

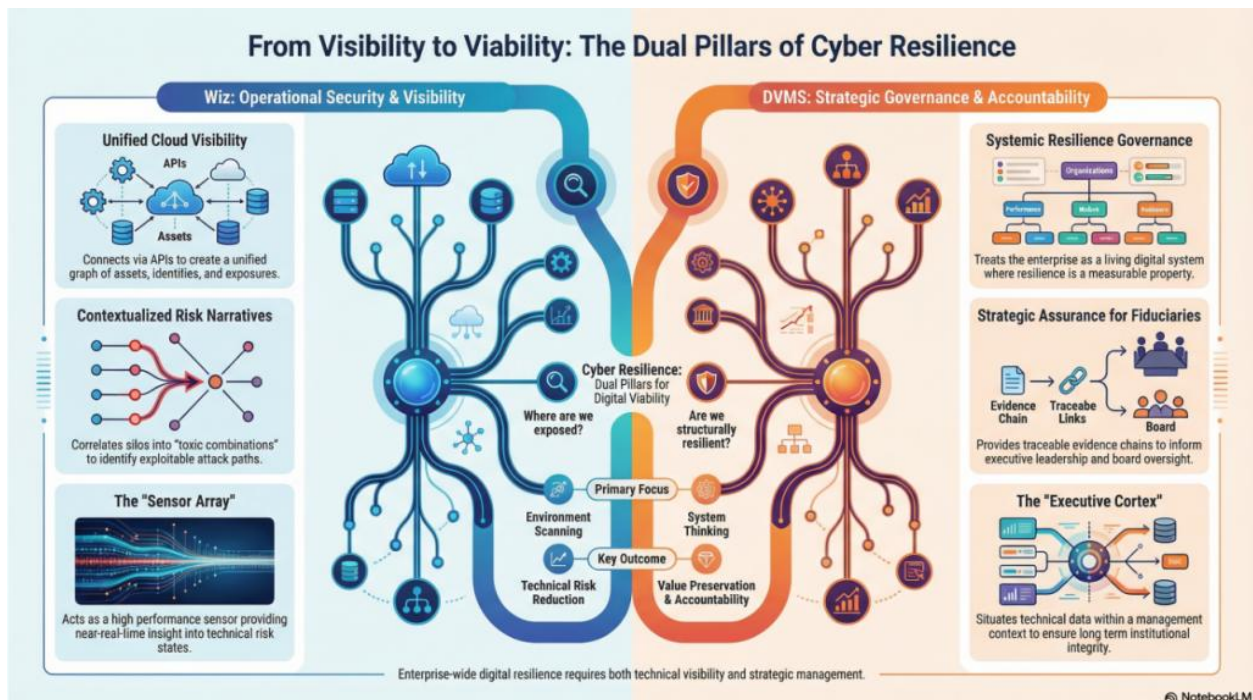


**Cyber Resilience Professional
Accredited Certification Training**

**Building an Overlay System that Governs Cyber
Resilience Through Assured Evidence and
Transparent Accountability (GRAA)**

www.dvmsinstitute.com

support@dvmsinstitute.com



From Visibility to Viability – The Dual Pillars of Cyber Resilience

Explainer Video – The Dual Pillars of Cyber Resilience

As enterprises accelerated their adoption of complex, cloud-native architectures, they encountered a new order of complexity. Infrastructure dissolved into services, workloads became ephemeral, and security boundaries blurred. In that environment, Wiz emerged as a transformational force in cloud technical security, offering radical visibility and risk prioritization across multi-cloud ecosystems.

At the same time, a broader and more consequential challenge emerged, one that extends well beyond isolated technical misconfigurations or discrete vulnerabilities.

Modern organizations function as dynamic, highly interconnected digital ecosystems shaped by siloed frameworks, technologies, applications, processes, data flows, and human actors, all operating in continuous interaction. Within this complexity, risks and outcomes are not confined to individual components; they arise from the relationships and dependencies between them.

This is the domain in which the Digital Value Management System® (DVMS) operates.

While Wiz redefined how organizations see *and secure* cloud environments, DVMS is redefining how enterprises govern, assure, and account for cyber resilience as an integrated dimension of digital business performance.

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.

Question Outcome / Question Metric (QO/QM) – This approach supports governance as testable intent by defining a clear Question Outcome (QO), the specific value or resilience condition that must be true at a given boundary, and pairing it with one or more Question Metrics (QM) that provide observable, decision-relevant evidence that the system can actually create, protect, and deliver that outcome under complex, living system operating conditions

These models and approaches work together to enable three 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 enables organizations to:

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

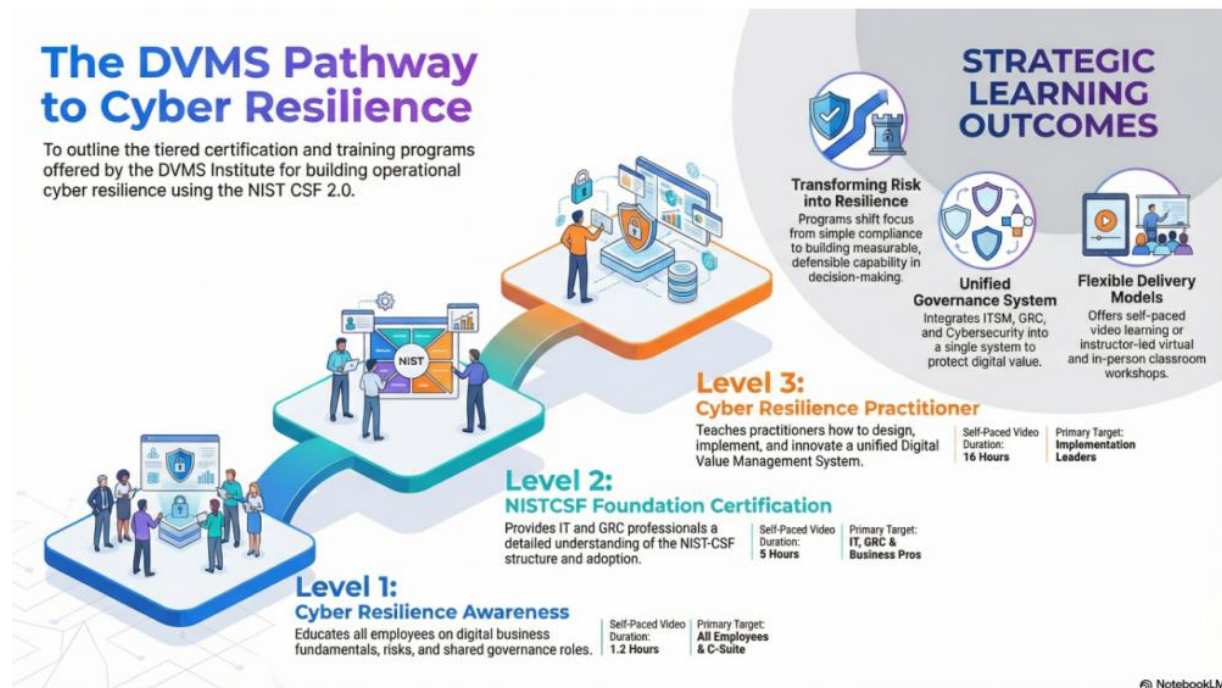
Leadership Benefits

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, the DVMS provides a unified approach to organizational digital value management, operational resilience, and regulatory compliance.



DVMS – Accredited Certification Training Programs

Explainer Video – The DVMS Training Pathway to Cyber Resilience

The DVMS Institute’s certification training programs equip leaders, practitioners, and employees with the skills to build a management architecture for governing, assuring, and accounting for resilience in complex digital ecosystems.

Through structured learning, applied certification, and authoritative publications, the Institute teaches a disciplined, outcome-driven approach to managing resilience as an integrated dimension of digital business performance.

DVMS Cyber Resilience Awareness Training

The DVMS Cyber Resilience Awareness non-certification 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**

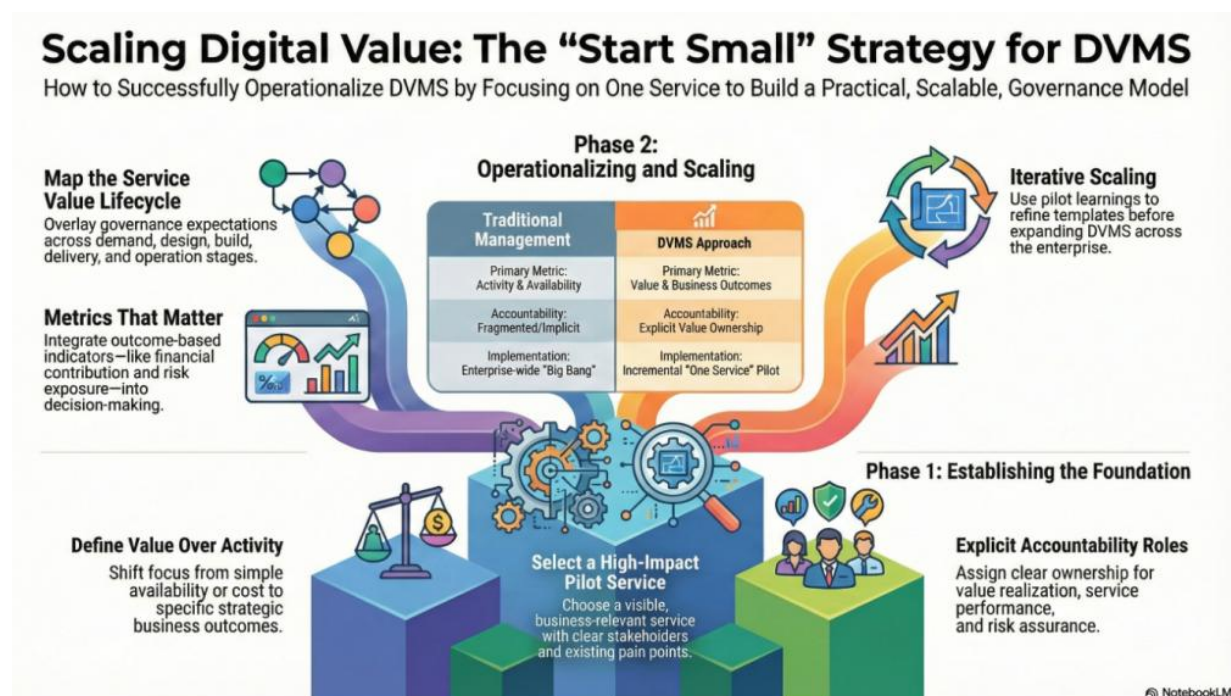
shared model of governance, resilience, assurance, and accountability for resilience in complex digital ecosystems.

[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 achieving resilience in complex digital ecosystems.

[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 build a unified governance, resilience, assurance, and accountability system designed to operationalize resilience in complex digital ecosystems.

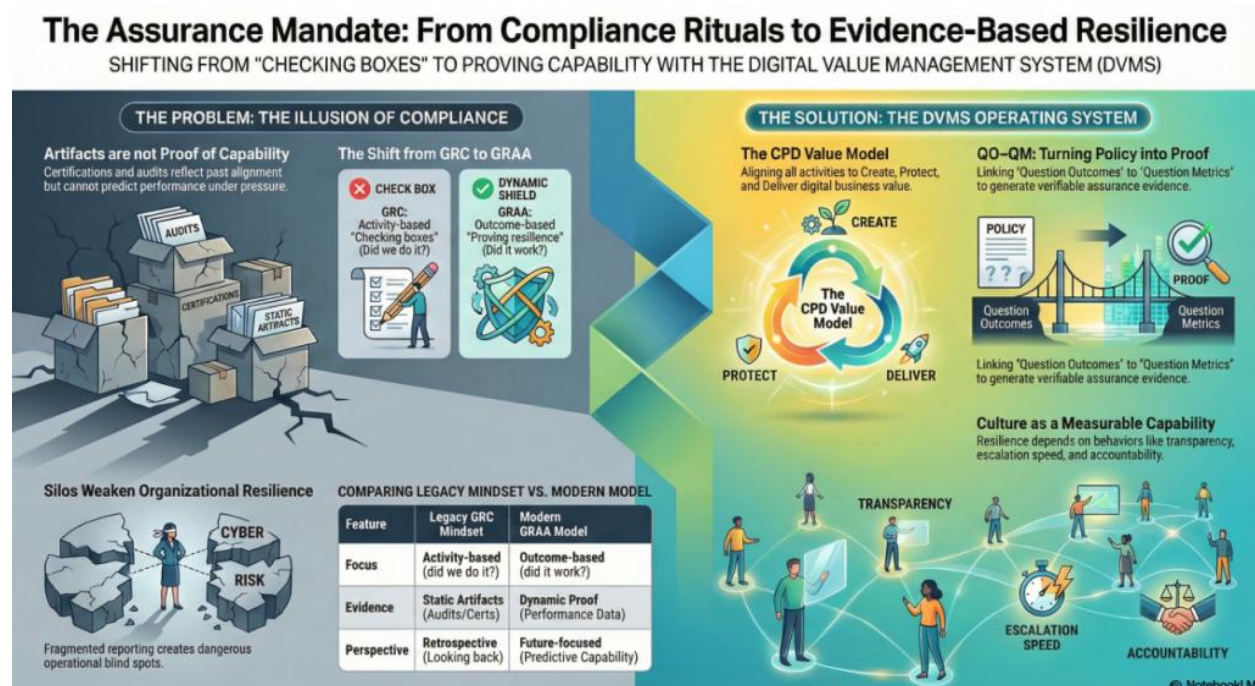


Launching A DVMS Program

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

The **DVMS FastTrack** is a phased, iterative approach that helps organizations mature a DVMS program over time, rather than trying to do everything at once. This approach breaks the DVMS journey into manageable phases of success.

It all starts with selecting the first digital service you want to make resilient. That service then becomes the blueprint for operationalizing resilience across the remaining digital services.



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.

Company Brochures and Presentation

- [DVMS Briefing Paper](#)
- [DVMS Company Brochure](#)
- [DVMS Product Brochure](#)
- [DVMS Company Presentation](#)

Explainer Videos

- [DVMS Architecture Video](#): David Moskowitz explains the DVMS System
- [DVMS Case Study Video](#): Dr. Joseph Baugh Shares His DVMS Story.
- [DVMS Overlay Model](#) – What is an Overlay Model
- [DVMS MVC ZX Model](#) – Powers the CPD
- [DVMS CPD Model](#) – Powers DVMS Operations
- [DVMS 3D Knowledge Model](#) – Powers the DVMS Culture
- [DVMS FastTrack Model](#) – Enables A Phased DVMS Adoption