grc 20/20
Bringing GRC into Focus

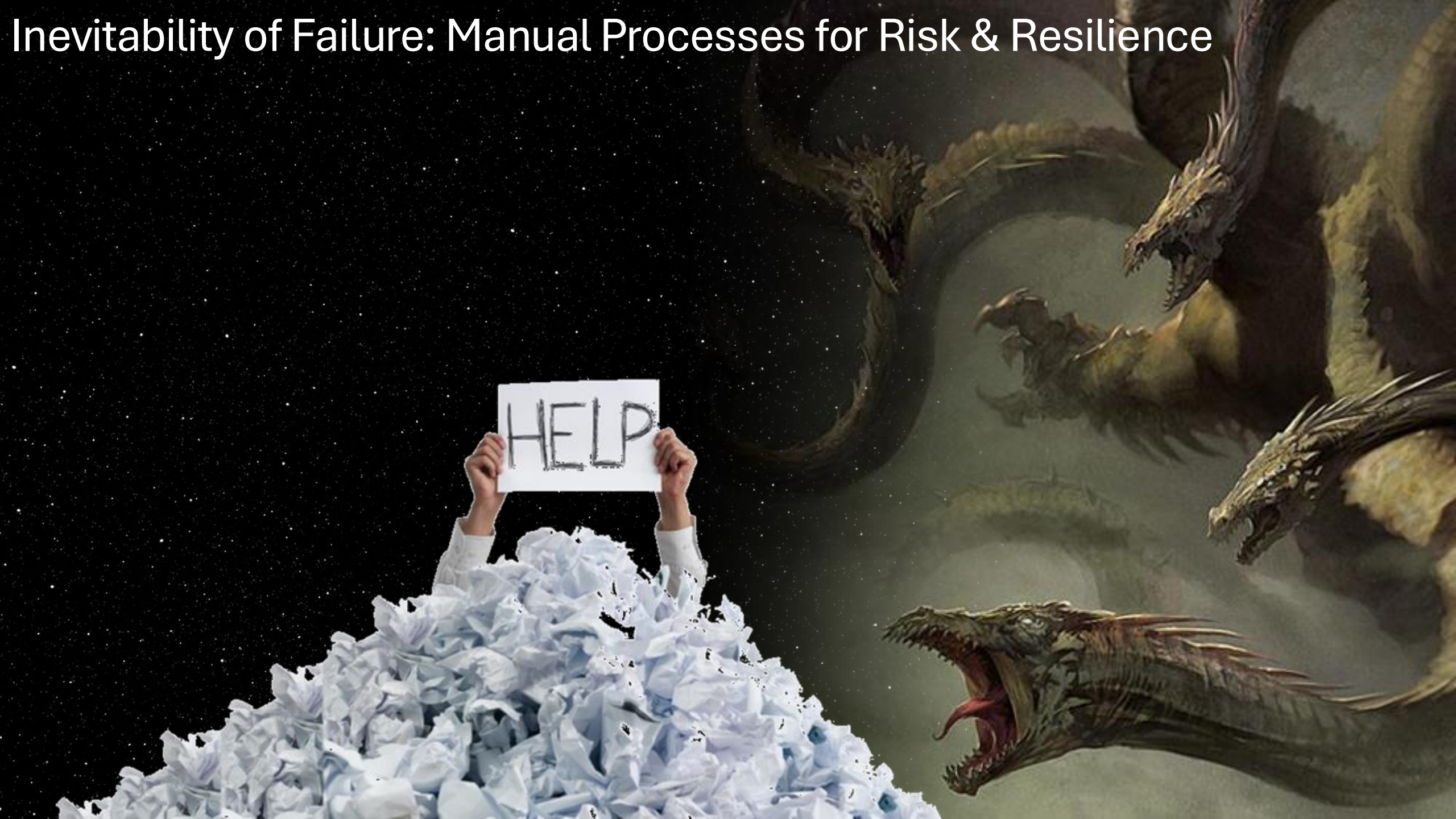
WORKSHOP

AI in GRC by Design

Michael Rasmussen, The GRC Pundit & Analyst

RISK IS OUR BUSINESS
grc report

Inevitability of Failure: Manual Processes for Risk & Resilience

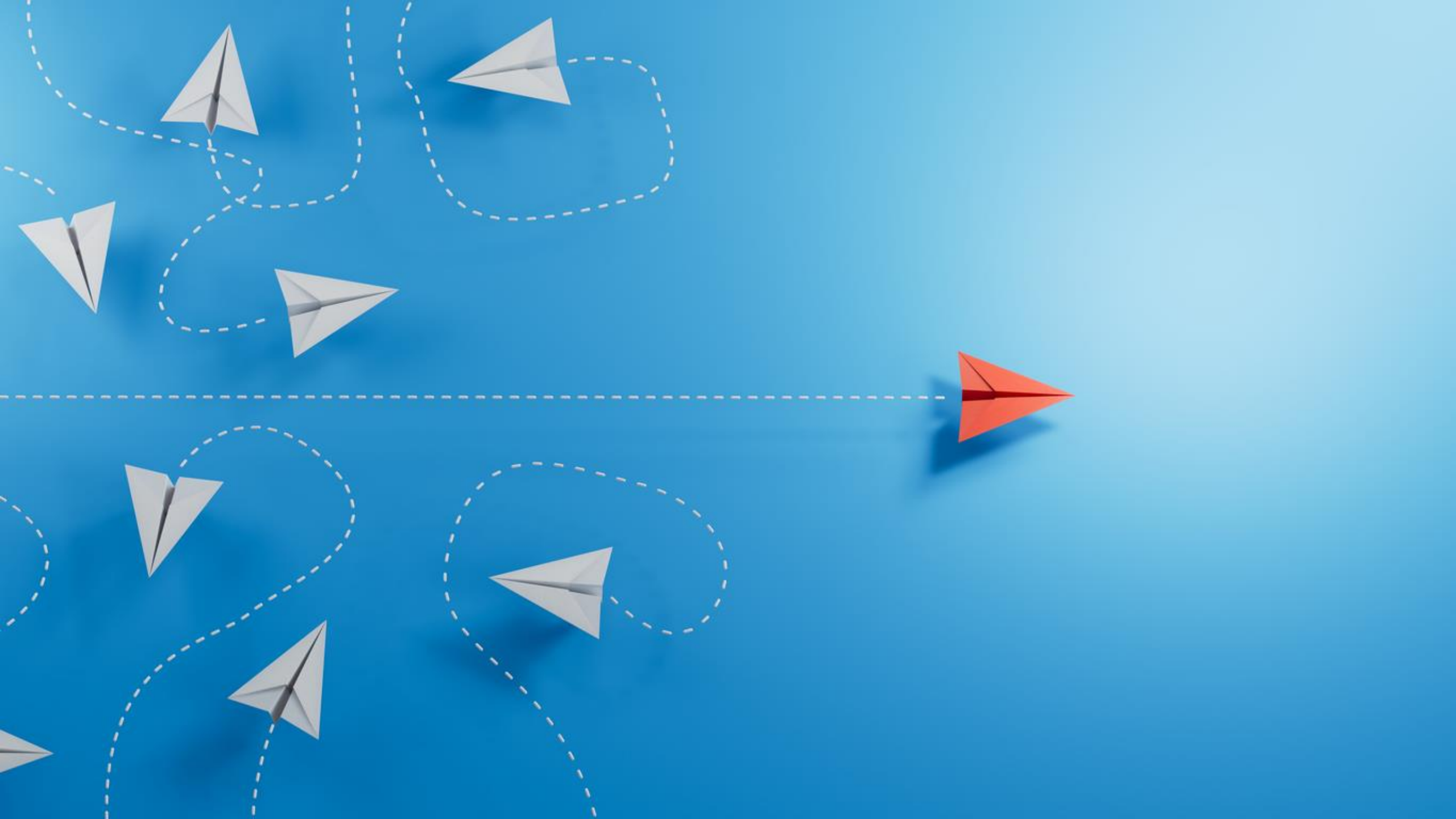


The more we study the major problems of our time, the more we come to realise that they cannot be understood in isolation. They are systemic problems, which means that they are interconnected and interdependent.

- Physicist Fritjof Capra

GRC Mystery House

- 160 rooms
- 47 fireplaces
- 6 kitchens
- 10,000 windows
- 65 doors to blank walls
- 13 staircases abandoned
- 25 skylights – in floors
- 147 builders/no architects
- Built without a blueprint
- $5.5 million over 38 years



The Official Definition of GRC . . .

GRC is a capability that enables an organization to:

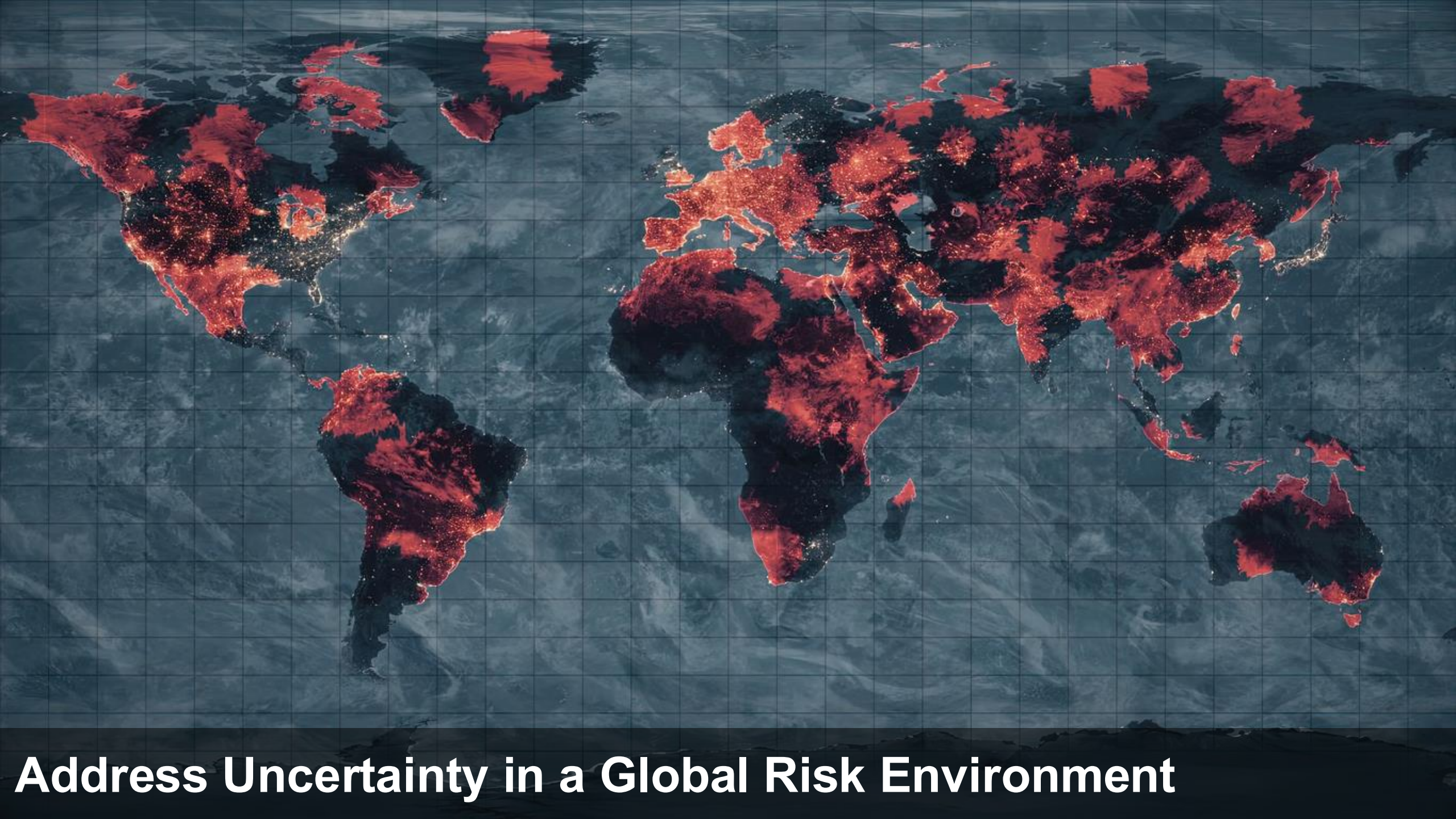
G) reliably achieve ***objectives***

R) address ***uncertainty***, and

C) act with ***integrity***.

SOURCE: OCEG GRC Capability Model

The Goal is to Reliably Achieve Objectives



Address Uncertainty in a Global Risk Environment

Act with Integrity to the Mandatory and Voluntary Boundaries

Why Many Programmes Stall

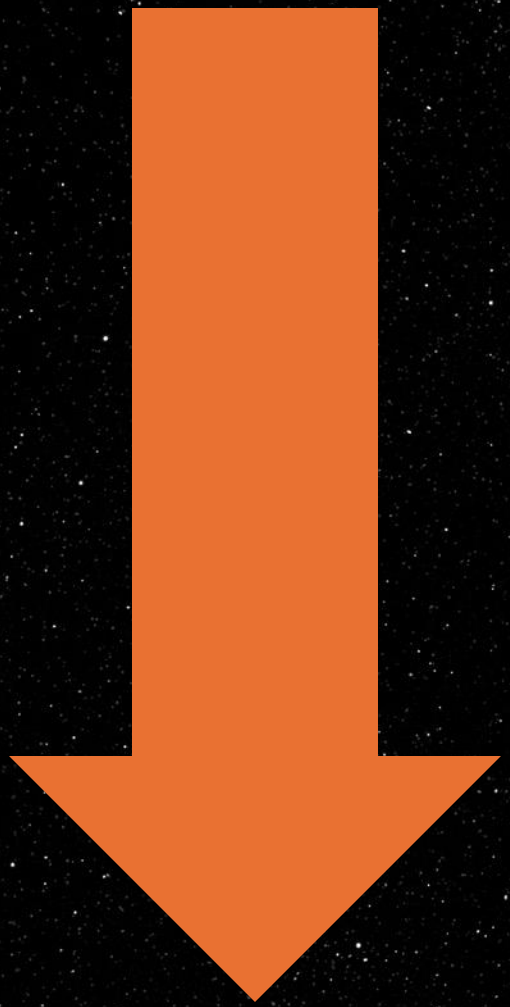
Fragmented Tooling

Inconsistent Processes

Weak Assurance

Noisy Metrics

GRC Management: a Top-Down Approach



- GRC Management Strategy
- GRC Management Process
- GRC Management Information
- GRC Management Technology


GRC Orchestration


Accountability


Confidence


Insight


Outcomes

GOAL: Lead with GRC Impact, Not Interfaces & Workflows

Innovating & Rearchitecting GRC

"Any intelligent fool can make things bigger, more complex and more violent. It takes a touch of genius – and a lot of courage to move in the opposite direction."

This quote has been attributed both to Einstein and E.F. Schumacher.


RETHINK

History of GRC Software . . .

Sarbanes-Oxley (SOX)

With SOX instituted as a U.S. federal law in 2002 — creating new and complex mandates for financial reporting — organizations focused much of their efforts on keeping up and less on delivering the broader GRC solution.

Enterprise GRC

With Enterprise or Integrated GRC, multiple departments could now work off a common platform, bringing together the first, second and third line functions. However, solutions still had constraints and required development.

GRC Architecture

As technology grew more sophisticated, GRC platforms began to emerge, but no single platform was able to solve an organization's entire risk management needs and required better integration with other business systems.

Agile GRC

The shift to GRC 4.0 began about five years ago, moving away from legacy systems and toward agile GRC solutions that required highly intuitive, configurable, and engaging systems for front-office to back-office risk functions.

GRC 5.0 and 6.0 build on and extend GRC 4.0

Cognitive GRC

As technology grew more sophisticated, Agile GRC solutions have leveraged cogntivie technologies – artificial intelligence such as machine learning, predictive analytics, robotic process automation, natural language processing to deliver greater levels of efficiency, effectiveness, resilience, and agility in GRC.

Business-Integrated GRC

Business-Integrated GRC is the next generation of GRC technology with a view focused on performance G[P]RC. GRC becomes an integrated part of a business management platform. The idea of a siloed GRC platform goes away to manage GRC as an integrated platform of the business, its objectives, its performance, and then risk, compliance, control, and assurance in this context.

GRC 7.0: GRC Orchestrate

GRC Orchestrate represents the 7th generation of GRC, a convergence of intelligent technologies and dynamic architecture that transforms GRC into a responsive, forward-looking, and fully integrated capability.

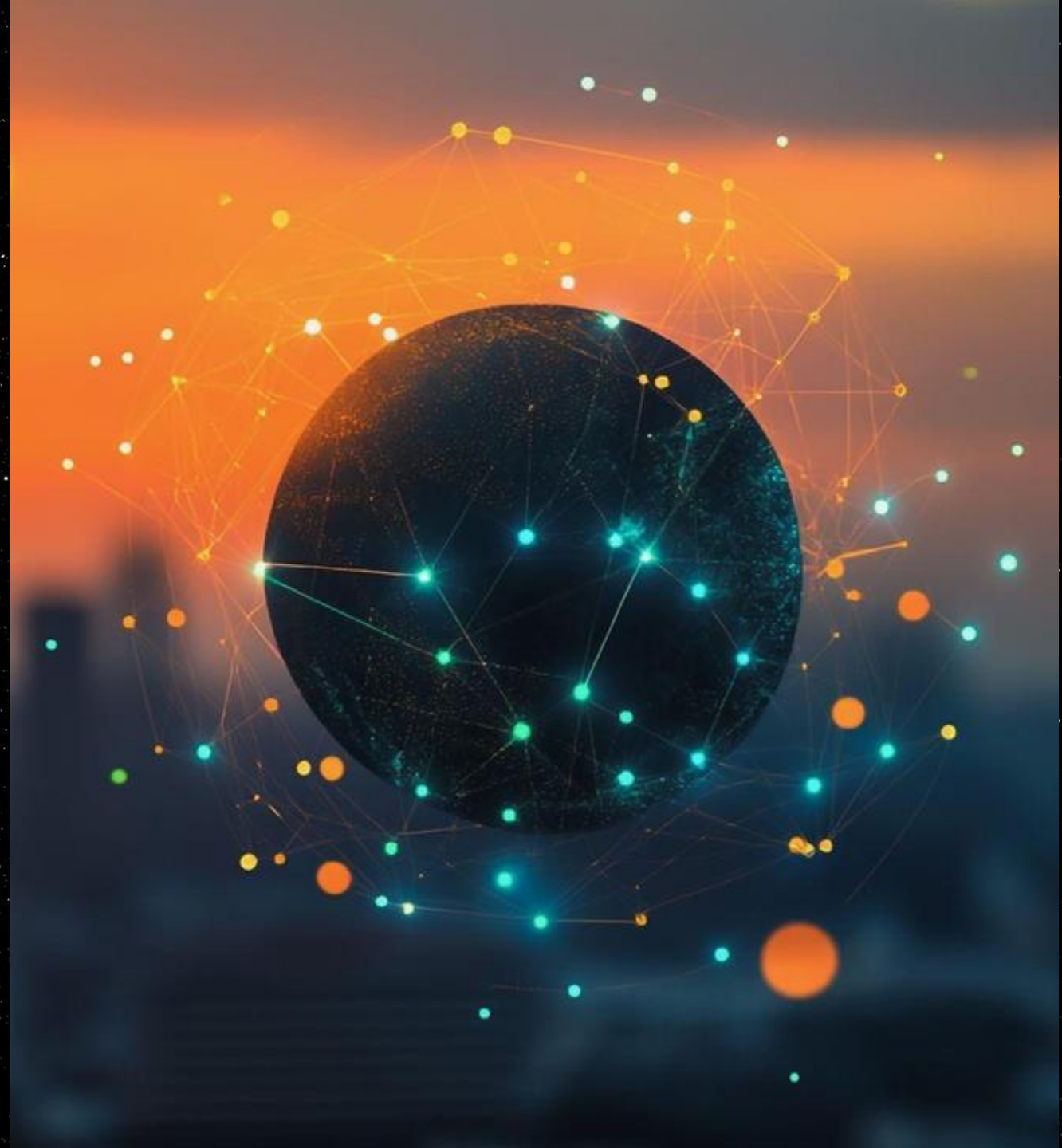
GRC 7.0 is powered by:

- ✓ **Agentic AI:** Introduces active, intelligent agents that sense, interpret, decide, and act across GRC processes.
- ✓ **Digital twins:** Provide real-time virtual models of the enterprise, enabling scenario simulation, predictive insight, and impact analysis.

GRC 7.0

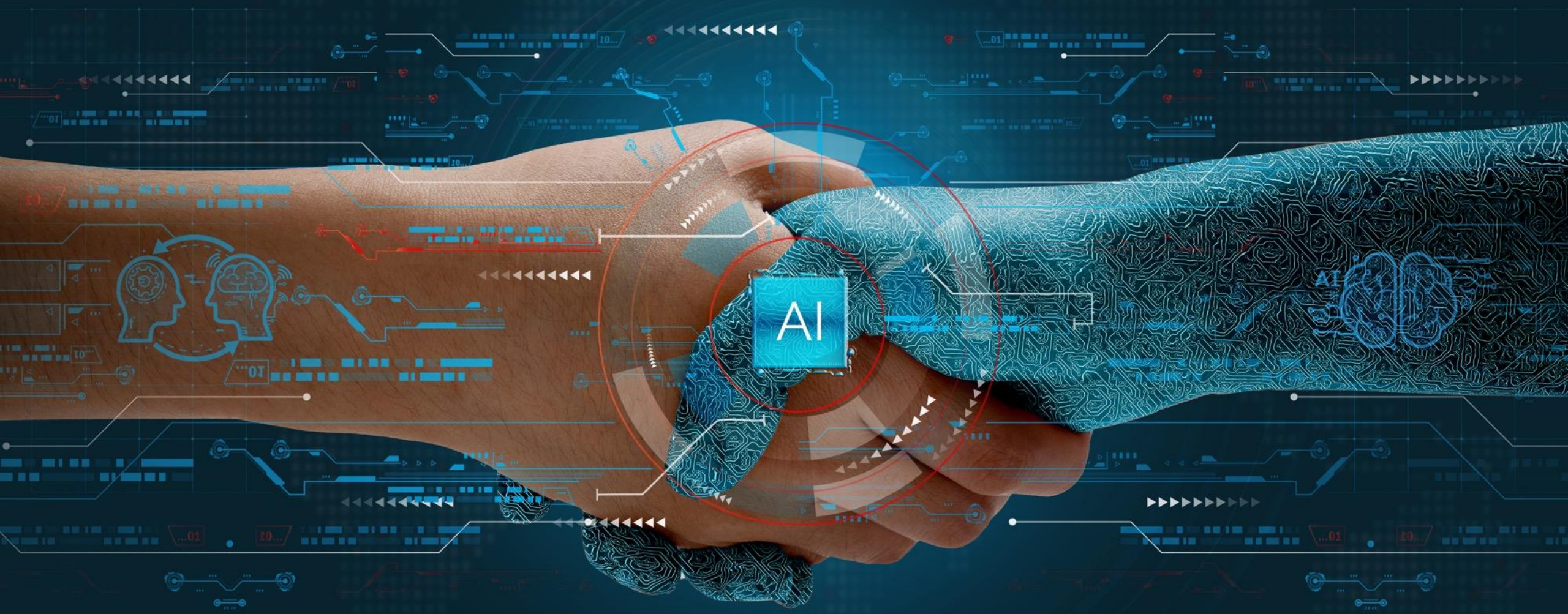
GRC Orchestrate is:

- ✓ **Connected:** Integrating risk, compliance, audit, performance, and sustainability into a seamless whole.
- ✓ **Dynamic:** Adapting in real-time to changes in business, regulation, and risk environments.
- ✓ **Contextual:** Aligning decisions with the mission, values, and strategy of the business.
- ✓ **Autonomous:** Operationalizing GRC through AI-driven agents that interact with systems, data, and stakeholders.
- ✓ **Foresight-driven:** Using digital twins to anticipate outcomes and optimize responses before disruption.



SOURCE: Martin-Vegue, Tony. From Heatmaps to Histograms: A Practical Guide to Cyber Risk Quantification, Chapter 3: GenAI Needs Adult Supervision, Jack Sparrow, Not Data from Star Trek

AI Is Reshaping Risk & Control: But We Must Be Wise



The Use of AI in GRC

GRC Platform Providing 360° Visibility

The Role of the Agentic AI


From System of Record to Homeostatic Risk & Control

Forecasting, Scenario Analysis, Risk Simulations

The Role of the Digital Twin in Scenario Modeling

Strategy & Decision Management

In the context of **GRC 7.0 – GRC Orchestrate**, strategy and decision management is about **enabling consistent, risk-informed decisions across the organization** — from the boardroom to the front line. It is not just about measuring performance, but **actively determining objectives and shaping strategy based on a clear analysis of risks, opportunities, and obligations**.

GRC technologies in this domain enable:

- **Decision-Centric Risk Analysis.** Risk is embedded directly into strategic and operational decision-making processes. Technologies evaluate the impact of risk on potential decisions, enabling decision-makers to weigh options and trade-offs with full context — not in isolation from risk, but integrated with it.
- **Objective Setting Aligned with Risk Capacity.** Decisions are guided by a clear understanding of enterprise risk appetite, tolerance thresholds, and regulatory boundaries. GRC tools help define and adjust objectives that are **achievable, ethical, and aligned with the organization's mission** under prevailing risk conditions.
- **Agentic AI for Decision Support.** Intelligent agents assist decision-makers at all levels by collecting, correlating, and interpreting relevant information — surfacing risks, obligations, and dependencies that influence or constrain the choice. These agents guide, but do not override, human judgment.
- **Scenario Planning with Digital Twins.** GRC platforms model multiple strategic options and simulate risk-adjusted outcomes using digital twins of the business. This allows leaders to visualize downstream effects, test assumptions, and select the most resilient and value-creating path forward.
- **Distributed but Aligned Decision-Making.** In GRC Orchestrate, decisions are not centralized, but they are **coordinated**. GRC technologies ensure that tactical, operational, and strategic decisions across business units remain consistent with enterprise objectives, shared values, and regulatory constraints.
- **Governance of the Decision Process.** Decision-making itself is subject to governance: who can decide, with what authority, using what data, under what conditions. GRC tools track and enforce this governance, ensuring transparency, accountability, and defensibility.

This is the strategic core of GRC Orchestrate: **A future where every decision — from frontline actions to executive strategy — is risk-aware, purpose-aligned, and governed by integrity.**

Performance & Objective Management

Within the GRC 7.0 – **GRC Orchestrate** framework, **Performance & Objective Management** ensures that an organization not only makes informed decisions but also consistently **executes on those decisions** to achieve intended outcomes. It connects strategic intent with operational execution, while dynamically aligning performance with risk, compliance, and ethical commitments.

Key capabilities of GRC technologies in this category include:

- **Risk-Aligned Goal Setting.** Objectives are not defined in isolation — they are established with visibility into the organization's internal and external risk environment, regulatory obligations, and stakeholder expectations. This ensures that performance targets are both **ambitious and attainable** within risk and compliance constraints.
- **Real-Time Performance Monitoring.** Technologies provide real-time dashboards and metrics that measure performance against objectives, KPIs, KRIs, and compliance obligations. These insights allow for **continuous performance assurance** and rapid intervention when thresholds are exceeded or progress stalls.
- **Dynamic Strategy Execution.** GRC Orchestrate connects goals, risks, and controls across the enterprise, enabling continuous adaptation as strategies evolve. When new risks emerge, regulations change, or performance lags, GRC tools help realign actions with strategy and adjust objectives accordingly.
- **Integrated Accountability & Oversight.** Roles and responsibilities are clearly defined across departments and levels. GRC systems track ownership, progress, and exceptions, enabling transparent accountability for performance across the enterprise.
- **Agentic AI for Performance Optimization.** AI agents proactively analyze gaps, flag underperformance, and recommend adjustments to objectives or processes. These agents help optimize pathways to achieving strategic and operational goals, while ensuring alignment with risk appetite and compliance requirements.
- **Performance Integrity.** It is not enough to achieve performance — it must be done with **integrity**. GRC technologies ensure that objectives are pursued within ethical, regulatory, and organizational boundaries, preventing misconduct or short-termism that undermines long-term value.

At its core, **Performance & Objective Management in GRC Orchestrate** is about **reliably achieving what matters** — with resilience, responsibility, and real-time visibility. It turns governance and risk management into **strategic enablers of success**, not obstacles to it.

Enterprise & Operational Risk & Resilience Management

In the GRC 7.0 – **GRC Orchestrate** architecture, **Enterprise Risk & Resilience Management** forms the connective tissue between strategy, decisions, and performance. It ensures that the organization not only identifies and manages risk, but also develops the **resilience to adapt and thrive** in a world of continuous disruption.

GRC technologies in this domain provide a forward-looking and dynamic approach to managing risk, uncertainty, and operational continuity across the enterprise:

- **Holistic Risk Identification & Assessment.** These platforms enable consistent identification and assessment of risks — strategic, operational, financial, regulatory, cyber, third-party, ESG, and beyond — across all business units and levels of the organization. Risk is not siloed but is integrated into a unified risk ontology and enterprise context.
- **Resilience-Oriented Risk Evaluation.** Modern tools go beyond static heat maps. They simulate potential events and cascading impacts through **probabilistic models, dependency mapping, and scenario analysis** — often powered by digital twins — to understand how one disruption may amplify another. This allows organizations to anticipate convergence risk, systemic fragility, and interdependencies across their risk landscape.
- **Dynamic Risk Response & Control Adaptation.** GRC platforms automate and guide risk responses that are appropriate to the business context, risk appetite, and changing conditions. Whether mitigating, transferring, avoiding, or accepting risk, the response is designed to preserve strategic intent and ensure continuity of performance.
- **Real-Time Monitoring & Early Warning Systems.** Through AI, IoT, and external data integration, organizations can monitor risk indicators and resilience metrics in real time. These systems provide **early warnings, anomaly detection**, and trigger-based actions — enabling a shift from reactive response to proactive resilience.
- **Embedded Risk in Strategy & Decisions.** Risk is a core input into strategic planning and operational choices. GRC Orchestrate technologies ensure that risks are **quantified, contextualized, and continuously updated** so that leaders and teams at every level can make informed decisions and set realistic, resilient objectives.
- **Resilience by Design.** These technologies guide organizations to build structural, operational, and behavioral resilience into processes, relationships, and supply chains. This includes business continuity planning, recovery strategies, and stress testing — not as separate exercises, but as integrated dimensions of strategic execution.
- **Agentic AI for Risk Intelligence.** Intelligent agents synthesize internal and external risk signals, continuously learn from evolving data, and generate forward-looking insights — becoming an essential risk advisory function embedded within workflows and decision cycles.

Enterprise Risk & Resilience Management in GRC Orchestrate is not about avoiding risk — it is about **understanding it, anticipating it, and thriving through it.**
It aligns risk and resilience with the organization's **decisions and objectives**, ensuring that strategy is not only achievable but **sustainable in the face of volatility.**

Digital Risk & Resilience Management

In the GRC 7.0 – **GRC Orchestrate** model, **Digital Risk & Resilience Management** evolves beyond traditional cybersecurity into a broader, integrated capability that enables **digital trust**. It connects information security, IT risk, cyber resilience, and digital compliance with the organization's enterprise risk strategy, performance objectives, and stakeholder expectations.

This category of GRC technology enables organizations to **protect, assure, and enable digital business** in an environment of escalating threats, regulatory demands, and stakeholder scrutiny. Key capabilities include:

- **Integrated Digital Risk Frameworks.** Digital risk is addressed holistically — not just through technical controls but across third-party relationships, privacy obligations, cloud environments, AI governance, data integrity, and business continuity. These platforms align digital risk domains with enterprise risk taxonomies and resilience frameworks.
- **Cyber and IT Risk Management.** GRC technologies support the identification, analysis, and mitigation of IT and cybersecurity risks. They provide structured assessments, control testing, vulnerability tracking, and risk quantification to evaluate exposure and prioritize response. These risks are mapped to business objectives and regulatory requirements, not managed in isolation.
- **Operational Technology (OT) and IoT Risk Integration.** As digital risk moves beyond IT systems into operational environments, platforms extend visibility to smart infrastructure, connected assets, and industrial control systems — ensuring comprehensive resilience across both digital and physical layers.
- **Digital Resilience & Incident Response.** Platforms integrate cyber resilience capabilities such as breach simulation, tabletop exercises, playbook automation, and coordinated response planning. Digital resilience becomes part of business resilience — ensuring critical services can recover quickly and securely.
- **AI-Driven Threat Intelligence & Automation**
  Agentic AI is embedded into digital risk solutions to automate control monitoring, threat detection, and compliance analysis. These agents can identify suspicious behavior, monitor external threat landscapes, and trigger adaptive responses in real time.
- **Digital Trust & Transparency.** Digital trust is established not only by securing systems but by demonstrating ethical, compliant, and resilient digital operations. GRC technologies ensure that digital risk management is **accountable, auditable, and aligned** with privacy expectations, regulatory requirements (e.g., GDPR, NIS2, DORA), and ESG reporting obligations.
- **Strategic Alignment with Enterprise Risk.** Digital risk is no longer just a technical issue — it is a **strategic risk**. These technologies ensure that digital risk scenarios, cyber events, and IT disruptions are directly connected to enterprise risk scenarios, key business decisions, and performance metrics.

Digital Risk & Resilience Management in GRC Orchestrate is how organizations achieve **trust at the speed of digital**.. It ensures that as businesses become more connected, automated, and data-driven, they are also secure, compliant, and resilient — not in isolation, but as a coordinated component of enterprise risk and strategy.

Compliance, Ethics & Obligation Management

In the GRC 7.0 – **GRC Orchestrate** model, **Compliance, Ethics & Obligation Management** defines the **moral and legal boundaries** of the organization — ensuring that both **mandatory expectations** (laws, regulations, contracts) and **voluntary commitments** (values, ethics, ESG promises) are understood, operationalized, and upheld across the business.

These technologies no longer live in the back office — they are embedded into the fabric of business operations, decision-making, and culture. They ensure that the organization acts with integrity as it pursues performance and manages risk. Key capabilities include:

- **Defined Boundaries of Conduct.** Platforms allow organizations to define and govern both the external obligations they are required to meet and the internal commitments they choose to uphold — from laws and regulations to codes of ethics, ESG goals, and cultural values.
- **Structured Obligation Inventory.** A centralized, dynamic record of all obligations — mapped to business functions, policies, controls, and risks — creates traceability and consistency across compliance efforts.
- **Regulatory Change Management.** GRC technologies monitor, interpret, and route changes in the global regulatory landscape using AI and expert curation — ensuring relevant updates reach the right people at the right time.
- **Compliance Assessments and Control Monitoring.** These systems facilitate ongoing compliance evaluation through structured assessments, self-checks, evidence collection, and real-time control testing tied to specific obligations.
- **Ethics and Culture Engagement.** Organizations build ethical strength through integrated case management, speak-up tools, values-based training, and behavioral analytics — turning values into measurable, lived behavior.
- **Stakeholder and Regulator Engagement.** Technologies track and govern interactions with regulators, boards, and assurance bodies — from formal inspections and audits to disclosures, certifications, and compliance attestations.
- **Embedded Compliance in Business Workflows.** Obligations and ethical boundaries are built into business processes — from vendor onboarding to product development — ensuring that compliance is proactive, intuitive, and aligned with performance.
- **Transparent Reporting and Assurance.** Real-time dashboards and reporting tools provide visibility into the state of compliance and ethics, enabling both internal governance and external assurance with confidence and clarity.

Compliance, Ethics & Obligation Management in GRC Orchestrate is how organizations define and defend both their **license to operate** and their **license to lead**. It ensures that what an organization stands for is not just stated — it is lived, measured, and aligned with how decisions are made and objectives are pursued.

Policy & Training Management

In GRC 7.0 – **GRC Orchestrate**, **Policy & Training Management** becomes the connective tissue between strategic intent and everyday behavior. Policies define **how the organization operates within its boundaries**, while training and engagement ensure that people — across all lines of defense — understand, internalize, and apply those expectations in real time.

These technologies are not just about managing documents or checking training boxes. They ensure that governance, risk, compliance, ethics, and performance expectations are clearly communicated, easily understood, and fully embedded in the workflows of employees and third parties alike. Key capabilities include:

- **Structured Policy Lifecycle Management.** GRC platforms manage the creation, review, approval, distribution, and version control of policies, standards, procedures, and guidelines — with audit trails, ownership, and contextual alignment to obligations and risks.
- **Engaging and Targeted Training Delivery.** Training is delivered through integrated eLearning, microlearning, and gamification strategies — personalized by role, geography, and risk exposure. These tools ensure comprehension and retention, not just completion.
- **Embedded Awareness and Just-in-Time Guidance.** Policies and training are made accessible where decisions happen — in workflows, applications, and communication channels — offering real-time guidance, not just static reference.
- **Forms, Attestations, and Disclosure Management.** GRC systems capture and manage critical compliance-related disclosures (e.g., conflicts of interest, gifts & hospitality, outside activities), including attestations to policies and ethical standards, with automated reminders and escalation workflows.
- **Extended Enterprise Engagement.** These technologies support training and policy communication to third parties — suppliers, partners, contractors — ensuring that the organization's expectations extend beyond internal boundaries and are understood across the ecosystem.
- **Auditability and Policy-to-Control Traceability.** Policies are mapped to risks, controls, obligations, and performance metrics — enabling assurance, impact analysis, and the ability to track how policy shifts influence compliance and behavior.
- **Culture and Behavior Analytics.** Platforms provide insights into training effectiveness, policy comprehension, and patterns of employee behavior — allowing organizations to measure culture and refine messaging to strengthen accountability and integrity.

Policy & Training Management in GRC Orchestrate is how organizations **translate risk and compliance into action and culture** — ensuring that the right expectations reach the right people at the right time, and that those expectations are understood, lived, and enforced across the enterprise.

Internal Control Management, Monitoring & Automation

In GRC 7.0 – **GRC Orchestrate**, **Internal Control Management** evolves from static documentation and manual testing into a dynamic, intelligent capability that enables the organization to design, monitor, and optimize its control environment in real time.

Controls are no longer just compliance checkpoints — they are **living safeguards of risk, performance, and integrity**, embedded into business operations and continuously orchestrated by technology. Powered by **agentic AI** and informed by **digital twins**, control systems now adapt with the business, sense changes in context, and respond with precision. Key capabilities include:

- **Control Design and Mapping.** GRC technologies provide structured tools to define, document, and map internal controls across business processes, systems, risks, policies, and regulatory obligations — establishing a clear control architecture across the organization.
- **Real-Time Control Monitoring.** Control effectiveness is monitored continuously through data integrations, control indicators, and system logs. Agentic AI identifies anomalies, flags control degradation, and suggests remediation pathways — transforming control oversight from periodic to perpetual.
- **Digital Twin–Driven Control Simulation.** Digital models of processes and systems allow organizations to simulate how controls perform under different scenarios and stress conditions. This enables proactive identification of gaps, overcontrols, or brittle dependencies.
- **Automated Testing and Assurance.** Control assessments are streamlined through automated workflows, integrated evidence capture, and AI-assisted testing. Self-assessments, control certifications, and testing results are tracked and aggregated for real-time visibility and audit readiness.
- **Control Automation and Orchestration.** Agentic AI orchestrates controls across multiple systems and teams — triggering controls based on business context, adjusting control logic dynamically, and even executing low-risk control actions autonomously.
- **Control Rationalization and Optimization.** Redundant or obsolete controls are identified and eliminated, while overlapping controls are streamlined. AI and analytics help ensure that the control environment remains efficient, cost-effective, and aligned with performance and risk objectives.
- **Auditability and Control Analytics.** Every control is tied to its purpose, owner, performance, and evidence — enabling complete transparency and accountability. Dashboards, heat maps, and audit trails provide on-demand insights for auditors, management, and regulators.

Internal Control Management in GRC Orchestrate is not a checklist exercise — it is a **strategic capability for resilience and accountability**.
Enabled by AI and modeled through digital twins, internal controls become intelligent safeguards that adapt to change, prevent breakdowns, and empower decision-makers to trust the systems that underpin performance and compliance.

Issue Reporting & Event/Case Management

In GRC 7.0 – **GRC Orchestrate**, **Issue Reporting & Event/Case Management** becomes a critical feedback and accountability system that empowers the organization to surface, track, and resolve the unexpected — from internal misconduct to external incidents, and everything in between.

These technologies give voice to the frontline and extended enterprise, enabling early detection, consistent handling, and transparent resolution of issues. They ensure that organizations do not just react to disruption, but **learn from it, respond with integrity, and strengthen resilience**. Key capabilities include:

- **Multi-Channel Issue Intake.** Platforms support anonymous and attributed reporting across hotlines, web portals, mobile apps, embedded workflow forms, and third-party channels — enabling a safe, confidential space to raise concerns, incidents, or misconduct.
- **Centralized Case Management.** GRC systems unify the intake, triage, investigation, documentation, and resolution of a wide range of issues — including fraud, ethics violations, data breaches, harassment, safety events, or operational incidents.
- **Structured Investigation Workflows.** Investigations follow consistent, rule-based workflows with clear case ownership, task assignment, escalation logic, legal holds, and evidence tracking — ensuring defensibility and accountability across all stages,
- **AI-Assisted Case Intelligence.** Agentic AI analyzes patterns across case data, prioritizes high-risk issues, identifies potential root causes, and flags trends — enabling a shift from isolated response to proactive insight and systemic remediation.
- **Digital Twin–Enabled Impact Simulation.** Event and incident data feed into digital twin models of operations, allowing organizations to simulate downstream business impact, understand interconnected failures, and refine response plans.
- **Disclosure, Loss, and Impact Recording.** Events are tied to operational loss, compliance exposure, reputational risk, and recovery time metrics — enabling both financial reporting and resilience performance tracking.
- **Integrated Remediation and Root Cause Analysis.** GRC platforms connect issues to underlying control failures, policy breakdowns, or training gaps— triggering corrective actions, risk re-evaluation, and continuous improvement across governance layers.
- **Reporting, Analytics, and Transparency.** Dashboards, heat maps, case metrics, and resolution timelines provide real-time insight for leadership, audit, and compliance — enabling full lifecycle visibility and demonstrating a culture of responsiveness.

Issue Reporting & Event/Case Management in GRC Orchestrate ensures the organization is not only alert to breakdowns — but able to **respond with speed, integrity, and insight.** It transforms incidents into opportunities to strengthen culture, reduce risk, and build resilience across the organization and its extended ecosystem.

ESG & Sustainability Management

In GRC 7.0 – **GRC Orchestrate**, **ESG & Sustainability Management** begins with **objectives** — environmental stewardship, social responsibility, and sound governance — and aligns the organization's strategy, operations, and disclosures around those commitments.

Rather than treating ESG as a reporting exercise or a compliance silo, GRC technologies enable ESG to be fully embedded into decision-making, performance management, and stakeholder engagement. ESG becomes a living framework — where objectives are not just set but measured, monitored, and improved through orchestrated data, controls, and accountability. Key capabilities include:

- **ESG Objective and Commitment Management.** Platforms capture and operationalize ESG goals — from carbon neutrality and DEI targets to ethical sourcing and board diversity — linking them to business units, performance indicators, and responsible owners.
- **Integrated ESG Data Collection and Workflow.** GRC systems coordinate the collection of qualitative and quantitative ESG data across the organization and supply chain — enabling structured disclosures aligned with global frameworks such as CSRD, ISSB, GRI, SASB, and TCFD.
- **Sustainability Risk in Context of Objectives.** Risk is addressed in direct relation to ESG goals: environmental risk to net-zero strategies, social risk to labor and human rights commitments, and governance risk to ethical and board oversight objectives. These risks are managed through the broader GRC architecture.
- **Embedded ESG in Business Operations.** ESG factors are integrated into procurement, product design, operations, and third-party engagements — ensuring sustainability is not a side project but a principle embedded in how the business runs.
- **Agentic AI for ESG Insight and Benchmarking.** Intelligent agents help gather, validate, and interpret ESG data from structured and unstructured sources — surfacing anomalies, measuring impact, and benchmarking performance against peers and industry standards.
- **Digital Twin Modeling for ESG Impact.** Digital twins simulate the business impact of ESG strategies, helping organizations test pathways to sustainability goals, assess dependencies, and model future scenarios across carbon, water, diversity, and other dimensions.
- **Cross-Domain Integration and Traceability.** ESG relies on capabilities from across the GRC ecosystem — regulatory change, third-party risk, ethics, incident management, health and safety, privacy, and more. GRC Orchestrate connects these silos into a cohesive ESG control and reporting environment.
- **Assurance and Stakeholder Transparency.** Platforms support structured disclosures, audit trails, third-party validation, and real-time dashboards — building trust with regulators, investors, customers, and employees through consistent, defensible reporting.

ESG & Sustainability Management in GRC Orchestrate transforms ESG from a reactive disclosure task into a **strategic performance system** — one that connects **purpose to process, integrity to innovation, and sustainability to success.**

Third-Party GRC Management

In GRC 7.0 – **GRC Orchestrate**, **Third-Party GRC Management** begins not with risk — but with **objectives**: the outcomes an organization seeks to achieve through its relationships with vendors, suppliers, contractors, outsourcers, and other third parties.

These relationships are extensions of the business. They carry strategic value, operational interdependence, and shared risk. GRC technologies in this domain ensure that organizations can **reliably achieve their third-party objectives** — while navigating uncertainty, enforcing compliance, and maintaining resilience across an increasingly complex and dynamic ecosystem. Key capabilities include:

- **Relationship-Centric Governance.** Platforms manage the full third-party lifecycle — from onboarding and due diligence through contracting, performance, compliance monitoring, and offboarding — all centered on the outcomes the relationship is intended to deliver.
- **Integrated Risk and Compliance Oversight.** Solutions assess and monitor third-party risk across financial, cyber, ESG, geopolitical, reputational, and regulatory domains — aligning due diligence and ongoing monitoring to relationship criticality and risk exposure.
- **Digital Twin Modeling of Third-Party Ecosystems.** Organizations can model their supply chains and extended enterprise using digital twins — simulating disruptions, dependencies, and cascading effects to understand how one failure or delay can impact broader objectives and operations.
- **Agentic AI for Third-Party Intelligence.** AI agents gather, analyze, and interpret data from internal systems and external sources (e.g., adverse media, sanctions lists, ESG ratings, performance metrics), surfacing hidden risks, flagging anomalies, and recommending actions in real time.
- **Assessment, Attestation & Disclosure Management.** Tools manage surveys, attestations, certifications, and disclosures from third parties — such as compliance with codes of conduct, ABAC policies, conflict of interest, sanctions; and data privacy obligations — and track them across time and engagements.
- **Performance and Service-Level Monitoring.** GRC platforms monitor contractual and operational performance, linking service-level indicators and relationship health back to objectives, obligations, and overall risk posture.
- **Cross-Domain Integration.** Third-party management intersects with multiple domains — from policy and incident management to ESG, cybersecurity, health and safety, and regulatory compliance. GRC Orchestrate connects these silos into a unified view of third-party integrity and performance.
- **Auditability and Lifecycle Reporting.** Complete documentation of third-party engagements, risk evaluations, control validations, and communications ensures defensibility and readiness for audits, certifications, and regulator reviews.

Third-Party GRC Management in GRC Orchestrate empowers organizations to manage their **extended enterprise with agility, intelligence, and purpose**.
It ensures that third-party relationships are not just compliant and secure — but aligned, adaptive, and resilient in pursuit of shared business outcomes.

Audit Management, Analytics & Assurance

In GRC 7.0 – **GRC Orchestrate**, **Audit Management, Analytics & Assurance** is no longer confined to retrospective reviews or static annual cycles. It becomes a **real-time assurance function**, deeply integrated into business strategy, risk oversight, and performance execution — powered by data, driven by risk, and enabled by intelligent automation.

Modern GRC technologies elevate internal audit into a **strategic advisory and assurance engine**, offering continuous, risk-aligned insights into the effectiveness of controls, the reliability of operations, and the integrity of decisions. Key capabilities include:

- **Risk-Based Audit Planning and Scoping.** Platforms align audit plans with enterprise risk registers, strategic objectives, compliance exposure, and business priorities — ensuring that limited audit resources are applied where they matter most.
- **Audit Lifecycle Management.** GRC systems manage the full audit lifecycle, from scheduling and scoping through fieldwork, workpapers, collaboration, issue tracking, and reporting — with real-time visibility and role-based task workflows.
- **Agentic AI for Audit Intelligence.** Intelligent agents support auditors by recommending areas of focus based on emerging risks, control failures, anomalies in operational data, or changes in external conditions — guiding audit teams with predictive insight.
- **Automated Testing and Continuous Auditing.** Platforms enable continuous control testing through integrations with business systems, automating evidence gathering, exception detection, and compliance checks — shifting from periodic sampling to **continuous assurance**.
- **Data Analytics and Exception Monitoring.** Audit analytics tools allow deep analysis of operational, financial, and control data — detecting trends, red flags, and anomalies that inform both current audits and enterprise-wide improvement efforts.
- **Digital Twin Integration for Audit Simulation.** By linking with digital twins of business processes and systems, auditors can simulate risk exposure, control behavior, and audit readiness across changing conditions and hypothetical scenarios.
- **Issue & Recommendation Management.** GRC platforms track audit findings through to resolution — assigning ownership, setting timelines, monitoring progress, and providing assurance to the board and regulators on remediation and accountability.
- **Integrated Reporting and Stakeholder Assurance.** Dashboards and assurance maps provide visibility into audit coverage, open issues, control health, and risk exposure — enabling real-time reporting to audit committees, regulators, and executives.

Audit Management, Analytics & Assurance in GRC Orchestrate transforms audit into an **orchestrator of trust** — validating that strategy is grounded in reality, that controls are effective, and that performance is delivered with integrity. It equips audit functions to move at the **speed of risk**, delivering value not just after the fact, but as a continuous partner in resilience, performance, and responsible growth.

AI GRC (AI Governance, Risk & Compliance)

In GRC 7.0 – **GRC Orchestrate**, **AI GRC** ensures that artificial intelligence is not just powerful — but **purposeful, trustworthy, and accountable.** As organizations increasingly rely on AI to drive decisions, automate operations, and shape engagement, GRC technologies provide the governance, risk, and compliance infrastructure necessary to align AI systems with strategy, ethics, and law.

AI GRC technologies help organizations **reliably achieve the intended objectives of AI**, manage the uncertainty it introduces, and act with integrity in its design, deployment, and use. This is not a separate function — it is a core orchestration capability that spans business, IT, data science, ethics, and compliance. Key capabilities include:

- **AI Governance and Oversight.** GRC platforms support the definition and enforcement of AI governance frameworks — including principles, policies, roles, and accountability structures — ensuring that AI systems align with the organization's mission, values, and risk appetite.
- **AI Lifecycle Risk Management.** Solutions identify, assess, and manage risks across the AI lifecycle — from design and development to deployment, retraining, and retirement — including model drift, bias, explainability, adversarial vulnerability, and operational failure.
- **Ethical and Responsible AI Use.** Technologies embed ethical standards into AI development and use — tracking adherence to fairness, transparency, human oversight, and non-discrimination principles — and operationalizing voluntary codes (e.g., OECD, NIST, ISO, G7 Hiroshima).
- **AI Compliance and Regulatory Alignment.** Platforms monitor evolving AI-related laws, standards, and guidance (e.g., EU AI Act, NIST RMF, ISO/IEC 42001), map obligations to controls and policies, and enable structured evidence gathering to demonstrate compliance.
- **Model Documentation and Explainability.** GRC tools support the documentation of model purpose, logic, data sources, and assumptions — providing traceability and explainability for internal governance, audit, and external regulators.
- **Third-Party AI Oversight.** Capabilities extend to vendor-provided AI systems and embedded models — ensuring risk, compliance, and ethical requirements are enforced across the extended digital ecosystem.
- **Agentic AI for Monitoring AI.** Intelligent agents monitor AI model behavior in production, detect anomalies or drift, trigger alerts, and suggest mitigations — enabling **AI to help govern AI** through feedback loops and machine-augmented oversight.
- **Integrated Reporting and Assurance.** Dashboards, model risk inventories, and control health reports provide stakeholders — including boards, regulators, and the public — with visibility into how AI is governed, managed, and monitored in real time.

AI GRC in GRC Orchestrate equips organizations to **innovate with confidence and integrity** — ensuring that AI is not only effective, but safe, fair, and aligned with what the business stands for. It transforms artificial intelligence into **accountable intelligence** — enabling transparency, resilience, and trust in a future increasingly shaped by algorithms.

Data GRC Management

In GRC 7.0 – **GRC Orchestrate**, **Data GRC** technologies are the backbone of trusted, ethical, and intelligent enterprise performance. Data is both an asset and a liability — it fuels decisions, drives digital transformation, and must be governed with clarity, consistency, and contextual intelligence.

Data GRC ensures that organizations define the rules of engagement around their data — how it is created, used, protected, and retired — with the same rigor applied to financial or physical capital. It operationalizes integrity in a world where data volume, velocity, and variability are accelerating exponentially. Core capabilities include:

- **Enterprise Data Governance Platforms.** Tools that define the direction, ontology, and information architecture to govern structured and unstructured data across silos. This includes data catalogs, lineage mapping, data classification, stewardship workflows, business glossaries, and metadata integration — all mapped to business objectives.
- **Data Risk Management.** Technologies to identify and assess data risk exposure: including unauthorized access, corruption, exfiltration, inconsistency, and data quality degradation. Supports ongoing monitoring of risk across cloud, on-premises, and third-party environments — with automated alerting and contextual risk scoring.
- **Data Compliance Management.** Manages regulatory, contractual, and ethical obligations related to data — such as GDPR, HIPAA, CCPA, AI Act, and financial sector data localization laws. Enables mapping of data sets to applicable requirements, policy controls, and evidence for audits and assessments.
- **Data Policy & Control Enforcement.** Enables organizations to define and enforce rules around data retention, access, encryption, masking, anonymization, and lifecycle management — across hybrid data environments. Supports automated remediation and reporting when controls are bypassed or fail.
- **Semantic Orchestration & Ontology Mapping.** Establishes common language and meaning across systems, departments, and jurisdictions — allowing for data harmonization across the organization. This is essential for integrated GRC reporting, cross-border compliance, and coordinated governance.
- **Digital Twins of Data Ecosystems.** Models the flow, lineage, and transformation of data across the organization in real-time. Enables simulation of breach scenarios, regulatory changes, or architectural shifts — and how they impact compliance, risk, and performance.
- **Agentic AI for Data Integrity, Privacy & Control.** AI agents autonomously monitor data behavior, flag anomalies, recommend governance adjustments, and predict where data may drift from policy or risk parameters. These agents support adaptive governance at scale, continuously learning and aligning with business needs and regulatory trends.

Data GRC in GRC Orchestrate transforms data from a fragmented liability into a trusted strategic asset — governed with precision, protected by design, and orchestrated intelligently through semantic coherence and agentic response.

Financial Crime GRC Management

In the age of **GRC Orchestrate**, managing financial crime risk is not a siloed compliance exercise — it is a coordinated and adaptive effort to ensure the organization reliably achieves objectives, addresses uncertainty, and acts with integrity in the face of dynamic and evolving financial crime threats.

Financial Crime GRC technologies enable organizations to govern and orchestrate their defenses against money laundering, sanctions violations, bribery and corruption, insider abuse, and fraud. These capabilities must be risk-aligned, intelligence-driven, and embedded across the lines of business — not bolted on as afterthoughts. This category includes:

- **Financial Crime Compliance Platforms.** Holistic solutions that bring together governance, policy, controls, risk assessments, monitoring, and reporting across AML, anti-bribery/anti-corruption (ABAC), sanctions, and fraud. These platforms enable centralized oversight and distributed ownership across the three lines of defense.
- **Transaction & Behavioral Monitoring.** Real-time and batch analysis of customer and counterparty behaviors, payment flows, and transaction patterns to detect red flags and emerging typologies. Combines rules-based detection with machine learning models for anomaly detection and trend identification.
- **Sanctions & Watchlist Screening.** Screening of individuals, entities, and instruments against global and regional lists (OFAC, EU, UN, HMT, BIS, etc.). Includes list management, phonetic and fuzzy matching, contextual screening, and audit trails. Increasingly enhanced with AI-driven name resolution and geoparsing.
- **Know Your Customer (KYC), KYB, and Continuous Due Diligence.** Customer and business onboarding technologies that integrate identity verification, risk scoring, beneficial ownership, and document validation. Also supports **cKYC** — ongoing refresh of profiles based on real-time signals, third-party intelligence, adverse media, and relationship changes.
- **Anti-Bribery & Corruption (ABAC) Risk Management.** Governance of third-party intermediaries, agents, vendors, and high-risk business relationships. Includes due diligence, ongoing monitoring, conflict of interest management, gift and hospitality tracking, and integration with whistleblower and investigations tools.
- **Fraud Detection & Insider Risk Management.** Solutions to detect and prevent fraud schemes — including payments fraud, application fraud, expense fraud, and insider misuse. Leverages user/entity behavior analytics (UEBA), pattern recognition, and anomaly scoring across physical and digital environments.
- **Case Management & SAR Filing.** End-to-end management of alerts, investigations, documentation, and regulatory reporting. Enables workflow automation, evidencelinkage, decision traceability, and submission of suspicious activity reports (SARs) to appropriate authorities.
- **Risk-Based Approach & Financial Crime Risk Assessment.** Supports enterprise-wide and business-unit level assessments of financial crime risk. Evaluates inherent risk across geographies, customer types, channels, products, and delivery methods. Links risk to control adequacy and residual exposure for board and regulator reporting.
- **Digital Twins & Simulations for Financial Crime Exposure.** Creates a real-time model of the organization's financial crime risk exposure across people, processes, technology, and third parties. Simulates impact of emerging threats, changes in regulation, or internal control failures to stress-test resilience.
- **Agentic AI for Alert Prioritization & Analyst Augmentation.** AI agents that assist in triage, provide contextual risk narratives, and recommend actions. Learns from analyst behavior to improve prioritization and reduce fatigue. Delivers transparency, speed, and alignment to policy and regulatory expectations.
- **Financial Crime Ontologies & Semantic Intelligence.** Structures the language of financial crime — from risks to regulations to controls — into an enterprise semantic architecture. Aligns policies, procedures, obligations, and systems to ensure consistency, defensibility, and scalability.

Financial Crime GRC is no longer just about avoiding penalties. It is about building trust, maintaining integrity, and protecting the organization from reputational and operational harm. In GRC 7.0, financial crime defense becomes proactive, orchestrated, and aligned to the core mission of the business.

Finance GRC Management

In GRC 7.0 – **GRC Orchestrate**, **Finance GRC Management** ensures that financial governance, risk, and compliance are not isolated to reporting cycles — but embedded into daily operations, decision-making, and organizational resilience.

Finance GRC technologies support the integrity of financial data, the transparency of disclosures, and the defensibility of internal control over financial reporting (ICFR). These solutions bring together risk awareness, control automation, analytics, and regulatory compliance into a unified orchestration layer — enabling CFOs, controllers, and audit committees to navigate complexity with confidence. Key capabilities include:

- **Internal Control over Financial Reporting (ICFR).** Platforms manage the design, documentation, monitoring, and testing of financial controls tied to SOX and other statutory requirements — with automation, workflow, and audit trails that ensure accuracy and assurance in financial disclosures.
- **Financial Close Management.** Tools streamline the financial close process, coordinate activities across stakeholders, and monitor reconciliations and certifications — helping reduce errors, delays, and control failures during month-end, quarter-end, and year-end cycles.
- **Statutory, Regulatory & Investment Reporting.** GRC systems help manage compliance with external financial reporting requirements, including SEC, ESMA, ESEF, and IFRS mandates — while aligning disclosures with investor, board, and ESG expectations.
- **Fraud Management.** Capabilities to detect, investigate, and prevent financial fraud through anomaly detection, transaction monitoring, whistleblower intake, and integration with case management — enabling early intervention and continuous monitoring of financial integrity.
- **Miscellaneous Financial GRC Tools.** Includes solutions for tax compliance risk, treasury control assurance, capital expenditure governance, and financial statement risk modeling — tied to broader enterprise controls and risk registers.
- **Agentic AI for Financial Integrity and Oversight.** Intelligent agents monitor financial control data, analyze trends in reporting anomalies, flag potential exposure, and suggest corrective actions — augmenting finance and compliance teams with real-time insight and intelligent audit readiness.
- **Digital Twin Simulation of Financial Risk & Control Environments.** Financial systems and reporting workflows are modeled to simulate control breakdowns, fraud scenarios, or regulatory impacts — enabling finance leaders to test assumptions and build resilience across financial processes.

Finance GRC Management in GRC Orchestrate empowers the organization to ensure **financial integrity, reporting transparency, and control reliability** — while enabling finance to act as a strategic partner in performance, trust, and accountability.

Environmental GRC Management

In GRC 7.0 – **GRC Orchestrate**, **Environmental GRC** ensures the organization can reliably achieve its **environmental obligations, goals, and values** — with full transparency, traceability, and responsiveness to an increasingly complex landscape of regulatory, operational, and stakeholder demands.

Environmental GRC technologies provide visibility and control over environmental performance and risk across business units, geographies, and supply chains. These capabilities enable organizations to manage compliance with environmental regulations, monitor impact, model disruption, and ensure alignment with sustainability and ESG objectives — all in a dynamic, connected architecture. Key capabilities include:

- **Environmental Management Platforms.** Core systems that monitor, analyze, and manage environmental programs, controls, and impact across operations — ensuring alignment with environmental regulations, internal policies, and enterprise sustainability goals.
- **Air, Water, and Waste Management.** Solutions track and manage air emissions, wastewater discharge, hazardous and non-hazardous waste, and resource usage — with reporting aligned to regulatory thresholds, permits, and voluntary frameworks.
- **Chemical Management.** Platforms control the classification, handling, storage, transport, and disposal of chemicals — including integration with SDS libraries and global compliance lists (e.g., REACH, TSCA, GHS).
- **Energy & Carbon Management.** Tools capture and analyze data related to energy use, carbon footprint, and GHG emissions — enabling emissions tracking, forecasting, and performance benchmarking aligned with net-zero and decarbonization goals.
- **Land Use & Permitting.** Systems manage environmental permits, land use restrictions, biodiversity impact, and related obligations — ensuring that operations respect environmental zoning, conservation boundaries, and remediation commitments.
- **Sustainability & Environmental Reporting.** GRC platforms support the compilation, calculation, and submission of data for regulatory reports, investor disclosures, and ESG frameworks (e.g., CDP, CSRD, GRI) — with auditability and assurance built-in.
- **Miscellaneous Environmental Tools.** Includes specialized tools for environmental modeling, spill and incident tracking, remediation planning, and impact assessments — often integrated into larger environmental or ESG platforms.
- **Digital Twin Integration for Environmental Impact Modeling.** Digital twins simulate the environmental consequences of strategic or operational decisions — allowing organizations to model the cascading effects of facility changes, supply chain shifts, or resource constraints.
- **Agentic AI for Monitoring and Compliance.** AI agents automate environmental data collection, analyze patterns, detect anomalies, and trigger alerts — enabling real-time compliance with environmental obligations and early detection of potential violations.

Environmental GRC in GRC Orchestrate empowers organizations to **embed environmental responsibility into enterprise performance and resilience.**
It ensures that environmental objectives are not managed in isolation — but integrated across risk, compliance, ESG, and operations to build a sustainable, adaptive, and trusted organization.

Health & Safety GRC Management

In GRC 7.0 – **GRC Orchestrate**, **Health & Safety GRC** empowers organizations to proactively manage the wellbeing of their workforce, the safety of their operations, and their obligations to regulators, communities, and stakeholders. These technologies ensure that health and safety expectations are not siloed in compliance manuals — but orchestrated across daily decision-making, frontline behavior, and organizational resilience.

Modern Health & Safety GRC solutions deliver integrated visibility, engagement, and control over H&S programs — from hazard identification and training to incident response and corrective action — aligned with enterprise objectives, risk posture, and ESG priorities. Key capabilities include:

- **Health & Safety Management Platforms.** Core systems that manage H&S policies, programs, procedures, compliance requirements, and performance indicators across locations and departments — providing a unified view of health and safety across the enterprise.
- **Health & Safety Forms & Document Management.** Digital forms and content tools for capturing risk assessments, safety walkthroughs, PPE checklists, job safety analyses, and other frontline documentation — with mobile, multilingual, and offline capabilities for global workforces.
- **Health & Safety Incident Solutions.** Systems for reporting, investigating, and tracking workplace incidents, near misses, and unsafe conditions — integrating corrective actions, root cause analysis, and trend monitoring to drive learning and prevention.
- **Occupational Safety Solutions.** Specialized tools for managing workforce safety — including ergonomics assessments, confined space entry, exposure tracking, and compliance with occupational health standards (e.g., OSHA, ISO 45001).
- **Hazard Analysis Solutions.** Platforms for proactive identification, evaluation, and control of workplace hazards using risk matrices, bowtie analysis, and job hazard analysis (JHA) — tied to risk registers and control frameworks.
- **Chemical Management & Labeling Solutions.** Tools for managing hazardous substances, container labeling, SDS libraries, and right-to-know requirements — ensuring compliance with global H&S chemical standards (e.g., GHS, WHMIS).
- **Miscellaneous Health & Safety Tools.** Includes PPE tracking, fatigue management, health surveillance, behavioral safety observation, emergency drills, and contractor safety management — all connected to broader GRC frameworks.
- **Agentic AI for Predictive Safety and Alerts.** AI agents analyze safety data in real time to detect leading indicators, trigger alerts, and recommend interventions — shifting from lagging indicators to predictive insight and preventive action.
- **Digital Twin Simulation of Safety Scenarios.** Digital twins of facilities and workflows allow simulation of incident scenarios, response timing, hazard spread, and control effectiveness — strengthening preparedness and informing operational decisions.

Health & Safety GRC in GRC Orchestrate ensures that safety is not just a compliance activity — it is a **core value operationalized at scale**, integrated into strategy, risk management, and organizational culture. It empowers organizations to protect people, ensure safe workplaces, and build resilience through visibility, accountability, and foresight.

Human Resources GRC Management

In GRC 7.0 – **GRC Orchestrate**, **Human Resources GRC Management** ensures that organizations can govern and support their most valuable asset: their people. HR GRC technologies integrate governance, risk, and compliance into the full employee lifecycle — ensuring that workforce strategy, conduct, and culture are aligned to business objectives, ethical standards, and regulatory expectations.

These tools extend beyond process automation. They embed **accountability, fairness, and engagement** into how people are hired, developed, evaluated, and protected — while ensuring HR risks are visible, managed, and reported in real time. Key capabilities include:

- **Human Capital Management Oversight.** Platforms enable governance over workforce-related strategies, policies, risks, and metrics — from hiring and onboarding to retention, leadership development, and succession planning, aligned with DEI, ESG, and strategic workforce objectives.
- **HR Investigations Management.** Solutions manage the intake, triage, documentation, investigation, and resolution of HR-related incidents — including harassment, discrimination, retaliation, bullying, and workplace conflict — with auditability, consistency, and sensitivity.
- **HR Policy & Training Governance.** GRC technologies manage the distribution, attestation, and training around HR policies (e.g., code of conduct, ethics, leave policies, hybrid work expectations), ensuring employees understand and commit to the organization's expectations and values.
- **Miscellaneous HR GRC Tools.** Includes tools for employee disclosures (e.g., conflicts of interest), attestation tracking, contractor compliance, workforce health/safety integration, and workplace well-being — integrated into broader GRC and ESG frameworks.
- **Agentic AI for Workforce Risk Monitoring.** Intelligent agents monitor trends in HR metrics, survey sentiment, case data, and training engagement to detect emerging issues, bias patterns, or compliance gaps — and recommend interventions before they escalate.
- **Workforce Digital Twins for Risk & Strategy Simulation.** HR digital twins model workforce structures, turnover risk, talent pipelines, and labor disruption scenarios — helping leadership plan and test decisions related to organizational change, labor strategy, and human capital investment.

Human Resources GRC in GRC Orchestrate transforms HR from a service function into a **governance and culture engine** — ensuring that human capital strategies are ethical, accountable, and aligned with enterprise performance, risk, and integrity.

Identity GRC Management

In GRC 7.0 – **GRC Orchestrate**, **Identity GRC** technologies serve as a foundational layer for enterprise integrity, enabling the organization to govern, manage, and assure that the right individuals — whether human or machine — have the right access, at the right time, for the right reason.

Identity is no longer just an IT issue. It is a business-critical layer of governance, risk, and compliance that intersects with every GRC domain. Identity GRC ensures accountability and traceability in how access is provisioned, modified, and removed — reducing the risk of internal fraud, external attack vectors, operational disruption, and regulatory non-compliance. Core capabilities include:

- **Identity Governance Platforms.** Technologies that manage the full lifecycle of identities (employees, third parties, bots, agents) — from onboarding to offboarding — including role-based access models, entitlement reviews, joiner/mover/leaver processes, and escalation workflows. Governance is contextualized to business objectives and GRC obligations.
- **Identity Risk Management & Segregation of Duties (SoD).** Tools that define access risk criteria, model toxic combinations of entitlements, and conduct real-time SoD analysis — enabling continuous monitoring and mitigation of identity risks against business-critical processes and systems.
- **Access Certification & Policy Enforcement.** Automated processes for periodic access reviews, recertification, and attestation — ensuring alignment between identity roles, organizational policies, and regulatory mandates. Includes policy violation detection, exception management, and enforcement.
- **Privileged Access & Entitlement Management.** Specialized tools for controlling high-risk access — such as admin, root, or critical infrastructure access — with elevated scrutiny, session monitoring, and just-in-time provisioning. Protects the organization from insider threats and credential abuse.
- **Identity Analytics & Behavioral Monitoring.** Capabilities to detect anomalies in access patterns, identify high-risk behavior, and dynamically adjust access controls — integrating with threat intelligence and incident response to support zero-trust architectures.
- **Agentic AI for Identity Lifecycle Automation & Risk Detection.** Intelligent agents autonomously manage access requests, flag unusual access combinations, and recommend revocation or remediation actions. AI learns from historical decisions, context, and peer comparisons to continuously optimize access governance.
- **Digital Twins of Identity & Access Ecosystem.** Digital representations of roles, access paths, and entitlement structures allow organizations to simulate onboarding/offboarding scenarios, assess cascading access risk, and proactively test the impact of access policy changes on organizational exposure.

Identity GRC in GRC Orchestrate empowers organizations to manage access with precision, accountability, and resilience — across human users, third parties, and machine identities. It integrates identity as a living layer of GRC: continuously sensing, governing, and adapting access in concert with risk, compliance, and business objectives.

Legal GRC Management

In GRC 7.0 – **GRC Orchestrate**, **Legal GRC Management** ensures that legal obligations, disputes, and exposures are managed with agility, integrity, and intelligence. Legal GRC technologies enable organizations to align legal strategy with business objectives, orchestrate discovery and evidence management, and enforce legal holds, retention, and response workflows — all while maintaining defensibility, transparency, and resilience.

This is not just about protecting the organization after something happens. In GRC Orchestrate, Legal GRC becomes a **proactive line of assurance** — surfacing risks early, enabling ethical decision-making, and embedding legal awareness across processes, policies, and relationships. Key capabilities include:

- **Legal Matter & Case Management.** Technologies manage the lifecycle of legal events, investigations, and cases — from intake and triage through documentation, counsel coordination, timeline tracking, and resolution — ensuring structured workflows and evidence-backed decisions.
- **eDiscovery and Legal Hold Automation.** Solutions support defensible discovery practices with tools to identify, preserve, collect, and review electronically stored information (ESI). Legal holds are issued, tracked, and enforced automatically across custodians and content systems.
- **Retention and Disposition Management.** GRC platforms integrate with enterprise content systems to define and enforce legal retention schedules — ensuring that information is retained or disposed of according to legal, regulatory, and policy obligations.
- **Integrated Risk and Regulatory Mapping.** Legal obligations and risks are mapped to contracts, regulations, policies, and controls — enabling visibility into how legal exposures intersect with operational and strategic activities.
- **Digital Twin Integration for Litigation Exposure Modeling.** Legal scenarios can be modeled through digital twins to simulate potential litigation or regulatory investigation outcomes, understand upstream failures, and assess financial or reputational impacts.
- **Agentic AI for Legal Intelligence.** Intelligent agents support legal teams by reviewing documents, surfacing risk signals, identifying privileged content, extracting obligations, and predicting areas of exposure based on internal data and legal trends.
- **Cross-Functional Legal Awareness.** Legal expectations and responsibilities are embedded into business workflows — from procurement and marketing to HR and third-party management — ensuring that legal risks are considered proactively, not reactively.
- **Auditability and Legal Reporting.** Platforms provide real-time dashboards and defensible audit trails across case activity, hold status, data retention, and resolution metrics — enabling compliance with regulators, courts, and oversight bodies.

Legal GRC Management in GRC Orchestrate transforms legal from a reactive cost center to a **strategic partner in enterprise integrity, accountability, and resilience**. It enables legal teams to move at the speed of business — equipped with intelligence, automation, and insight to guide the organization through uncertainty with confidence.

Privacy GRC Management

In GRC 7.0 – **GRC Orchestrate**, **Privacy GRC Management** ensures that privacy is not treated as a reactive compliance obligation — but as a dynamic and embedded component of **trust, digital governance, and responsible innovation**. Privacy GRC technologies help organizations operationalize privacy principles across jurisdictions, business units, and systems, enabling the ethical and compliant use of personal data throughout its lifecycle.

These platforms orchestrate people, processes, and technology to uphold individual rights, fulfill regulatory requirements, and align privacy with business objectives and digital transformation. Key capabilities include:

- **Privacy GRC Management Platforms.** Centralized systems that oversee privacy programs, frameworks, roles, and governance structures — enabling coordination across legal, IT, compliance, marketing, and third-party risk domains.
- **PIA/DPIA Controls & Automation.** Tools to perform, manage, and automate Privacy Impact Assessments (PIAs) and Data Protection Impact Assessments (DPIAs), including risk scoring, control recommendations, approvals, and evidence logging.
- **Data Mapping & Inventory Solutions.** Platforms that map personal data flows, process inventories, systems, data categories, and purposes of processing — enabling compliance with obligations such as GDPR Article 30 and CPRA data tracking.
- **Privacy Rights Automation Solutions.** Capabilities to automate fulfillment of Data Subject Access Requests (DSARs), deletion requests, opt-outs, and consent changes — integrated across data systems and aligned with regulatory timelines.
- **Privacy Incident Management Solutions.** Solutions to triage, investigate, and respond to data breaches and privacy incidents — managing timelines, impact analysis, regulatory reporting, and communications with data subjects and authorities.
- **Privacy Policy & Training Solutions.** Tools for managing privacy-related policies, delivering employee and third-party training, tracking attestation, and reinforcing awareness of privacy expectations and obligations across roles.
- **Miscellaneous Policy & Training Management Tools.** Includes consent and cookie management, vendor privacy assessments, cross-border transfer tracking, and tools that embed privacy into digital design processes ("Privacy by Design").
- **Agentic AI for Privacy Monitoring and Response.** Intelligent agents assist in identifying unauthorized data use, flagging policy misalignment, interpreting global regulatory updates, and initiating automated responses to risks or rights requests.
- **Digital Twin Modeling for Privacy Impact Simulation.** Digital representations of data ecosystems allow simulation of privacy risks, policy changes, and breach scenarios — helping organizations forecast and optimize privacy control strategies in advance.

Privacy GRC Management in GRC Orchestrate empowers organizations to treat privacy not as a burden, but as a **strategic enabler of digital trust and ethical data use**.
It delivers agility, accountability, and alignment in navigating a world of rising expectations around personal data — from consumers, regulators, and society at large.

Quality GRC Management

In GRC 7.0 – **GRC Orchestrate**, **Quality GRC** technologies ensure that product and service quality is not just monitored — it is proactively governed, risk-aligned, and strategically integrated into enterprise performance, compliance, and customer trust.

Quality GRC connects operational excellence with strategic resilience by embedding quality oversight across product development, manufacturing, service delivery, and supply chain operations. These technologies enable organizations to prevent defects, respond quickly to failures, comply with regulations, and drive continuous improvement through orchestrated data, controls, and collaboration. Key capabilities include:

- **Quality Management Platforms.** Core systems that manage quality programs, audits, metrics, certifications, and standards across the enterprise — including ISO, FDA, GMP, and other regulatory and industry-specific frameworks.
- **Non-Conformance & Variance Solutions.** Tools to track, investigate, and resolve product and process non-conformances — integrating root cause analysis, risk scoring, and resolution workflows.
- **Equipment Management Solutions.** Capabilities for managing calibration, maintenance, and performance tracking of critical manufacturing and testing equipment — ensuring uptime, accuracy, and compliance.
- **Product Regulation & Labeling Solutions.** Tools to manage compliance with product-related laws, technical standards, labeling requirements, and safety certifications — often across complex global jurisdictions and markets.
- **Corrective Action/Preventive Action (CAPA) Solutions.** Platforms for identifying systemic issues, implementing corrective measures, and tracking preventive actions — tightly integrated with incidents, audits, and supplier feedback loops.
- **Miscellaneous Quality Management Tools.** Includes supplier quality oversight, complaint handling, deviation management, risk-based quality reviews, and field service quality — all connected to broader GRC and operational systems.
- **Agentic AI for Quality Analytics and Early Detection.** Intelligent agents continuously monitor quality data, detect early signals of deviation, assess defect patterns, and recommend interventions — driving predictive and preventive quality assurance.
- **Digital Twin Modeling for Quality Simulation and Scenario Testing.** Digital representations of products, production lines, and service environments enable simulation of process changes, disruption scenarios, and risk impact — enhancing design quality and operational adaptability.

Quality GRC in GRC Orchestrate transforms quality from a reactive checkpoint to a **strategic enabler of customer trust, compliance assurance, and operational resilience**. It ensures that quality is not just built in — it is governed, measured, and continuously improved in alignment with business goals and stakeholder expectations.

Measuring the Value of GRC

GRC Value: It’s More Than Just ROI

Efficiency = Traditional ROI (Time-Saved, Money-Saved)

GRC Efficiency

Reducing friction, manual effort, and redundancies across GRC processes . . .

- ✓Automation of workflow and tasks.
- ✓Eliminating duplicate/redundant processes and activities.
- ✓Efficiency in reporting with a single record of truth.
- ✓Single data entry flows into multiple reporting outputs (regulatory, board, operational).
- ✓Automated control testing and evidence collection.

Efficient GRC is about doing things right.
But effective GRC is about doing the right things.

Effectiveness = Effectiveness is about actual/measurable risk reduction

GRC Effectiveness

Improving the ability to identify, evaluate, and treat real risk exposure . . .

✓Risk indicators linked to business objectives trigger early warnings.

✓Control effectiveness validated through incident correlation, not just testing.

✓Dynamic risk scoring reflects real-time changes in environment or exposure.

✓Risk appetite thresholds are tied to escalation rules and board reporting.

✓Ensuring things do not slip through the cracks.

If you cannot demonstrate that your GRC program is measurably reducing risk to your objectives, then you are not being effective — just active, perhaps like a hamster on a wheel not truly getting anywhere.

Resilient = Ability to Anticipate and Recover from Incidents & Disruption

GRC Resilience

Detecting and containing risk events before they escalate into crises . . .

✓Integrated monitoring flags critical disruptions before service impacts.

✓Cross-functional incident playbooks streamline coordinated response.

✓Near-miss reporting channels improve learning and future mitigation.

✓Role-based alerts ensure issues are acted upon quickly by the right teams.

✓Risks are linked to upstream and downstream dependencies.

Resilience is what keeps a compliance issue from becoming a scandal.

A system failure from becoming a shutdown.

A risk exposure from becoming a crisis.

Agility = Navigating Uncertainty on the Road Ahead

GRC Agility

Adapting GRC processes to support evolving strategy, objectives, and risks . . .

- ✓Risk libraries easily updated to reflect changing objectives and emerging threats.
- ✓Scenario modeling evaluates risk to strategic pivots and objectives.
- ✓GRC dashboards shift focus based on changing KPIs and objectives.
- ✓Expansion into new markets triggers realignment of risk and compliance workflows.
- ✓Rapid deployment of new regulatory requirements without re-architecting.

GRC should not be the handbrake.

It should be the navigation system — helping the business steer safely through uncertainty toward its objectives.

GRC 20/20's Four Dimensions of GRC Value Framework

Stop selling GRC as time savings.

Start showing how it enables the business to achieve objectives, adapt to change and uncertainty, and act with integrity in an uncertain world.

The End Game: Business Confidence

grc 20/20
Bringing GRC into Focus

Thank You!
Questions?

Michael Rasmussen, The GRC Pundit & Analyst

RISK IS OUR BUSINESS
grc report

- GRC 20/20 Research • www.**GRC2020**.com
- News • The GRC Report • www.**GRCreport**.com
- Podcast • Risk Is Our Business Podcast
- Podcast • Hitchhiker's Guide to the GRC Technology Galaxy
- mkras@grc2020.com • www.linkedin.com/in/mkrasmussen/