The Assurance Mandate

Moving Beyond GRC to Evidence-Based Operational Resilience

A Whitepaper for Boards and Executives

Author:
David M. Nichols
DVMS Institute

Date:
October 2025

About this Whitepaper

Boards and executives today operate in an environment characterized by volatility, uncertainty, complexity, and ambiguity. Traditional measures of progress, such as certifications, maturity scores, and audit reports, have helped organizations develop discipline and show accountability. However, as recent disruptions demonstrate, these artifacts provide reassurance but not the confidence that stakeholders now demand.

This white paper, drawn from the LinkedIn Assurance Mandate Series, advocates for the next stage of governance maturity: transitioning from Governance, Risk, and Compliance (GRC) to Governance, Resilience, and Assurance (GRA). This isn't a rejection of GRC but rather an evolution. GRC has provided organizations with a foundation; GRA builds on that foundation to meet the needs of a digital, always-on, disruption-prone world.

The goal is to equip leaders with clarity, evidence, and a systemic approach to protect stakeholders, build trust, and ensure that organizations can continue to create, safeguard, and deliver digital business value under stress. GRA offers an opportunity for boards and executives to shift from reactive compliance to proactive assurance, transforming resilience into a measurable, strategic advantage.

Executive Summary

Boards and executives have made significant progress in governance over the past twenty years. Certifications, maturity scores, and audit reports have established a common language of accountability and improvement. These efforts were worthwhile; they set the stage for discipline and regulatory trust.

But the world has changed. Today's digital business landscape is characterized by constant volatility, systemic interconnection, and an unprecedented pace of disruption. What provided reassurance yesterday no longer suffices to inspire confidence today.

This marks the next phase in the governance journey, where Governance, Resilience, and Assurance (GRA) play a key role. Unlike Governance, Risk, and Compliance (GRC), which confirms that practices are in place, GRA offers forward-looking proof that an organization can continue to create, protect, and deliver value under pressure. Where GRC helped organizations mature, GRA helps them thrive.

The Digital Value Management System (DVMS) drives this progress. It provides a framework to link governance intent with operational capabilities and generate assurance evidence instantly. With advancements in AI and agent-based systems, the long-standing "burden of assurance" — the effort required to gather, analyze, and interpret data across complex organizations — is no longer a hurdle. Assurance can now be automated, continuous, and adaptable, providing boards and executives with a live view of resilience instead of static snapshots.

This whitepaper, drawn from the Assurance Mandate Series of LinkedIn articles, argues that boards and executives must lead this transition. It explores:

- Why compliance artifacts, while valuable, cannot predict resilience.
- How frameworks provide structure but must be operationalized through systems.
- Why culture and collaboration, not just controls, determine outcomes.
- How DVMS, supported by AI-enabled assurance, creates a continuous improvement cycle that keeps organizations ahead of disruption.

The message is forward-looking:

- Compliance brought us here. Assurance will take us further.
- Frameworks provide the map. Systems create the journey.
- GRC gave comfort. GRA delivers confidence.

The mandate for boards is clear: build on what has been achieved, shift from reassurance to resilience, and lead the next phase in governance by establishing a system of assurance that turns uncertainty into strength.

Introduction

Over the past twenty years, Governance, Risk, and Compliance (GRC) has effectively supported organizations. It established structure, fostered accountability, and assured boards that risks were under control. Certifications and audits built a foundation of trust with regulators, customers, and shareholders. These achievements should not be overlooked—GRC professionalized governance.

However, the digital age has brought new challenges that GRC alone cannot fully handle. Disruption is no longer a rare event; it is a constant aspect of interconnected supply chains, evolving cyber threats, and changing regulations. In this climate, reassurance isn't enough. Boards and leaders must be confident that their organizations can adapt, recover, and continue to provide value—even when disruptions are at their worst.

High-profile events have made this clear. The SolarWinds supply chain breach in 2020, the Colonial Pipeline ransomware attack in 2021, and the Snowflake breach in 2024 all followed a similar pattern: on paper, the organizations appeared to be compliant. They held certifications, passed audits, and maintained maturity scores. But when tested by disruption, those artifacts proved insufficient.

The lesson isn't that GRC failed; instead, it shows that GRC has reached its limit. It reassures us that processes are in place, but it doesn't prove whether those processes will succeed under pressure. It tells us what was true yesterday, but not what will be true tomorrow.

This is where Governance, Resilience, and Assurance (GRA) come into play. GRA builds on the strengths of GRC, pushing governance into the future. It ensures that resilience, the ability to continue creating, protecting, and delivering value during disruptions, is the standard of success. Assurance provides evidence, not just documents and reports, but real-time proof that the system is functioning effectively.

The timing for this evolution couldn't be better. Progress in AI and agentic systems is eliminating the historical burden of assurance, the meticulous work of gathering and analyzing evidence across different areas. What once seemed too expensive and complicated can now be automated and done continuously. Boards no longer need to wait for quarterly reports; they can access real-time, forward-looking evidence of resilience.

This paper examines why boards need to shift from GRC to GRA and how the Digital Value Management System (DVMS) offers an operating model to make that transition a reality. It's not about replacing what existed before but about building on it — from good to great, from reassurance to resilience, from compliance to confidence.

1. The Illusion of Compliance

For decades, boards and executives have depended on certifications, audits, and maturity reports as a quick way to show security and resilience. These artifacts are tangible, easy to include in board packets, and widely accepted by regulators. They reassure stakeholders that the organization has "done the right things."

But as recent history shows, this reliance often fosters a dangerous illusion: compliance artifacts may indicate order, but they do not ensure capability.

SolarWinds: Certified, but Compromised

When SolarWinds was compromised in 2020, it was not a minor, little-known vendor. Its Orion software was utilized by thousands of organizations, including U.S. federal agencies and numerous Fortune 500 companies. However, attackers managed to infiltrate the supply chain — embedding malicious code into updates that were later distributed as legitimate patches.

According to Holland & Knight, TechTarget, and Tech Talkies, the intrusion remained undetected for months before being discovered. For many victims, the first sign of compromise did not come from their own systems but from public disclosures. Although SolarWinds boasted industry certifications and compliance with many cybersecurity standards, none of that prevented a disastrous failure that spread through government and industry.

The lesson is clear: certifications show SolarWinds had controls in place. However, certifications cannot prove that those controls were sufficient, adaptable, or resilient against a skilled adversary.

Snowflake: Trusted, but Exposed

Similarly, in 2024, Snowflake — a trusted cloud data platform used by major enterprises — experienced a breach that exposed customer environments. Reports indicate that over 160 customer accounts were compromised, resulting in the theft of sensitive data from organizations such as AT&T, Ticketmaster, and Advance Auto Parts.

According to BleepingComputer, SecurityWeek, and the Cloud Security Alliance, many of the affected environments were deemed "secure" based on current industry standards and regulations. Customers had adhered to these standards, implemented prescribed configurations, and trusted the credibility of a vendor widely endorsed by analysts. However, when attackers exploited vulnerabilities in access controls and identity management, resilience faltered.

On paper, Snowflake followed best practices. In practice, the breach revealed that compliance offered reassurance but not absolute confidence.

Why Compliance Fails as Assurance

These incidents are not isolated; they are part of a pattern. Verizon's annual Data Breach Investigations Report consistently shows that many breaches happen in organizations that were already certified, audited, or considered compliant with recognized frameworks. Similarly, the U.S. Government Accountability Office (GAO) has repeatedly pointed out that federal agencies aligned with the NIST Cybersecurity Framework still fail to properly manage basic risks, such as identity and access management ("Federal Information Security: Agencies Need to Strengthen Practices to Address Increasing Cybersecurity Risks," December 2020).

The reason is simple: compliance artifacts measure alignment, not adaptability.

- **Certifications** tell you that controls exist, not that they work under pressure.
- **Audits** confirm that processes were followed, but only at a moment in time.
- **Maturity scores** indicate how many boxes have been checked, not whether systems, people, and culture can adapt when conditions change.

Compliance looks backward. It shows what has been accomplished. Assurance must look forward. It demonstrates what the organization is capable of when it matters most.

Why Leaders Gravitate to Compliance

If compliance is such a poor proxy for resilience, why do boards and executives rely on it?

The key is in governance habits. Certifications and audit reports are transparent, comparable, and defensible. They turn complexity into a single number or badge. They also offer plausible deniability; "we were certified" sounds responsible in hindsight. Regulators often see them as proof of due diligence. Analysts rank organizations based on their compliance maturity, which reinforces the notion that certification is a measure of competence.

In this way, compliance artifacts are appealing not because they demonstrate resilience, but because they are simple to understand and communicate. They give the impression of control in an environment characterized by volatility, uncertainty, complexity, and ambiguity.

The Leadership Risk

For boards, the risk is obvious. When directors rely on compliance artifacts as proof of resilience, they risk managing based on appearances instead of results. This makes organizations vulnerable in two ways:

1. **False confidence** – believing the organization is secure when in fact it may only have been lucky.
2. **Strategic blindness** – focusing governance discussions on audit scores and maturity rankings instead of resilience evidence and operational performance.

As a result, boards might praise themselves for progress, even though the organization stays fragile.

From Illusion to Assurance

The SolarWinds and Snowflake breaches reveal the core issue: compliance might show that an organization follows good practices, but it doesn't prove the organization can withstand disruption.

Compliance records the past. Assurance protects the future.

For boards and executives, the mandate is to stop equating certifications with capability. They must demand evidence that systems, people, and culture will withstand stress. Without this shift, governance will remain an illusion, and organizations will stay one disruption away from failure.

2. Frameworks Are Maps, Not the Territory

The cases of SolarWinds and Snowflake demonstrate how organizations can appear resilient through certifications, audits, and maturity scores, yet still fail to demonstrate their ability to manage disruptions. The same issue applies to how boards and executives rely on frameworks like ISO 27001, the NIST Cybersecurity Framework (CSF), ITIL, or COBIT.

Frameworks remain essential. They condense decades of lessons, offer structure to complex issues, and create a shared language across industries. They have raised the conversation around risk and governance, giving directors and regulators a way to measure progress and build confidence. But frameworks alone do not create resilience. They are maps, not the actual terrain; progress requires walking the ground.

The Comfort of Frameworks

Boards naturally prefer frameworks because they are familiar, trusted, and easy to communicate. They represent maturity to regulators, auditors, and customers. When an organization references alignment with these frameworks, it reassures stakeholders that it follows global best practices.

This sense of comfort is not minor. Frameworks help organizations feel in control. They offer predictability, benchmarks, and defensibility in governance discussions. They enable executives to say, “We’ve adopted NIST,” or “We’re ISO certified,” as proof of diligence. However, comfort does not always translate to capability.

The 2017 Equifax breach serves as a warning. The company had adopted frameworks like PCI-DSS and passed its audits. However, a single unpatched vulnerability enabled attackers to access over 140 million consumer records. The framework was in place, but the discipline to implement it effectively in real time was missing.

Frameworks supply the map; resilience demands the journey.

Maps vs. Journeys

A map shows terrain, landmarks, and routes. But having a map isn’t the same as reaching your destination. Progress needs movement, adaptation, and the experience of traveling.

The same holds for resilience. Certification under ISO 27001 or alignment with NIST CSF is helpful, but it only indicates that the map exists. Unless those frameworks are incorporated into an active system of governance, workflows, and evidence of assurance, they stay abstract. Too often, organizations celebrate having the map as if the journey is finished.

Compliance becomes the goal, rather than a means to achieve capability. The illusion of resilience grows stronger when organizations mistake artifacts — such as documents, policies, and certificates — for evidence of performance under pressure.

Why Frameworks Fall Short

The shortcomings lie not in the frameworks themselves, but in how organizations depend on them. Three limitations stand out:

1. **Frameworks are retrospective.** They show alignment at a point in time but do not prove adaptability to new conditions. A high maturity score last quarter is not evidence that the organization is ready for tomorrow’s disruption.
2. **Frameworks are siloed.** ISO, NIST, ITIL, and COBIT each address part of the challenge. But resilience requires integration across functions and disciplines. Without a system to unify them, frameworks create fragmentation instead of synergy.
3. **Frameworks are passive.** They describe what should be done, but do not ensure it is done. Culture and accountability determine whether frameworks are implemented in practice or remain merely as checklists to satisfy auditors.

As Gartner noted in its 2022 Board of Directors Survey, 88% of boards now consider cybersecurity a business risk rather than just an IT problem. However, most still gauge progress by framework adoption instead of assurance evidence. This reveals a significant gap: frameworks set expectations, but resilience depends on actual performance.

The Leadership Trap

Why do executives fall into this trap? For the same reason, they rely on compliance artifacts: frameworks make complexity simpler. They transform chaos into structured models, providing executives with language they can justify and that regulators will accept. But this dependence risks confusing adoption with assurance.

Boeing's 737 MAX crisis highlights this dynamic beyond cybersecurity. Certification processes were followed, but cultural pressures undermined honesty and safety practices. Compliance was met; resilience was lacking.

Frameworks can become another form of illusion if they are viewed as final points instead of parts of an ongoing process.

From Frameworks to Systems

If frameworks are maps, resilience requires an operating system that brings those maps to life. Systems thinking is the missing ingredient. Frameworks provide guidance, but only a system ensures that intent is turned into action, and that action is translated into evidence of assurance.

This is where the Digital Value Management System® (DVMS) comes in. DVMS doesn't replace frameworks; it makes them work in real life. It transforms alignment into practical action by connecting governance goals, operational processes, and assurance results into a seamless cycle. Frameworks show the destination; DVMS makes sure the journey actually happens.

The challenge of building assurance has traditionally made this transition tough. Gathering, analyzing, and reporting evidence has required many resources. However, emerging technologies, including AI and agentic systems, are starting to reduce this challenge. They can automate evidence collection, track workflows in real time, and identify differences between "fit for use" and "fit for purpose." For the first time, the potential to move beyond reactive GRC into proactive GRA can be scaled up.

The Executive Imperative

For today's boards, the lesson is not to abandon frameworks, but to see them as necessary yet incomplete. They are essential tools, but they do not stand alone as proof of resilience.

The key question is no longer, 'Which frameworks have we adopted?' The right question is, 'How are our frameworks integrated into a system that demonstrates performance under stress?'

By viewing frameworks as starting points instead of endpoints, boards can shift from comfort to confidence, and from good to great.

3. Silos Weaken Resilience

Organizations may have controls in place and even align with the right frameworks, but when governance, operations, and cybersecurity remain isolated in separate domains, resilience suffers. Silos don't just slow information flow; they distort accountability, create response gaps, and prevent leaders from seeing the whole picture.

Lost in Translation

Boards and executives are used to hearing from three distinct roles: the Chief Information Security Officer (CISO), the Chief Information Officer (CIO), and the Chief Risk or Compliance Officer. Each uses its own language: cybersecurity focuses on threats and vulnerabilities, IT emphasizes uptime and efficiency, and compliance revolves around audit readiness.

Individually, each report appears impressive. However, when viewed together, they often give an incomplete picture. A board might hear that compliance scores are strong, uptime is high, and threats are managed, and still be caught off guard when disruption occurs.

The 2017 Equifax breach clearly demonstrates this problem. The company had adopted established frameworks, passed multiple audits, and received positive reports. However, because risk, IT, and cyber departments operated independently, a critical patch notification was not addressed promptly. A known vulnerability remained unpatched for months, leading to the compromise of over 140 million consumer records (U.S. House Committee on Oversight and Government Reform, The Equifax Data Breach, December 2018). Each department believed it was meeting its responsibilities, but the lack of coordination turned a preventable issue into a catastrophic failure.

When Silos Become Blind Spots

The danger of silos isn't just inefficiency; it's blind spots. Critical information in one area may never reach another.

- A cyber team may detect repeated phishing attempts but fail to escalate the business impact to operations or governance.

- IT may notice rising downtime incidents but not connect them to governance concerns about business continuity.
- Compliance may highlight repeat audit findings but frame them as documentation issues rather than systemic weaknesses.

Resilience relies on the whole system working together. When governance, operations, cybersecurity, and culture don't support each other, vulnerabilities grow.

The 2021 Colonial Pipeline ransomware attack is a clear example. Technical safeguards were in place, but cyber was still considered just "IT's problem." Business continuity governance did not fully incorporate cyber risk. When the disruption occurred, executives lacked a comprehensive view to direct a response. What could have been a regional incident turned into a national crisis.

MOVEit: A Supply Chain Failure Across Silos

The 2023 MOVEit breach highlights how siloed thinking can increase risk in a connected world. A zero-day flaw in MOVEit, a widely used file transfer program, enabled hackers to steal data from hundreds of organizations, including U.S. federal agencies, banks, universities, and multinational corporations.

On paper, many of the impacted organizations had robust cyber programs, effective compliance processes, and well-managed vendor relationships. However, gaps between different teams persisted: vendor risk teams concentrated on contracts and certifications, IT handled patching schedules, and governance depended on third-party attestations. None of these silos alone could guarantee that critical software dependencies were continuously monitored and secured.

The lesson from MOVEit is clear: resilience requires more than checklists and isolated oversight. It calls for integrated governance that connects vendor risk, IT operations, and cyber monitoring into a unified feedback loop. Without integration, vulnerabilities can bypass oversight and quietly spread across industries.

The Cost of Fragmentation

Silos not only create operational risks — they also weaken governance at the board level. Directors often only see silo outputs: compliance reports, IT uptime metrics, and cybersecurity dashboards. Each artifact offers a part of the puzzle, but none connect the dots.

A 2022 World Economic Forum report on cyber governance warned that boards "often struggle to receive integrated reporting across risk, cyber, and operations," noting that fragmentation can give directors a false sense of security. Gartner's 2022 Board of Directors survey reached a

similar conclusion: while 88% of boards now recognize cyber as a business risk, most still review reporting framed only in technical or compliance terms.

The result is governance by fragments, not governance by assurance.

Why Leaders Tolerate Silos

Why do silos persist? Partly because specialization is necessary. Each domain, cyber, IT, and compliance, involves expertise that is hard to translate across functions. Cyber dashboards are highly technical; IT metrics focus on operational efficiency, and regulations drive compliance reports. Keeping them separate often seems more straightforward.

But simplicity comes with its risks. By allowing silos to persist, leaders may overlook issues that only become clear during disruptions. Metrics that seem strong on their own can hide systemic flaws. Silos might offer comfort, but they don't help build capability.

Breaking Down Silos

The way forward isn't to eliminate silos but to unify them. While specialization will always be necessary, integration ensures that governance goals, operational actions, and proof of assurance are aligned. Boards don't need three separate dashboards; they need a single, integrated view showing whether the organization as a whole can endure disruption.

This is precisely the role of the Digital Value Management System® (DVMS). As detailed later in this paper, DVMS does not replace frameworks or functions. Instead, it acts as the operating system that binds them together. In a DVMS model, the board no longer sees disconnected compliance reports, IT metrics, and cyber dashboards. Instead, it assures that resilience is being demonstrated across various domains.

A Forward-Looking Imperative

Breaking down silos is no longer optional; it's the next step in organizational maturity. GRC and frameworks helped organizations establish essential practices, but in today's volatile digital environment, they are not enough on their own.

Emerging technologies, such as AI and agentic workers, emphasize this point. When automation operates in isolation, it can lead to greater fragmentation. When integrated into a system like DVMS, AI improves assurance by providing real-time evidence and predictive insights across governance, IT, and cybersecurity.

For boards and executives, the clear imperative is to stop managing in silos. Require comprehensive assurance. Don't just ask whether cyber, IT, or compliance has met the requirements; demand proof that they are collaborating effectively in real-time.

The key question is this: *Are we seeing the entire system, or just its parts?*

Until silos are unified into a single operating model, resilience will stay fragile. When integrated through DVMS, they form the foundation for confidence.

4. Culture Eats Controls for Breakfast

Peter Drucker's famous phrase, *"Culture eats strategy for breakfast,"* remains as relevant as ever in the digital age, but with a twist. Today, culture doesn't just undermine strategy; it can also weaken controls. Organizations may have frameworks, certifications, and technical dashboards in abundance, yet if the culture resists accountability, discourages escalation, or values appearances over honesty, resilience will break down at the very moment it is most needed.

Why Culture Gets Ignored

Boards and executives naturally prefer measurable data. Compliance scores, patch rates, maturity levels, and audit results are tangible; they can be tracked, benchmarked, and presented clearly and concisely. Culture, by contrast, is intangible. It is more challenging to determine whether employees feel secure in reporting vulnerabilities, whether managers reward transparency or penalize it, or whether teams promptly escalate problems.

Because culture is difficult to measure, it often takes a back seat in governance discussions. Yet, ironically, culture frequently influences the effectiveness of controls more than the controls themselves. A perfectly designed policy fails if the culture tolerates delays. A sophisticated crisis plan fails if escalation is discouraged. A compliance audit becomes meaningless if passing the test becomes the goal instead of building true resilience.

Case 1: Boeing — Compliance Without Candor

The Boeing 737 MAX disasters demonstrate this reality beyond cybersecurity. Boeing's aircraft program met regulatory standards and got certifications. On paper, they were compliant. However, the company's culture — one that prioritized deadlines and shareholder profits over engineering safety — weakened safety.

Engineers who raised red flags were marginalized. Issues were reclassified as documentation problems rather than design risks. The culture of silence turned safety rules into empty rituals. Certification was in place, but honesty was lacking. The result was tragic crashes, lost lives, reputational damage, and billions in shareholder value wiped out.

Case 2: Equifax — The Patch That Culture Ignored

The 2017 Equifax breach, discussed earlier, was not due to a lack of frameworks. The company adhered to multiple standards and passed audits. The technical vulnerability was known, and a patch was available. However, the organizational culture viewed patching as a routine compliance task rather than a matter of urgency and accountability.

The vulnerability stayed open. Attackers took advantage of it. Over 140 million consumer records were compromised. The control was in place, but the culture decided if it was enforced with discipline.

Case 3: Colonial Pipeline — Cyber as "IT's Problem"

Similarly, the 2021 Colonial Pipeline ransomware attack was not caused by a lack of cybersecurity tools. Technical controls were in place. The problem was cultural: cyber was viewed as a technical silo, rather than a governance or business continuity issue.

When ransomware struck, the culture hadn't promoted escalation, cross-functional rehearsals, or systemic awareness. Leadership was unprepared. What could have been managed as an IT incident escalated into a nationwide supply disruption. The controls existed, but the culture viewed them as someone else's responsibility.

DVMS: Making Culture Visible

What unites Boeing, Equifax, and Colonial Pipeline is not the lack of frameworks or tools. Each organization had them. What failed was culture. Rules, patches, and controls existed — but the prevailing culture kept them from being effective.

This is where the Digital Value Management System® (DVMS) offers a different approach. In "Thriving on the Edge of Chaos" and the "Practitioner's Guide to Building Cyber-Resilience" (Second Edition), DVMS is not presented as just another framework, but as a system overlay that makes culture visible.

- If a policy is ignored, assurance evidence exposes the gap.
- If a risk is escalated, governance captures it as proof of resilience.
- If controls fail, feedback loops show whether the culture corrected the issue or buried it.

Through this systemic connection of governance intent, operational workflows, and assurance evidence, DVMS transforms culture from a vague background factor into an observable, manageable aspect of resilience. Boards can oversee culture with the same rigor they apply to financial performance.

The Executive Imperative

For boards and executives, the lesson is clear: don't just oversee controls, cultivate the culture that makes controls effective.

Key questions to ask include:

- Do our audits measure whether employees escalate risks, or only whether they document them?
- Can we prove that our culture reinforces accountability, or do we assume it does?
- When disruption occurs, will our people adapt responsibly, or will they conceal problems and delay action?

Until boards demand evidence of culture in practice, resilience will remain fragile.

Closing the Gap

Controls can be copied. Frameworks can be adopted. Technology can be purchased. But culture must be lived and governed, and too often, it isn't.

The difference between resilience and fragility often depends not on the existence of controls but on the culture that drives them. Boeing's engineers were silenced. Equifax's patch was ignored. Colonial Pipeline's cyber risk was overlooked. In each case, culture determined whether controls were adequate.

DVMS bridges this gap by incorporating culture into governance as a visible, measurable, and actionable element. It shifts leadership from governing by appearances to governing based on evidence.

The mandate for boards is straightforward: demand assurance not only of controls but also of the culture that upholds them. Culture will always overshadow controls. Leaders' challenge is to ensure it becomes a source of strength rather than a vulnerability.

5. DVMS as a Journey, Not a Big Bang

Executives are often familiar with large-scale transformation projects. These initiatives usually follow a familiar pattern: announce the program, allocate funding, implement the tool, celebrate milestones, and eventually announce success. They have starts, middles, and finishes that can be easily tracked and reported to stakeholders.

But resilience does not follow that script. You cannot "install" it. You cannot buy it off the shelf. Resilience is not a project with a ribbon-cutting ceremony at the end; it is a discipline, cultivated over time through deliberate practice and incremental improvement.

The Myth of the Big Bang

In governance discussions, there is often an implicit expectation that resilience can be achieved through a single decisive act. Executives may believe that implementing ISO 27001, aligning with NIST CSF, or completing a digital transformation program will somehow deliver resilience all at once.

The reality is different. Frameworks, certifications, and even cultural initiatives offer comfort but not confidence. They are helpful starting points, but they do not ensure that the organization can survive a disruption. Resilience is not the result of a single project. It is the outcome of a continuous process that combines governance, operations, and assurance into an ongoing system.

This distinction is vital because organizations that see resilience as a one-time achievement risk becoming complacent. Once they earn the certificate or pass the audit, their motivation declines, and the effort to develop lasting capabilities often falls short.

Why DVMS Must Be Understood as a Journey

The Digital Value Management System® (DVMS), as explained in Thriving on the Edge of Chaos and the Practitioner's Guide to Building Cyber-Resilience (Second Edition), is not just another framework to add to the collection. Instead, it functions as the operating system that unifies existing frameworks, governance intent, and assurance into a dynamic cycle.

Since it is systemic, DVMS cannot be implemented all at once. It develops gradually, evolving in tandem with the organization. The process starts small by connecting governance goals to a few workflows and generating the initial set of assurance evidence. Over time, DVMS spreads throughout the enterprise, integrating resilience into everyday practices until it becomes the organization's default way of operating.

The goal is not to "achieve DVMS" as a fixed milestone. The aim is to embed resilience into the organizational DNA so that with every governance cycle, resilience becomes more substantial and more evident.

Small Steps, Real Outcomes

Boards sometimes hesitate to embark on systemic change because they fear it requires massive, disruptive effort. But DVMS demonstrates that resilience can be built incrementally, with each step yielding visible value.

Consider what organizations can achieve early in the journey:

- **Incident Response Evidence**: Instead of simply reporting patch counts or compliance charts, a board can review assurance evidence that shows how quickly critical services were restored during the last disruption. That shift demonstrates organizational capability, not just adherence to policy.
- **Continuity Reframed**: A company that once defined success by certification can now prove that its supply chains continued operating despite disruption. The certificate still matters, but evidence of continuity provides a far stronger basis for stakeholder trust.
- **Cultural Reinforcement**: Early application of DVMS reveals whether teams escalate risks in practice or bury them. This feedback loop makes culture visible and governable, ensuring that resilience is not undermined by silence or avoidance.

These are not revolutionary leaps. They are gradual steps that create new habits. Over time, those habits become norms. Eventually, resilience becomes something the organization naturally exhibits, not just a project result, but an integral part of its identity.

Why This Matters for Boards

The journey mindset changes the questions boards should ask. For too long, the primary governance question has been: When will we be compliant? That framing is outdated.

The more critical and forward-looking question is*: Where are we on the journey from artifacts to assurance?*

If a governance report still relies on certifications, maturity scores, or analyst rankings, then the organization is governing by appearances. If the report shows evidence that systems, people, and culture can withstand stress, then the organization is governing with confidence.

This shift requires directors to view resilience as a continuous practice rather than a final goal. Oversight should not only celebrate isolated milestones but also demand ongoing evidence of progress.

The Executive Imperative

For executives and boards, the clear imperative is that resilience isn't built in a single moment. Instead, it is gained over time by consistently integrating governance, capabilities, and assurance.

Directors should ask:

- *Are we stronger today than we were last quarter?*
- *Can we demonstrate resilience in critical workflows, not just in audit reports?*
- *Do we have forward-looking assurance that our systems will hold under pressure?*

These questions focus oversight on meaningful outcomes. They go beyond reassurance and require proof.

Closing the Gap

Controls can be copied. Frameworks can be adopted. Culture can be declared. But resilience must be lived, reinforced, and proven every day.

DVMS provides the framework for that proof. It turns resilience from a static goal into an ongoing practice. By incorporating incremental innovation into organizational capabilities, DVMS guarantees that the organization is not one disruption away from failure, but one cycle stronger each time it adapts.

For boards and executives, the rule is simple: resilience isn't a final goal; it's an ongoing process. The only way to manage that process is to demand and provide assurance, step by step.

Luck runs out. Systems endure. The journey to resilience starts where you are and continues every day.

6. From GRC to GRA: A New Mandate for Boards

The earlier sections of this paper highlighted the strengths and limitations of today's governance practices. Compliance artifacts, such as certifications and audits, as seen with SolarWinds and Snowflake, offer reassurance but not resilience. Frameworks such as ISO and NIST-CSF provide helpful guides, but are not the journey itself. Silos across governance, IT, and cyber fragment accountability, and culture — though difficult to measure — often determines whether controls succeed or fail.

Taken together, these lessons highlight an apparent reality: Governance, Risk, and Compliance (GRC), the model that has shaped oversight for the past twenty years, has reached its limits. It was a significant step forward at the time. GRC helped organizations establish discipline, identify risks, standardize controls, and document compliance. In a relatively stable environment, this represented progress: boards could demonstrate diligence, regulators could assess consistency, and organizations could compare themselves to peers.

But the world has changed. Today's environment is characterized by volatility, uncertainty, complexity, and ambiguity. Disruption is no longer rare; it is now a constant occurrence. Emerging technologies, from AI-driven business models to digitally connected supply chains, generate both opportunities and risks at an unprecedented pace. In this context, GRC alone is no longer enough. To shift from reassurance to confidence, boards must adopt a new model: Governance, Resilience, and Assurance (GRA).

Why GRC Falls Short

At its core, GRC believes that documenting risks and controls offers assurance. It creates artifacts, audit reports, compliance scores, and risk registers that show diligence but not capability. These artifacts reassure stakeholders yet leave boards without the forward-looking evidence they need most: Can we withstand disruption tomorrow?

Consider the limitations:

- Controls are fragile. They may work under expected conditions but often fail when crises or adversaries shift the environment. GRC equates existence with success.
- Audits are retrospective. They confirm what was done in the past but reveal nothing about how the organization will adapt in the future.
- Risk registers are static. They freeze threats in time even as technologies, business models, and attacker tactics evolve daily.
- Maturity models can mislead. They reward breadth of documentation over depth of resilience. Organizations may appear "advanced" on paper, yet collapse under stress.

In short, GRC provides evidence of due diligence, not proof of resilience. Certifications may enable boards to assert oversight, but when put to the test in practice, they often do not ensure continuity.

From GRC to GRA

The shift from GRC to GRA isn't a rejection of the past but an evolution. GRC established a foundation of discipline; GRA builds on that base to foster adaptability.

Governance remains the foundation, but is redefined. In GRA, governance is not bureaucracy for its own sake but clarity of intent. Boards set resilience outcomes as strategic priorities and ensure that decisions align with those outcomes.

Resilience now replaces "risk" as the main guiding principle. Risks can be listed endlessly, but resilience decides whether those risks weaken or strengthen the organization. It is measured not by the absence of disruptions, but by how well it can adapt, recover, and continue to provide value under stress.

Assurance replaces "compliance" as the proof point. Compliance confirms that requirements were met at a point in time. Assurance provides future-oriented evidence that systems, people, and culture can perform under pressure.

This reframing alters the board's role. Directors are no longer just reviewers of policies and scorecards but overseers of a living system that shows resilience in action.

DVMS: Operationalizing GRA

The Digital Value Management System® (DVMS) is the operating system that brings GRA to life. As described in Thriving on the Edge of Chaos and the Practitioner's Guide to Building Cyber-Resilience (Second Edition), DVMS does not replace frameworks like NIST CSF or ISO 27001. Instead, it overlays them, aligning governance intent with the Minimum Viable Capabilities (MVC) needed to create, protect, and deliver digital business value.

This overlay identifies capability gaps, prioritizes improvements, and ensures that every control, process, and cultural behavior supports governance outcomes. By embedding the QO–QM (Question Outcome–Question Metric) model, DVMS connects fit-for-purpose outcomes with fit-for-use measures. The result is assurance evidence that links policy intent with operational reality.

Instead of examining fragmented artifacts, boards using DVMS view integrated evidence: recovery metrics, escalation behaviors, continuity performance, and cultural indicators. Assurance becomes tangible, real-time, and forward-looking.

Implications for Boards

For boards, adopting GRA changes both mindset and practice:

Board conversations evolve. Directors move from asking *"Are we compliant?" to asking "Can we demonstrate resilience under stress?"*

Oversight deepens. Rather than reviewing artifacts of past performance, boards evaluate evidence of adaptability, continuity, and recovery.

Fiduciary duty is expanding. In a world where digital trust supports enterprise value, boards can't fulfill their duty of care just by citing certifications. Protecting stakeholder value now means demanding proof of resilience.

The contrast is stark. In GRC, success is measured by passing audits. In GRA, success is measured by the ability to deliver value without interruption in the face of disruption.

A Positive Future

This transition is not about abandoning what has been built but expanding it. GRC established discipline; GRA broadens that discipline to address the demands of a digital and volatile era.

Importantly, advances in artificial intelligence and automation are removing traditional barriers to assurance. What once seemed burdensome, continuous monitoring, real-time reporting, and dynamic assurance, are now becoming achievable. With agentic AI systems and digital governance platforms, assurance at scale is finally within reach.

This means the "burden of assurance" that once discouraged boards from demanding evidence is easing. GRA is not only essential but more attainable than ever.

The Executive Question

The challenge for boards is no longer whether they can demonstrate compliance; it is whether they can demonstrate effective compliance. The real question is: *When disruption occurs, will we endure because we are strong, or merely because we were fortunate?*

With GRA, supported by DVMS, boards no longer have to rely on luck. They can shift from reassurance to confidence, from artifacts to certainty, and fulfill their duty to safeguard trust in the digital age.

7. DVMS: From Frameworks to an Assurance Operating System

If frameworks are maps, organizations still need a system that guides the journey. Resilience can't be built just through documents, audits, or certifications. It calls for a living, adaptable operating system that connects governance goals to operational capabilities and provides assurance evidence that boards and stakeholders can rely on.

This is the role of the Digital Value Management System® (DVMS): Not a Replacement, but an Overlay.

DVMS does not replace ISO 27001, NIST CSF, ITIL, or COBIT. Nor does it discard the progress organizations have already made with GRC disciplines. Instead, DVMS functions as an overlay, a unifying layer that ensures governance intent is translated into capabilities that can be executed, monitored, and evidenced across the enterprise.

Where frameworks prescribe "what good looks like," DVMS provides the operating system that ensures those frameworks are practiced consistently and integrated into daily decision-making. It turns static adoption into dynamic assurance.

- Frameworks describe expectations.
- DVMS operationalizes capabilities.
- Assurance emerges when the two are continuously connected**.**

The CPD Model at the Core

As explained in Thriving on the Edge of Chaos and the Practitioner's Guide to Building Cyber-Resilience (Second Edition), the DVMS is based on the Create, Protect, Deliver (CPD) Model. CPD provides the framework that guides all activities related to business value.

- **Create** digital business value through innovation and delivery of products, services, and experiences.
- **Protect** that value against threats, disruptions, and systemic risks.
- **Deliver** that value consistently to stakeholders, even under pressure.

Resilience exists only when organizations achieve all three simultaneously. CPD helps managers and executives reframe every policy, process, or initiative based on how it creates, protects, and delivers value.

Surfacing Gaps with Minimum Viable Capabilities (MVC)

The MVC overlay illustrates how DVMS implements policy. Managers compare current practices with the MVC, highlighting gaps that hinder the organization from achieving resilience. These gaps are viewed not as failures but as opportunities for small, innovative improvements.

For example:

- A policy might state, “Ensure customer trust is protected during disruption.”
- CPD frames this in business-value terms: service continuity must be created, protected, and delivered.
- MVC mapping may reveal that while incident response procedures exist, cross-functional escalation is weak or vendor continuity planning is absent.
- Managers then incrementally build those capabilities into workflows, rehearsals, and monitoring systems.

Over time, this cycle develops an integrated, non-siloed capability system — one that generates objective assurance evidence.

Assurance Through QO–QM

DVMS also embeds the **QO–QM (Question Outcome – Question Metric)** discipline. This closes the loop between governance intent and operational execution by asking:

- **QO:** What is the outcome the board requires (fit for purpose)?
- **QM:** What metrics prove the organization can achieve it (fit for use)?

For example, an outcome may be “restore services within four hours of disruption.” The metric serves as evidence of the mean time to recovery (MTTR). The difference—the delta between purpose and use—drives continuous improvement and innovation.

This is how DVMS ensures assurance is not a static artifact but a living feedback system.

Technology as an Enabler

Historically, executives have resisted demanding continuous assurance because they viewed the burden of data collection and reporting as too great. But with today’s progress in analytics, automation, and AI, assurance is now more feasible.

- Agentic AI workers can monitor workflows continuously, validate recovery benchmarks, and flag exceptions in real time.

- Automated dashboards can integrate IT, risk, and cyber metrics into a single view for the board.
- Machine learning can detect resilience gaps before they manifest in disruption.

DVMS uses these tools not to replace leadership but to support it — empowering managers to provide the evidence boards require without becoming overwhelmed by reporting demands.

The Strategic Advantage

The shift from GRC to GRA isn't about discarding the past but building upon it. GRC offered structure, discipline, and accountability. DVMS builds on that foundation to create a system that consistently demonstrates resilience.

Executives and managers alike gain confidence that their investments in frameworks and controls are genuinely practical, not just symbolic. Boards can communicate with stakeholders by providing proof of resilience, rather than merely offering reassurances of compliance.

In this context, DVMS is more than just a governance tool; it is a comprehensive solution. It is the assurance operating system that organizations require to succeed in an era of constant disruption.

8. From Burden to Opportunity: The Role of Assurance in Strategy

For years, executives have quietly acknowledged what some called the "burden of assurance." The traditional view was that assurance involved multiple layers of reporting, continuous audit cycles, and increasing demands from regulators and stakeholders. Assurance was viewed as a necessary expense of doing business, a compliance-driven burden that consumed time, money, and attention without providing clear value.

That mindset is beginning to shift.

From Defensive to Strategic

In reality, assurance is not a cost center. It is a strategic asset. Organizations that excel in assurance are not only better prepared for disruption but are also more trusted by customers, investors, regulators, and partners. Trust is the currency of the digital era, and assurance is how it is earned.

This is the transformation executives must adopt: shifting from viewing assurance as a duty to seeing it as an opportunity. Instead of considering assurance evidence merely as paperwork for

regulators, boards can begin to recognize it as proof that the strategy is effective. It shows not only that policies are in place, but also that they deliver resilience, continuity, and confidence in practice.

The Assurance Gap

The main challenge so far has been execution. Boards may require assurance, and managers might see the need to provide it, but the systems for collecting and validating assurance evidence were piecemeal, slow, and often backward-looking. By the time reports reached the boardroom, the data was outdated and disconnected from the current risk environment.

This delay strengthened the view of assurance as a burden. Executives often felt stuck in a cycle where they were judged by lagging indicators instead of being guided by forward-looking evidence.

Technology as a Catalyst

What changes the equation today is the rise of automation, analytics, and AI. Agentic AI systems, for example, can continuously monitor workflows, track recovery performance, and validate compliance with governance intent in real time. Instead of periodic snapshots, assurance becomes ongoing and adaptable.

- Automated monitoring can flag whether vendor dependencies are being tested in practice.
- Analytics can correlate IT uptime with customer trust metrics, linking operations to strategic outcomes.
- AI-enabled dashboards can provide boards with a single, integrated view of assurance evidence across risk, operations, and cyber domains.

This shift eliminates the traditional burden of assurance reporting. Instead of requiring extensive manual documentation, executives can focus on analyzing real-time evidence, asking better questions, and making proactive decisions.

Assurance as a Driver of Innovation

The most forward-thinking organizations are learning that assurance isn't just about showing resilience; it's about driving innovation. When gaps between "fit for purpose" and "fit for use" are identified through the DVMS QO–QM discipline, they become opportunities for capability innovation.

For example:

- A recovery drill may reveal that incident escalation lags across functions. That evidence doesn't simply satisfy an audit; it drives the design of new cross-functional workflows.
- Vendor assurance metrics may show weaknesses in continuity planning. That evidence informs contract redesigns and deeper integration with strategic suppliers.
- Customer-impact metrics during disruptions may show communication breakdowns. That evidence leads to investment in new engagement platforms or AI-enabled customer service.

In this way, assurance is no longer the final goal. It becomes the feedback loop that constantly enhances the organization.

Turning the Narrative

The main message for executives is clear: assurance is not a burden to manage; it's an opportunity to lead. Boards that view assurance as a proactive discipline will not only prevent disruption but also stand out in the marketplace.

Investors and regulators are increasingly demanding more than just compliance. They seek confidence that organizations can handle uncertainty and continue delivering value. Customers expect more than service availability; they want assurance that their trust remains intact. Employees require more than policies; they want proof that leadership decisions protect the future.

By redefining assurance as a strategic advantage, executives can shift the narrative from one of fear and obligation to one of leadership and opportunity.

The Executive Imperative

The question for leaders is no longer: *"How do we minimize the burden of assurance?"*
It is: *"How do we leverage assurance to strengthen trust, guide strategy, and accelerate innovation?"*

Organizations that effectively answer this question will not only survive disruption but will also thrive during it. This forms the core of the governance shift, from GRC to GRA, and DVMS is the system that enables this transformation.

About the author:

David is the Executive Director of the DVMS Institute (DVMS), where our mission is to help organizations of every size create, protect, and deliver (CPD) digital business value by operationalizing the NIST Cybersecurity Framework through the Institute's Digital Value Management System approach**.**

Our goal is to create a global community of operational resilience professionals who not only help develop adaptive, operationally resilient businesses but also contribute directly to the ongoing development of the NIST Cybersecurity Framework and the DVMS body of knowledge.

In his role, he collaborates with leading practitioners in **r**isk management, service management, cybersecurity, assurance, and executive leadership to develop industry-leading guidance, training programs, and certifications**.** These resources equip boards, executives, and practitioners to govern with confidence, build resilience into their operations, and demonstrate assurance in a digital-first business world.

His career foundation was established in the U.S. Navy submarine service, where he learned the realities of complex systems, the importance of precise teamwork, and the demands of high-pressure leadership. These early experiences shaped his approach to leadership in high-pressure, challenging environments. He later applied these lessons to civilian life, building a successful career in software development and IT service delivery, where he managed high-performance teams focused on providing essential capabilities.

He led the development of the APMG International-accredited DVMS programs and their certification offerings. This initiative, now widely adopted worldwide, enables organizations to quickly create and implement cybersecurity risk management strategies that meet the needs of executives, regulators, and auditors. The program has received certification from the UK's National Cyber Security Centre (NCSC). It is recognized as qualified training by the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA).

David co-authored "Thriving on the Edge of Chaos" with David Moskowitz, which has influenced the work we've done, helping organizations adopt a systems thinking approach to creating, protecting, and delivering digital business value to their stakeholders.

Today, he is focused on leading the Assurance Mandate: helping boards and executives go beyond just meeting compliance requirements to building evidence-based resilience. Through the DVMS Institute, he is committed to ensuring organizations can not only survive disruptions but also thrive in chaotic environments.