



**Cyber Resilience Professional  
Accredited Certification Training**

**Digital Value Management System® (DVMS)**

**Teaching Enterprise How to Govern, Assure, and  
Account for Operational Resilience in Complex,  
Living Digital Ecosystems**

[www.dvmsinstitute.com](http://www.dvmsinstitute.com)

[support@dvmsinstitute.com](mailto:support@dvmsinstitute.com)

# From Paper to Practice: Governing by Assurance (GRAA)

## The Governance Gap: Paper vs. Living Systems



## Traditional GRC vs. The GRAA Mandate

Traditional GRC	vs.	The GRAA Mandate
Focus: Artifact Collection		Focus: Evidence-Based Capability
Frequency: Periodic Reassurance		Frequency: Continuous Assurance
Logic: Are we compliant?		Logic: Can this system recover?

## The GRAA Mandate

### Defining the GRAA Model

Focuses on continuous assurance, tested capability, and evidence that travels.



### DVMS: The Operating Overlay

Digital Value Management System monitors boundaries where risk and value concentrate.



### Culture as a Control Surface

Managing behaviors the system rewards—like escalating bad news early versus hiding it.



## From Paper to Practice – Why Enterprises Must Govern, Assure, and Account for Operational Resilience in Their Living Digital Ecosystem

### Explainer Video – Governing By Assurance

Despite an abundance of frameworks, metrics, and dashboards, many leaders still lack a clear line of sight into how their digital value streams perform when conditions deteriorate.

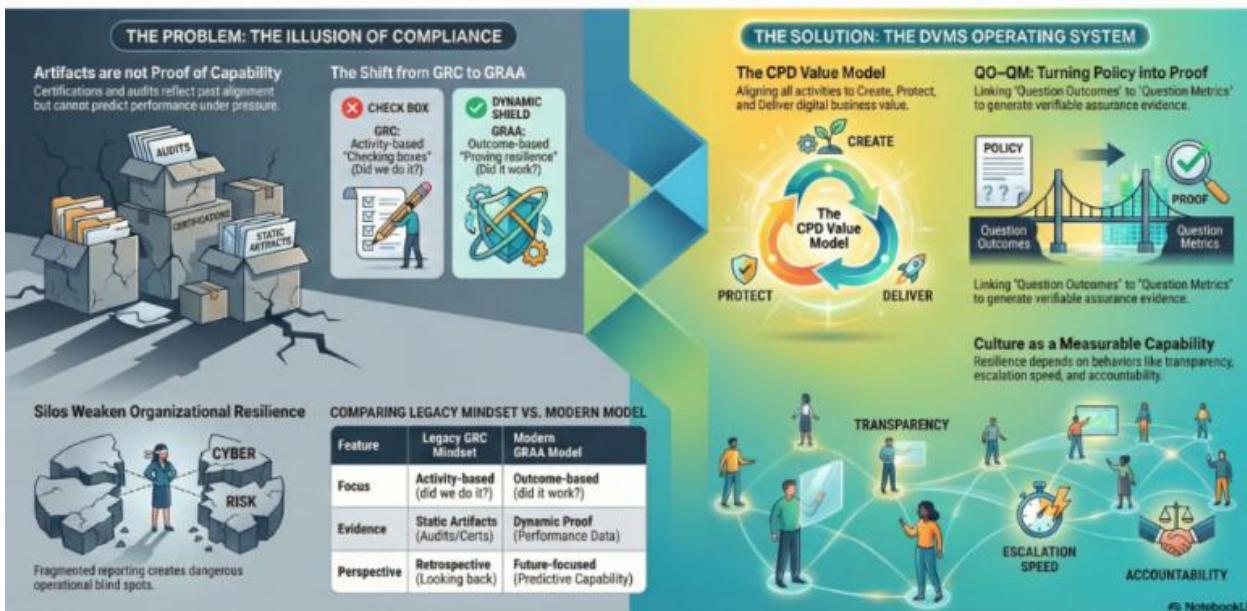
Strategic intent, organizational structures, and day-to-day behaviors are evaluated separately, producing static snapshots that fail to reveal how decisions, dependencies, and human actions interact within a dynamic digital system.

The result is governance that appears comprehensive in documentation yet proves fragile under pressure, leaving leaders to reconcile disconnected controls rather than systematically strengthen resilience.

What is needed is a framework-agnostic operating overlay that enables operational resilience to be governed, assured, and accounted for coherently across complex, living digital ecosystems.

## The Assurance Mandate: From Compliance Rituals to Evidence-Based Resilience

SHIFTING FROM "CHECKING BOXES" TO PROVING CAPABILITY WITH THE DIGITAL VALUE MANAGEMENT SYSTEM (DVMS)



## DVMS Institute White Papers - The Assurance Mandate Series

### Explainer Video – From Compliance Rituals to Evidence-Based Resilience

The whitepapers below present a clear progression from compliance-driven thinking to a modern system of Governance, Resilience, Assurance, and Accountability (GRAA). Together, they define an evidence-based approach to building and governing resilient digital enterprises.

[\*\*The Assurance Mandate Paper\*\*](#) explains why traditional compliance artifacts offer reassurance, not proof, and challenges boards to demand evidence that value can be created, protected, and delivered under stress.

[\*\*The Assurance in Action Paper\*\*](#) shows how DVMS turns intent into execution by translating outcomes into Minimum Viable Capabilities, aligning frameworks through the Create-Protect-Deliver model, and producing measurable assurance evidence of real performance.

[\*\*The Governing by Assurance Paper\*\*](#) extends this model to policy and regulation, positioning DVMS as a learning overlay that links governance intent, operational capability,

and auditable evidence—enabling outcome-based governance and proof of resilience through measurable performance data.



## The Digital Value Management System® (DVMS)

[Explainer Video – What is a Digital Value Management System \(DVMS\)](#)

The DVMS is an overlay management system that governs, assures, and accounts for operational resilience in complex, living digital ecosystems

**At its core, the DVMS is a simple but powerful integration of:**

- **Governance Intent** – shared expectations and accountabilities
- **Operational Capabilities** – how the digital business performs
- **Assurance Evidence** – proof that outcomes are achieved and accountable
- **Cultural Learning** – for governance intent and operational capability fine-tuning

**Underpinning this integration are three distinctive DVMS models**

**Create, Protect, and Deliver (CPD)** – The CPD Model™ is a systems-based model within the DVMS that links strategy-risk and governance to execution to create, protect, and deliver digital business value as an integrated, continuously adaptive capability.

**3D Knowledge (3DK)** – The 3D Knowledge Model is a systems-thinking framework that maps team knowledge over time (past, present, future), cross-team collaboration, and alignment to strategic intent to ensure that organizational behavior, learning, and execution remain integrated and adaptive in delivering digital business value.

**Minimum Viable Capabilities (MVC)** – The Minimum Viable Capabilities (MVCs) model supports the seven essential, system-level organizational capabilities—Govern, Assure, Plan, Design, Change, Execute, and Innovate—required to reliably create, protect, and deliver digital business value in alignment with strategy-risk intent.

**The models work together to enable the following organizational capabilities:**

**A Governance Overlay** that replaces fragmentation with unity. The DVMS provides organizations with a structured way to connect strategy with day-to-day execution. Leaders gain a consistent mechanism to direct, measure, and validate performance across every system responsible for digital value.

**A Behavioral Engine** that drives high-trust, high-velocity decision-making. The DVMS embeds decision models and behavioral patterns that help teams think clearly and act confidently, even in uncertain situations. It is engineered to reduce friction, prevent blame-based cultures, and strengthen organizational reliability.

**A Learning System** that makes culture measurable, adaptable, and scalable. Culture becomes a managed asset—not an abstract concept. The DVMS provides a repeatable way to observe behavior, collect evidence, learn from outcomes, and evolve faster than threats, disruptions, or market shifts.

## Unlocking Digital Enterprise Value: The DVMS Advantage



## DVMS Benefits – Organizational and Leadership

[Explainer Video – DVMS Organization and Leadership Benefits](#)

### Organizational Benefits

Instead of replacing existing operational frameworks and platforms, the DVMS elevates them, connecting and contextualizing their data into actionable intelligence that validates performance and exposes the reasons behind unmet outcomes.

**By adopting a DVMS, enterprises are positioned to:**

- **Maintain** Operational Stability Amidst Constant Digital Disruption
- **Deliver** Digital Value and Trust Across A Digital Ecosystem
- **Satisfy** Critical Regulatory and Certification Requirements
- **Leverage** Cyber Resilience as a Competitive Advantage

### Leadership Benefits

The Digital Value Management System (DVMS) provides leaders with a unified, evidence-based approach to governing and enhancing their digital enterprise, aligning with regulatory requirements and stakeholder expectations.

**For the CEO**, the DVMS provides a clear line of sight between digital operations, business performance, and strategic outcomes—turning governance and resilience into enablers of growth and innovation rather than cost centers.

**For the Board of Directors**, the DVMS provides ongoing assurance that the organization's digital assets, operations, and ecosystem are governed, protected, and resilient—supported by evidence-based reporting that directly links operational integrity to enterprise value and stakeholder trust.

**For the CIO, CRO, CISO, and Auditors**: an integrated, adaptive, and culture-driven governance and assurance management system that enhances digital business performance, resilience, trust, and accountability.



## DVMS – Accredited Certification Training Program

[Explainer Video – The DVMS Training Pathway to Cyber Resilience](#)

**The Digital Value Management System® (DVMS) training programs** teach leadership, practitioners, and employees how to integrate fragmented systems into a unified, culture-driven governance and assurance system that accounts for the resilience of digital value within a living digital ecosystem.

## DVMS Cyber Resilience Awareness Training

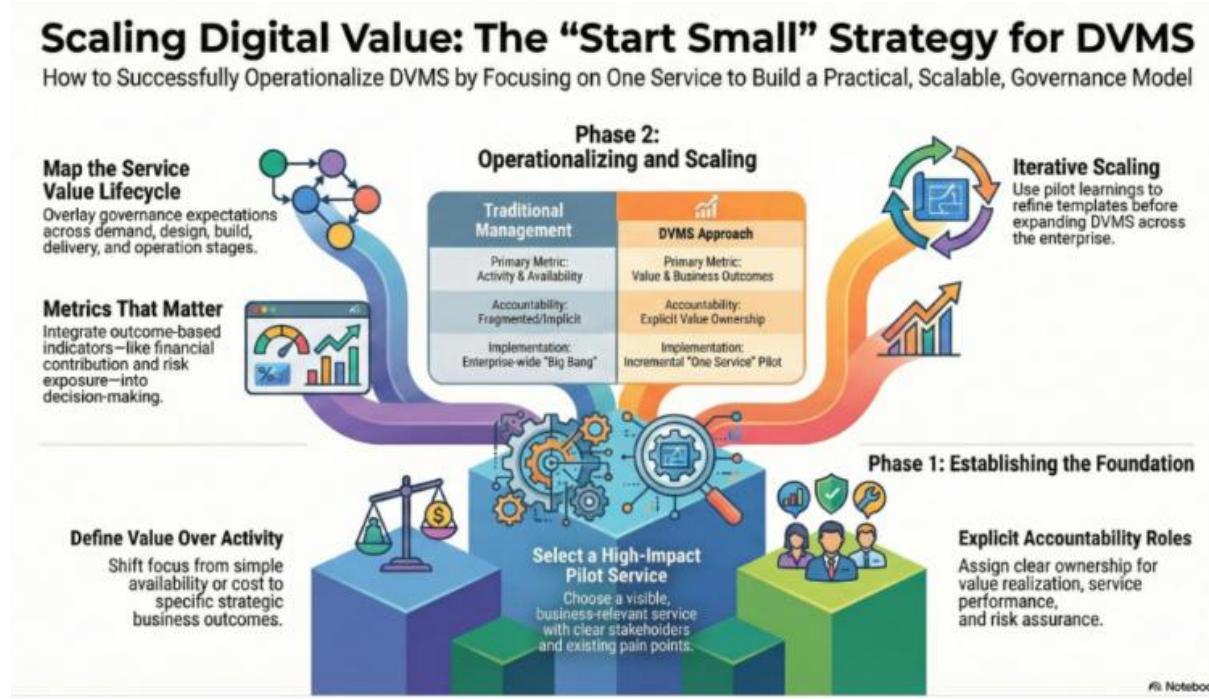
The DVMS Cyber Resilience Awareness course and its accompanying body of knowledge publication educate all employees on the fundamentals of digital business, its associated risks, the NIST Cybersecurity Framework, and their role within a shared model of governance, resilience, assurance, and accountability for creating, protecting, and delivering digital value.

## DVMS NISTCSF Cyber Resilience Foundation Certification Training

The DVMS NISTCSF Cyber Resilience Foundation certification training course and its accompanying body of knowledge publications provide ITSM, GRC, Cybersecurity, and Business professionals with a detailed understanding of the NIST Cybersecurity Framework and its role in a shared model of governance, resilience, assurance, and accountability for creating, protecting, and delivering digital value.

## DVMS Cyber Resilience Practitioner Certification Training

The DVMS Practitioner certification training course and its accompanying body of knowledge publications teach ITSM, GRC, Cybersecurity, and Business practitioners how to elevate investments in ITSM, GRC, Cybersecurity, and AI business systems by integrating them into a unified governance, resilience, assurance, and accountability system designed to proactively identify and mitigate the cyber risks that could disrupt operations, erode resilience, or diminish client trust.



## A FastTrack Approach to Launching Your DVMS Program

### [Explainer Video – Scaling a DVMS Program](#)

The DVMS FastTrack approach is a phased, iterative approach that helps organizations mature their DVMS over time, rather than trying to do everything simultaneously.

This approach breaks the DVMS journey into manageable phases of success. It all starts with selecting the first digital service you want to make cyber resilient. Once that service becomes resilient, it becomes the blueprint for operationalizing cyber resilience across the enterprise and its supply chain.