DVMS Institute®

Creating a culture of innovation capable of mitigating digital risk to protect digital business performance, resilience, and trust

- Cybersecurity Culture Assessment Tool (DVMS-CAT™)
- NIST Cybersecurity Framework Certified training programs
- Body of Knowledge Publications
- Advisory Services

History and Creation of Cybersecurity Regulations and the NIST Cybersecurity Framework

2015

Executive Order 13636

The Obama administration issued Executive Order 13636 to provide a uniform standard that governments and businesses could adopt to guide their cybersecurity activities and risk management programs.

2017

Executive Order 13800

The Trump administration issued Executive Order 13800 to Strengthen the Cybersecurity of Federal Networks and Critical Infrastructure. It was ordered that each agency head should use The NIST Cybersecurity Framework to manage the agency's cybersecurity risk.

2019

COSO

The Committee of Sponsoring Organizations (COSO) of the Treadway Commission, which includes the American Accounting Association (AAA), American Institute of CPAs (AICPA), Financial Executives International (FEI), The Institute of Management Accountants (IMA) and The Institute of Internal Auditors (IIA) issued guidance to provide an overview for business executives and board members on cyber risk management. This guidance, built around the NIST Cybersecurity Framework, provides context related to the fundamental concepts of cyber risk management techniques but is not intended to be a comprehensive guide to developing and implementing technical strategies.

2022

SEC Proposed Cybersecurity Rule Changes

The Securities and Exchange Commission proposed amendments to its rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies.The proposed amendments would require, among other things, current reporting about material cybersecurity incidents and periodic reporting to provide updates about previously reported cybersecurity incidents. The proposal also would require regular reporting about a registrant's policies and procedures to identify and manage cybersecurity risks, the registrant's board of directors' oversight of cybersecurity risk; and management's role and expertise in assessing and managing cybersecurity risk and implementing cybersecurity policies and procedures.

The World Economic Forum Launched its Digital Trust initiative to help solve the digital trust and complexity challenge. The industry's critical question was: How can leaders, using best practices like the NIST Cybersecurity Framework, make better, more trustworthy decisions regarding technology and technology services?

2023

National Cybersecurity Strategy

The Biden-Harris Administration announced the National Cybersecurity Strategy. The strategy states that the U.S. will use all of its instruments of national power to disrupt and dismantle threat actors whose actions threaten its interests. These efforts may integrate diplomatic, information, military (kinetic and cyber), financial, intelligence, and law enforcement capabilities.

SEC Approves Cybersecurity Rule Changes

The Securities and Exchange Commission adopted the rules proposed in 2022 that required registrants to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance. The Commission also adopted rules requiring foreign private issuers to make comparable disclosures.

DVMS® Institute

The DVMS programs teach organizations how to create a culture of innovation capable of mitigating cybersecurity risk to protect organizational digital. business performance, resilience, and trust

Introducing the DVMS Institute

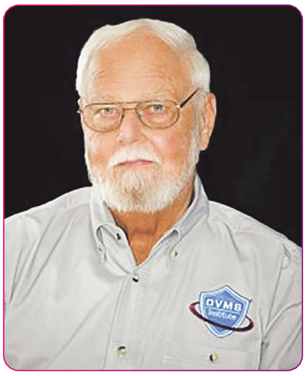
Protecting Organizational Digital Business Performance, Resilience, and Trust.

The DVMS Institute's mission is to provide organizations of any size, scale, or complexity with an affordable way to **mitigate cybersecurity risk to assure digital business performance, resilience, and trust.**

The DVMS Institute's vision is to teach organizations **how to build a NIST Cybersecurity Framework risk management program capable of meeting the stringent cybersecurity requirements in government regulations**.

As Cloud Services revolutionized the creation and management of digital infrastructure, the **DVMS NIST Cybersecurity Framework Overlay System™** will revolutionize how organizations operationalize a culture capable of mitigating cybersecurity risk that meets the stringent cybersecurity expectations of government regulators and business stakeholders.

Follow the creators and experts on LinkedIn

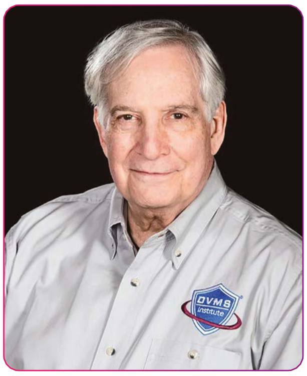


David Nichols

Executive Director

Rick Lemieux

Executive Director of Programs



David Moskowitz

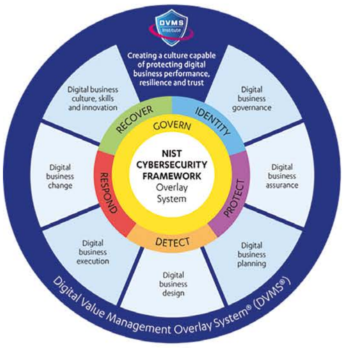
Executive Director and Content Architect

Lori Perrault

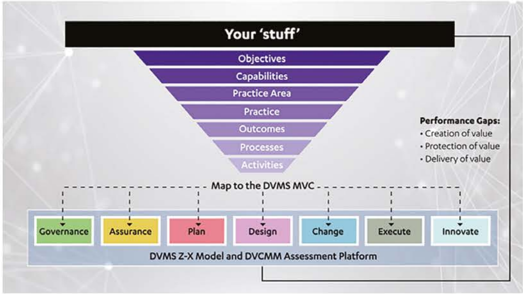
Director of Operations

> *“Leaders must appreciate technical capabilities and have people to handle them, but leaders themselves need to be something different: an influential voice in business strategy, technology decisions, and enterprise risk management.* “

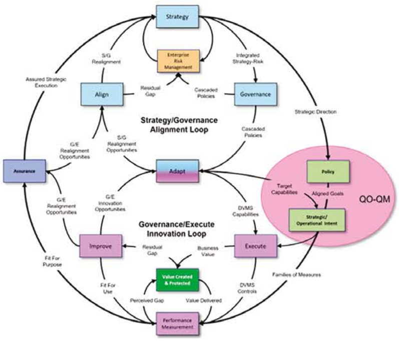
Introducing the DVMS NIST Cybersecurity Framework Overlay Model


DVMS Institute
Creating a culture capable of protecting digital business performance, resilience and trust
Digital business culture, skills and innovation
Digital business governance
Digital business change
Digital business assurance
Digital business execution
Digital business planning
Digital business design
RECOVER
IDENTITY
GOVERN
RESPOND
PROTECT
DETECT
NIST CYBERSECURITY FRAMEWORK Overlay System
Digital Value Management Overlay System® (DVMS®)

DVMS NIST Cybersecurity Framework Overlay System
© DVMS Institute 2024 All Rights Reserved



DVMS Z-X MVC Model
© DVMS Institute 2024 All Rights Reserved



DVMS CPD Model
® DVMS Institute 2024 All Rights Reserved

The QR Codes below will take you to a set of **Explainer Videos** that provide the details behind the DVMS NIST Cybersecurity Framework Overlay System and the models that underpin it.

Institute Introduction: The Institute's introduction video encapsulates the Institute's core philosophy. It's not just about technology; it's about culture. We advocate for a culture where digital business value creation, protection, and delivery are paramount.

The DVMS Overlay Model is a deep dive into how we operationalize universally recognized frameworks like NIST and ISO. We believe that a one-size-fits-all solution is often not the answer. Tailoring frameworks to specific needs ensures both security and auditability.

The DVMS CPD™ Model: Layer upon layer, the digital enterprise is a complex web of operations. The CPD Model breaks down this complexity, ensuring each layer remains secure, resilient, and audit ready.

The DVMS Z-X™ Model is the embodiment of comprehensive planning. From inception to execution, every stage is designed to innovate and support the delivery of secure digital outcomes. It's a roadmap for organizations to follow.

The DVMS 3D Knowledge™ Model: Digital outcomes aren't achieved in isolation. The 3D Knowledge Model fosters communication and collaboration, ensuring that every cog in the organizational machinery works harmoniously, by understanding everyone's role and dependencies in delivering secure digital outcomes.

The DVMS FastTrack™ Model: For those keen on a phased, systematic adoption of these frameworks, our Fast-Track Model serves as a guide. It emphasizes the pace, ensuring digital security and resilience without overwhelming adaptation.

The DVMS Cybersecurity Culture Assessment Tool (DVMS-CAT™)

In today's digital world, humans pose the highest risk regarding cybersecurity incidents. No single behavior will keep individuals from falling victim to a threat actor looking to steal valuable client data. Protecting organizational digital business value requires multiple interrelated behaviors, each potentially influenced by different factors.

The DVMS Institute Culture Assessment Tool provides a snapshot of an organization's cybersecurity culture to better understand what cultural innovations are necessary to protect organizational digital business value. Using a set of Likert scale[2] statements, participants are asked to evaluate various questions based on the Johnson and Scholes culture web, which includes six themes:

Symbols: Visual representations of the organization, including brands and/or logos, perks, and benefits. They are what you see when you walk in the door

Power structures: Reflect how formal and informal sources influence decisions, operations, and strategic direction

Organizational structures: The formal relationships related to the power structures described above

Control systems: What and how the organization monitors and measures performance and controls resources

Habits and routines: What the staff do and how they do it – including staff interactions

Stories: What and how the organization chooses to memorialize past people and events

The tool's corresponding report provides actionable insights and advisable next steps based on the results. You can then perform continuous data analysis via dedicated focus groups to better understand what's happening across the organization.

Download example auto report

Register your interest: **tools.dvmsinstitute.com**

The DVMS Institute Certified Training Programs

All training programs are accredited by APMG International, certified by the National Cybersecurity Council (NCSC) in the UK, and recognized by the U.S. Department of Homeland Security CISA organization as qualified NIST Cybersecurity Framework training in alignment with the cybersecurity roles defined in the NICE Cybersecurity Workforce Framework.

A breakdown of the DVMS-accredited training programs:

Digital Business Risk Awareness Training

This course teaches Business Leaders and Operational Stakeholders will acquire the knowledge they need to understand the fundamentals of digital business value and risk, its threat landscape, the NIST Cybersecurity Framework, and their role in deterring digital risk.

Foundation Certification Training

This course teaches business leaders and operational stakeholders the knowledge to communicate with Senior Leadership and the rest of the organization about the value a NIST Cybersecurity Framework program underpinned by a Digital Value Management System™ brings to the business regarding:

- Understanding the Cybersecurity Controls and Management Systems required to protect organizational data and business resiliency.
- Understanding why organizations must establish a culture centered around Creating, Protecting, and Delivering organizational digital value.
- Understanding how a NIST Cybersecurity Framework program can help businesses meet government cybersecurity regulatory mandates

800-53 Practitioner Certification Training

This course teaches cyber implementers, auditors, and business professionals the knowledge to design, implement, and operationalize the controls, management systems, and culture necessary to:

- Operationalize the Controls and Management Systems to protect organizational data and business resiliency
- Operationalize a Culture centered around Creating, Protecting, and Delivering organizational digital value.
- Operationalize the cybersecurity risk management capabilities to meet government cybersecurity regulatory mandates

800-171 Specialist Certification Training

This course is an extension to the 800-53 Practitioner Certification Course and is designed to teach 800-53 certified practitioners how to adapt the NIST 800-171 control families in the context of a NIST Cybersecurity Framework program.

ISO 27001 SPECIALIST IMPLEMENTER
ISO 27001 SPECIALIST AUDITOR
APMG International

ISO 27001 Specialist Certification Training

This course is an extension to the 800-53 Practitioner Certification Course and is designed to teach 800-53 certified practitioners how to adapt the ISO 27001 control families in the context of a NIST Cybersecurity Framework program.

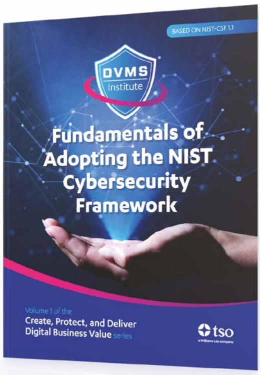
Find an approved training partner **www.dvmsinstitute.com/certification-training**

Hewlett Packard Enterprise · IIL · QA · SOLUTIONS3 · ITSM HUB · DCG DISRUPTIVE CYBER GROUP

The DVMS Institute Publications

More publications coming soon

The Institute's publications provide the guidance necessary for organizations to build a DVMS NIST Cybersecurity Framework Overlay System capable of assuring Digital Business Protection, Performance, Resilience and Trust.



BASED ON NIST-CSF 1.1
DVMS Institute
Fundamentals of Adopting the NIST Cybersecurity Framework
Volume 1 of the Create, Protect, and Deliver Digital Business Value series
tso

Fundamentals of Adopting the NIST Cybersecurity Framework

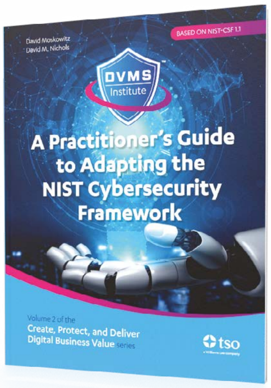
This DVMS publication takes business leaders and operational stakeholders on a journey into the world where the ever-changing cyber threat landscape intersects with digital business risk.

Print: 9780117093706

eBook: 9780117093713

Order your copy: www.tsoshop.co.uk/Business-and-Management/DVMS-Institute

---



David Moskowitz
David M. Nichols
BASED ON NIST-CSF 1.1
DVMS Institute
A Practitioner's Guide to Adapting the NIST Cybersecurity Framework
Volume 2 of the Create, Protect, and Deliver Digital Business Value series
tso

A Practitioners Guide to Adapting the NIST Cybersecurity Framework

This DVMS publication provides practitioners with detailed guidance on creating a DVMS NIST Cybersecurity Framework overlay program based on the NIST Special Publication 800-53.

Print: 9780117093959

eBook: 9780117093966

Order your copy: www.tsoshop.co.uk/Business-and-Management/DVMS-Institute

Join the community of practice

An online support community that enables members to:

- Share ideas, participate in online events, and expand one's NIST Cybersecurity Professional network.
- Become a Contributing Member to the scheme and Community of Practice by sharing ideas and approaches that make the scheme more valuable to the community.
- Participate in NIST Cybersecurity Professional master's level training course that takes candidates on a deep dive into creating DVMS case studies that can be leveraged by the community in general.

LinkedIn

“ The DVMS NIST Cybersecurity Professional certification I earned this past summer supported the successful completion of a project my employer, Guidehouse Security won to help an energy company become compliant with the recently issued TSA Security Directive for Pipeline Security. This engagement required detailed knowledge of the NIST Framework and the application of the NIST 800-53 controls called out in the framework. We will continue to apply the sound principles and lessons learned that underlie the certification process. “

Dr. Joseph Baugh

Associate Director, Risk, Compliance, & Security Energy, Sustainability and Infrastructure Practice

“ The DVMS systems thinking perspective and mental model approach are something that I practice and study extensively and have contributed to my success as a scientist, Cybersecurity Governance Advisor, and GRC professional. I’m pleased to see science and Socratic Inquiry in a cybersecurity course. Using a question/goals-based approach is not heavily leveraged in our field; therefore, observing this being used in this program is refreshing and eye-opening. I’m rarely moved and influenced by training organizations due to their limited and myopic viewpoints, but I truly believe you all are on the brink of something unique and game-changing. “

Dr. Blake Curtis

CGEIT, CRISC, CISM, CISA, CISSP, CDPSE, COBIT - Deloitte

https://dvmsinstitute.com

tso
a Williams Lea company

APMG International

All information, prices, dates, titles and jackets are correct at time of going to press but may be subject to change without notice.