a platform on a strong upward trajectory — the prevailing narrative is clear: CoreStream GRC provides a flexible ERM spine that improves visibility, sharpens decisions, and strengthens the enterprise's ability to take the right risks with confidence.

CoreStream GRC Enables an Integrated ERM Lifecycle

GRC 20/20 finds that CoreStream GRC is a solution that grows and evolves with the organization, adapting as its business strategy, risk profile, and regulatory environment change. It can be deployed rapidly to address specific enterprise risk management needs — such as risk registers, controls, and assurance — or scaled as the backbone of a fully integrated ERM architecture. Many clients have leveraged the platform's agility to extend beyond traditional risk use cases, building tailored applications for internal audit, controls management, incident response, and even strategic governance workflows.

Specific enablers CoreStream GRC provides in the ERM context include:

- **From Burden to Enabler.** CoreStream GRC transforms the perception of ERM technology from a burdensome reporting tool into an enabler of performance and resilience. Rather than imposing rigid frameworks, it delivers a configurable architecture that mirrors each organization's risk methodology, culture, and terminology. This allows risk and assurance teams to act as strategic partners to leadership, enabling risk-informed decisions, not just compliance reporting. Its no-code, modular design supports rapid deployment (in weeks, not months), the ability to start small and scale over time, customization to match risk taxonomies, and seamless integration with business systems. Real-time dashboards, scenario tracking, and automated reporting give executives immediate visibility into emerging risks and strategic exposures.

- **ERM Orchestration at Work.** Where many platforms digitize isolated risk registers, CoreStream GRC orchestrates risk across the enterprise—connecting strategy, objectives, performance, and uncertainty. It unifies risk identification, assessment, response, monitoring, and assurance into one continuous, auditable ecosystem. Organizations use CoreStream to automate risk workflows, align with regulatory and governance frameworks (ISO 31000, COSO ERM, UK Corporate Governance Code), and integrate enterprise, operational, and project risks into a single system of record. This orchestration delivers not just risk data, but strategic insight and accountability across all three lines of defense.

- **A Lego-Brick Platform.** CoreStream GRC's modular architecture enables organizations to build their ERM program like Lego bricks, starting with core risk solution and expanding as maturity grows. Clients can pilot specific capabilities, such as risk registers or control assurance, then extend into internal audit, material controls, or performance management without disruption. Unlike monolithic systems that require extensive configuration and lock-in, CoreStream GRC allows continuous evolution: adding new features, integrating additional risk domains, or linking to external analytics tools, all without reengineering the environment.

- **No-Code Flexibility.** CoreStream GRC is distinguished by genuine no-code configurability. Risk managers — not developers — can adjust fields, workflows, and notifications, adapt terminology to local frameworks, and create dashboards for executives, risk owners, or board committees. This flexibility accelerates adoption, reduces dependency on IT, and empowers the second line to maintain agility as the business or risk taxonomy evolves. In fast-changing environments—whether responding to new regulations, emerging ESG risks, or geopolitical shifts—this adaptability ensures that the risk framework remains current and operationally relevant.

- **Integration Without the Pain.** Clients emphasize CoreStream GRC's ability to integrate cleanly with existing systems across the enterprise — ERP, HR, finance, and data visualization tools like Power BI. Through standardized APIs and configurable data flows, CoreStream GRC aggregates risk information from disparate sources into a unified view. This integration allows KRIs, incidents, controls, and actions to be continuously updated and analyzed in real time. Whether linking to external risk intelligence feeds or internal reporting systems, organizations achieve a single source of truth for enterprise risk and assurance.

- **Built for Complexity, Adopted for Simplicity.** CoreStream GRC meets the needs of both global enterprises with complex, multi-entity structures and mid-sized organizations establishing or maturing their risk programs. It supports layered governance models, localized workflows, and jurisdictional compliance while remaining intuitive for end users. From multinational energy companies to specialized financial institutions, CoreStream GRC has proven capable of managing risk complexity without overwhelming the business, bringing transparency, consistency, and speed to decision-making across the enterprise.

- **Client-Led, Expert-Driven.** CoreStream GRC is more than a software provider; it is a collaborative partner. Clients consistently highlight its practitioner-led design ethos, rapid proof-of-concept deployments, and responsiveness to evolving needs. The CoreStream GRC team — comprising former risk and assurance professionals — brings real-world understanding to configuration and delivery. Subscription pricing begins only after implementation, reinforcing client trust. As one client noted, "We didn't just buy software—we gained a partner who understands both our technical needs and our culture."

How CoreStream GRC Addresses the ERM Lifecycle

As detailed previously, many organizations still treat risk management as a periodic, form-filling exercise. Producing registers and reports once or twice a year rather than embedding ERM into the rhythm of business performance and decision-making. Once risks are logged, ownership and accountability often fragment across departments, leaving the enterprise blind to how uncertainty evolves. CoreStream GRC addresses this challenge by orchestrating oversight across the ERM lifecycle — from strategy and context through to continuous review and refresh — ensuring governance, visibility, and accountability at every stage.

CoreStream GRC enables:

- **Strategy & Context.** CoreStream GRC anchors risk management in the business context. The platform links objectives, KPIs, and KRIs to risks, controls, and assurance activities within a unified business architecture. Organizations can model their value streams, services, and assets to understand precisely where risk attaches to operations. Risk appetite and tolerance levels are defined directly in the system and mapped to measurable performance thresholds, allowing leadership to visualize whether risks are within acceptable bounds or require escalation. By connecting risk to strategic outcomes, CoreStream GRC turns ERM from a reactive reporting function into a proactive enabler of strategy execution.

- **Risk Identification & Assessment.** CoreStream GRC simplifies the identification and assessment of risk across the enterprise. Users can capture threats, opportunities, causes, and consequences using customizable templates aligned to the organization's risk taxonomy. Qualitative and quantitative assessments are supported — from simple scoring and heatmaps, to bow-tie risk assessments, to integration of methodologies like Monte Carlo simulation via API integration. The platform can incorporate feeds from enterprise risk intelligence (ERI) like Black Kite, Xapien and Signal AI providers or internal business systems to surface early warning indicators and weak signals. Risks can be categorized by business unit, geography, or objective, ensuring that what emerges locally can be aggregated globally for executive insight.

- **Risk Response, Controls, and Initiatives.** CoreStream GRC translates risk analysis into tangible action. The platform supports all treatment strategies — accept, avoid, mitigate, or transfer — with structured workflows that assign clear ownership, budget, and deadlines. Controls are linked directly to risks, with the ability to evidence design and operational effectiveness through

automated reminders and testing logs. Strategic initiatives designed to reduce exposure or enhance resilience are tracked like projects, complete with milestones, dependencies, and impact measures. Scenario planning, playbooks, and resilience metrics (such as impact tolerances for critical services) are all configurable, giving leadership a clear "flight path" to achieving the desired risk posture.

- **Risk Monitoring, Indicators, and Reporting.** CoreStream GRC provides the heartbeat of ongoing risk management through dynamic dashboards and automated monitoring. KRIs and KPIs are continuously tracked against appetite, with threshold alerts and trend visualization to show risk trajectory over time. Data from external feeds — market movements, regulatory updates, geo-political risk, or cyber intelligence — can be integrated to enrich monitoring and provide context. Leadership dashboards adjust in real time as indicators change, enabling proactive responses rather than retrospective reports. CoreStream GRC replaces static heatmaps with contextual analytics that link risk movement to business performance, ensuring that decision-makers see both the signal and the story behind it.

- **Risk Incidents, Issues, and Decisions.** When events or deviations occur, CoreStream GRC ensures that issues are captured, triaged, and resolved systematically. Incidents, near-misses, and audit findings can be recorded directly against related risks or controls. The system drives structured workflows for investigation, escalation, and remediation; with notifications, evidence capture, and root-cause analysis built in. Lessons learned are automatically linked back to affected objectives, controls, and scenarios, reinforcing a continuous learning loop. Decision logs and approvals provide a defensible record for governance reviews and board reporting, ensuring transparency and accountability in how management responds to uncertainty.

- **Risk Assurance, Testing, and Challenge.** CoreStream GRC supports an integrated assurance model across the three lines. Risk management, compliance, and internal audit can coordinate testing programs within the same environment, sharing data but maintaining independence. Control testing is supported through scheduled reviews, sampling, and workflow evidence collection. Results are automatically mapped to risk appetite and tolerance thresholds, providing management and boards with a clear view of where assurance confirms strength — or where it signals weakness. The system's traceability from risk through control, test, and finding builds a strong foundation for external assurance and regulatory defensibility.

- **Risk Review and Refresh.** Finally, CoreStream GRC closes the loop by institutionalizing continuous review and refresh. Frameworks, appetites, methodologies, and metrics can be updated within the system as strategy, regulation, or the external environment evolve. Automated prompts remind risk owners to re-evaluate exposures and controls on a defined cadence, ensuring that the framework remains living and current. Trends, lessons learned, and historical data feed directly into refreshed assessments, enabling the organization

to pivot quickly in response to change. This makes ERM a continuous, self-improving capability rather than a cyclical reporting burden.

In summary, CoreStream GRC transforms enterprise risk management from a static, compliance-oriented function into a connected, orchestrated lifecycle. By unifying strategy, identification, response, monitoring, assurance, and review within a single system of record, CoreStream GRC delivers the agility, visibility, and assurance organizations need to navigate uncertainty and seize opportunity. The result is an ERM framework that is not only efficient and defensible, but alive — continuously learning, adapting, and enabling informed, risk-intelligent decisions at every level of the enterprise.

Benefits Organizations Have Received with CoreStream GRC for ERM

Most CoreStream GRC clients moved to the solution because their manual, document-centric approaches to enterprise risk management consumed excessive resources, lacked consistency, and failed to deliver the real-time visibility leadership needed. Teams were buried in spreadsheets, PowerPoint decks, and emails—making aggregation across regions, functions, and business units slow, error-prone, and unsustainable. Others turned to CoreStream GRC after outgrowing legacy GRC systems that were too rigid, costly, or slow to adapt to evolving governance and regulatory expectations. Across these organizations—from global energy producers to financial institutions and service firms—there is consistent recognition of CoreStream GRC's low total cost of ownership, speed of deployment, flexibility in aligning to unique frameworks, and rapid time to value.

Clients particularly highlight the transparency and insight CoreStream GRC brings through a **single source of truth for enterprise risk information**. Risk, control, and assurance data are unified across the enterprise—enabling everyone from first-line managers to board members to see consistent, current, and reliable information. Auditability and accountability are built in, giving leaders confidence that governance and risk oversight are not just documented but evidenced.

Specific benefits that GRC 20/20 finds CoreStream GRC ERM clients have achieved include:

- *360° visibility into enterprise risk* where clients gain a real-time, consolidated view of strategic, operational, project, and compliance risks across global operations. One organization spanning nearly 40 countries now delivers board-ready dashboards showing top risks and mitigations at group, regional, and country levels instantly, something previously requiring weeks of manual consolidation.

- *Elimination of spreadsheet chaos* in which CoreStream GRC replaces fragmented registers and static reports with an automated, workflow-driven environment. Leadership teams no longer manage risk through email chains or siloed documents; instead, they engage with live, contextual dashboards that continuously update as risk owners act.

- *Efficiency and speed of reporting* where organizations report saving days—sometimes weeks—each quarter previously spent collating data for committees and board packs. Automated workflows, reminders, and report generation allow CROs and risk leaders to reallocate time from administration to analysis and decision support.

- *Enhanced decision-making and board engagement* with live dashboards and analytics that enable executives and board committees to drill into risks in real time during meetings, exploring scenarios, controls, and mitigations without waiting for static slide decks. This has shifted risk management from a compliance-driven update to a strategic discussion.

- *Fewer blind spots and missed signals* through automated notifications, escalations, and reminders ensure that risk reviews, control tests, and actions occur on schedule. Clients emphasize that near-misses and emerging issues are now caught early, enabling proactive response rather than post-incident reaction.

- *Streamlined enterprise workflows* for risk identification to monitoring and assurance, CoreStream GRC orchestrates a continuous ERM lifecycle. Each step—assessment, treatment, testing, and review—is tracked with clear ownership, timelines, and dependencies, reducing ambiguity and ensuring accountability across the three lines of defense.

- *Integrated intelligence and contextual insight* with API integrations and data imports, CoreStream GRC aggregates internal and external risk indicators. Clients use these signals to inform risk assessments, horizon scanning, and early warning dashboards, creating a dynamic link between enterprise performance and risk exposure.

- *Granular, flexible reporting and analytics* as CoreStream GRC provides advanced risk aggregation and segmentation by business unit, region, or category. Organizations can visualize risk in multiple dimensions—residual exposure, trend trajectories, control effectiveness—using interactive dashboards that eliminate the need for manual data modeling.

- *Stronger accountability and engagement* where risk ownership is clearly defined at every level, supported by automated prompts and easy-to-use interfaces. In one financial services firm, adoption rose from 40% to 95% within a single cycle, reflecting how intuitive design and personalized workflows drive participation and accountability.

- *Collaboration across risk, the business, and assurance* so functions work within one system, sharing data while maintaining independence. Assurance testing results automatically link to the relevant risks and controls, ensuring consistent evidence for regulators and boards without redundant effort.

- *Data consistency and confidence* because CoreStream GRC enforces standardized taxonomies, workflows, and scoring methodologies, giving

executives confidence that risk data from different entities is comparable and trustworthy. Clients describe the platform as their "single source of truth" for enterprise risk and assurance information.

- *Full auditability and defensibility* as every change, review, and decision is timestamped and traceable. Audit trails provide a clear record of who did what, when, and why. This is essential for demonstrating governance and control effectiveness to auditors, regulators, and boards.

- *Agility in responding to change* such as new regulations like the UK Corporate Governance Code or integrating emerging risk domains such as sustainability and AI governance, clients highlight CoreStream GRC's configurability as a differentiator. Adjusting frameworks, taxonomies, or dashboards requires configuration, not code.

- *Continuous learning and improvement* through built-in lessons-learned and root-cause analysis features, risk incidents feed directly back into appetite reviews and control design. Clients report that risk management has evolved from a backward-looking reporting function into a learning discipline that actively improves performance and resilience.

CoreStream GRC modernizes enterprise risk management by replacing fragmented, manual oversight with an integrated, automated, and adaptive platform. Clients across industries consistently cite improved visibility, faster reporting, and greater engagement among leadership as transformative outcomes. The result is not just efficiency but a stronger risk culture, one where accountability is clear, insights are timely, and decisions are made with confidence across the entire enterprise.

Considerations in Context of CoreStream GRC for ERM

Every solution has its strengths and weaknesses, and CoreStream GRC is no exception. It may not be the right fit for every organization or ERM maturity level. While GRC 20/20 has identified many positive attributes of CoreStream GRC in enabling organizations to establish consistent, integrated, and data-driven enterprise risk management practices, this should not be interpreted as an unconditional endorsement.

Across multiple client references, CoreStream GRC is consistently praised for delivering strong return on investment through its speed of deployment, configurability, and ability to unify previously fragmented risk management processes into a single system of record. Clients report that the platform has replaced spreadsheets, siloed databases, and cumbersome legacy GRC tools with a modern, agile environment that increases efficiency, transparency, and engagement across the three lines of defense. The solution's balance of power and simplicity is a recurring theme: clients emphasize that CoreStream is sophisticated enough for enterprise needs yet intuitive enough for broad adoption.

Clients also commend CoreStream GRC's people, culture and approach to partnership. The vendor's responsiveness, willingness to listen, and practitioner-led support model are

repeatedly described as key differentiators. As one client put it, "CoreStream is serious about what they do and able to deliver in a friendly, approachable way — it's clear they care from the senior team down to the analysts supporting us."

At the same time, client references identified several opportunities for continued growth. Some would like to see expanded self-service capabilities for dashboards, reports, and workflow configuration to give business users even more autonomy. Others pointed to the potential for greater automation in report generation and risk analysis, along with a desire for enhanced AI-driven insights to assist with trend identification, drafting, and horizon scanning. A few global organizations expressed interest in broader regional support presence as CoreStream GRC continues to expand internationally. They currently have team members in EMEA, UK, USA and the Middle East. These are evolutionary improvements rather than deficiencies—natural expectations for a solution that has already proven itself as both capable and adaptable.

Overall, CoreStream GRC has established itself as a capable, flexible, and value-driven platform for organizations seeking to modernize and embed enterprise risk management into daily operations. It delivers measurable impact by replacing outdated manual processes with integrated, automated workflows and by empowering risk leaders with real-time insight across the enterprise. For organizations prioritizing agility, usability, and partnership over complexity and rigidity, CoreStream GRC represents a compelling choice, and one that continues to evolve in alignment with client needs and the future of ERM.

About GRC 20/20 Research, LLC

GRC 20/20 Research, LLC (GRC 20/20) provides clarity of insight into governance, risk management, and compliance (GRC) solutions and strategies through objective market research, benchmarking, training, and analysis. We provide objective insight into GRC market dynamics; technology trends; competitive landscape; market sizing; expenditure priorities; and mergers and acquisitions. GRC 20/20 advises the entire ecosystem of GRC solution buyers, professional service firms, and solution providers. Our research clarity is delivered through analysts with real-world expertise, independence, creativity, and objectivity that understand GRC challenges and how to solve them practically and not just theoretically. Our clients include Fortune 1000 companies, major professional service firms, and the breadth of GRC solution providers.

Research Methodology

GRC 20/20 research reports are written by experienced analysts with experience selecting and implementing GRC solutions. GRC 20/20 evaluates all GRC solution providers using consistent and objective criteria, regardless of whether or not they are a GRC 20/20 client. The findings and analysis in GRC 20/20 research reports reflect analyst experience, opinions, research into market trends, participants, expenditure patterns, and best practices. Research facts and representations are verified with client references to validate accuracy. GRC solution providers are given the opportunity to correct factual errors, but cannot influence GRC 20/20 opinion.

GRC 20/20 Research, LLC
313 North Plankinton Avenue, Suite 204
Milwaukee, WI 53203 USA
info@GRC2020.com
www.GRC2020.com