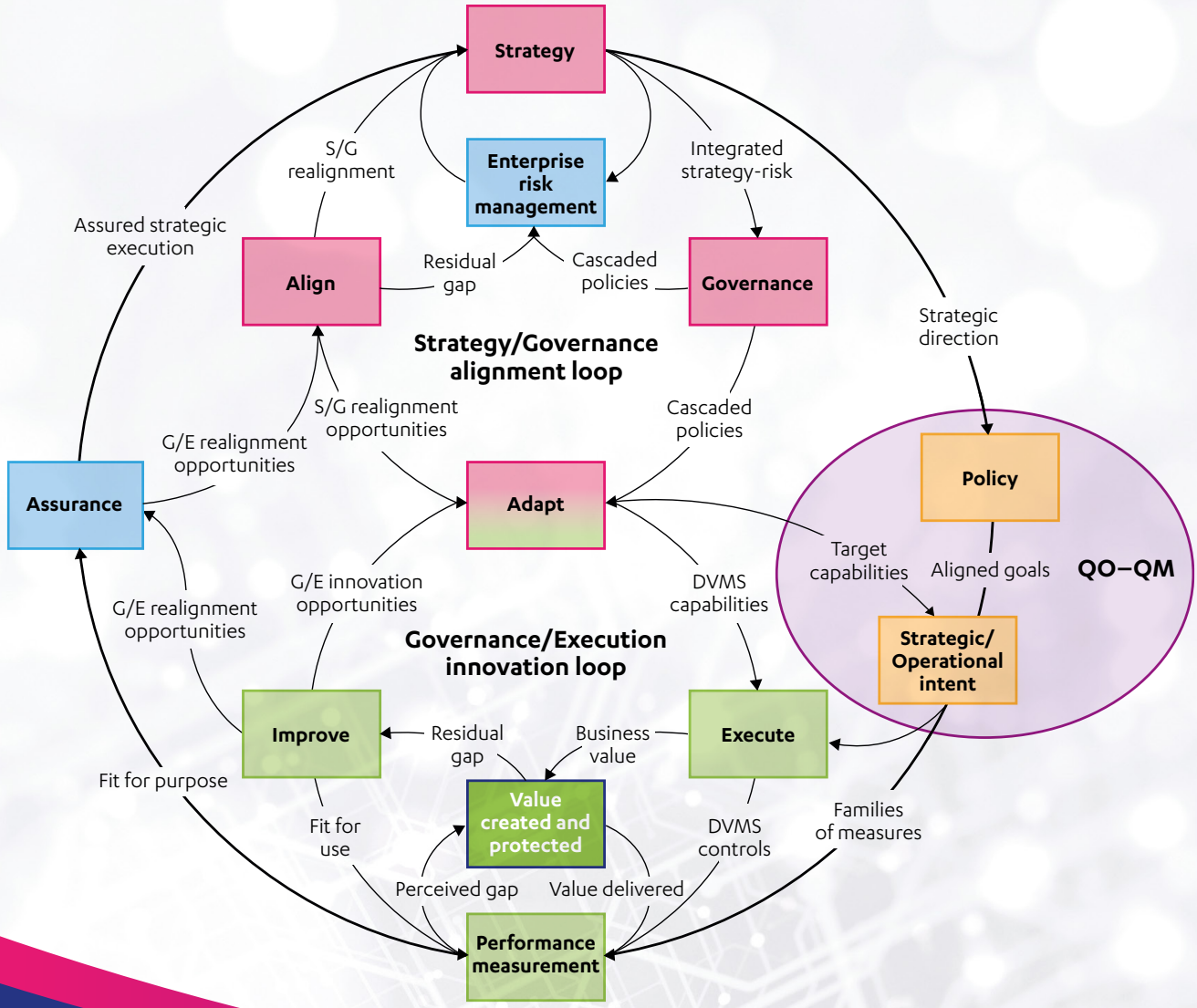
AUTHORIZED TRAINING PARTNER



Teaching organizations **how** to solve their digital risk, resiliency, and privacy management complexity problem

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.

Introducing the DVMS Institute

Solving the Digital Risk, Resiliency and Privacy Management Complexity Problem

The landscape of digital outcomes has rapidly evolved, as have the accompanying threats and challenges. The DVMS Institute recognizes these challenges and is committed to reshaping how organizations perceive and manage digital risk, resiliency, and privacy.

The institute's vision is to serve as that guiding light by teaching organizations of any size, scale, or complexity how to create a digital value overlay system capable of meeting the stringent expectations of both government regulators and operational stakeholders.

As Cloud Services revolutionized the creation and management of digital infrastructure, the DVMS Overlay Model, underpinned by well-known frameworks from NIST and standards from ISO, will revolutionize how organizations manage their digital risk, resiliency, and privacy. In this rapidly evolving digital world, the DVMS Institute stands at the forefront, ready to guide, educate, and equip. Let's journey together towards secure, resilient, and auditable digital outcomes.

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

Understanding the DVMS Overlay Model and its Relationship to NIST, ISO, and other Cybersecurity Frameworks

The DVMS Overlay Model enables organizations of any size, scale, and complexity to leverage existing business capabilities and well-known frameworks and standards (NIST, ISO, ITSM, GRC) to facilitate the delivery of secure, resilient, and auditable digital outcomes. The following explainer videos will guide you through the specific facets of our comprehensive digital value management system (DVMS™) approach.

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 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 senior leadership, boards, and all employees the fundamentals of digital business, its risks, and WHY organizations of any size, scale, and complexity need to build an overlay model capable of operationalizing any framework (NIST, ISO, COSO, ITSM, GRC, etc.) or standard (ISO) to facilitate secure, resilient, and auditable digital business outcomes.

Foundation Certification Training

This course teaches business leaders and operational stakeholders how to communicate with Leadership and Board Members on WHAT investments must be made to build an overlay model capable of operationalizing any framework (NIST, ISO, COSO, ITSM, GRC, etc.) or standard (ISO) to facilitate secure, resilient, and auditable digital outcomes.

800-53 Practitioner Certification Training

This course teaches digital risk, audit, IT, and cybersecurity practitioners HOW to build an overlay model capable of operationalizing the NIST Cybersecurity Framework and its NIST 800-53 controls to facilitate the secure, resilient, and auditable digital outcomes expected by government regulators & operational stakeholders.

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 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.

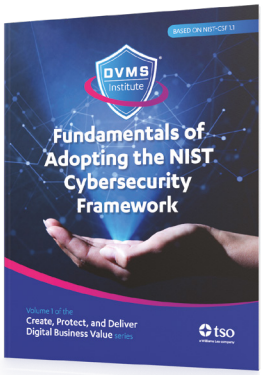
To inquire or enroll, please contact your QA account manager or Richard.beck@qa.com, Director of Cyber QA.

Details of the DVMS Institute Programme - NIST training courses can be found at https://www.qa.com/training/partners/dvms

The DVMS Institute Publications

More publications coming soon

The Institute's publications provide the guidance necessary for organizations to build a digital value management system capable of delivering the secure and resilient outcomes expected by executives, government regulators, and operational stakeholders.



Fundamentals of Adopting the NIST Cybersecurity Framework

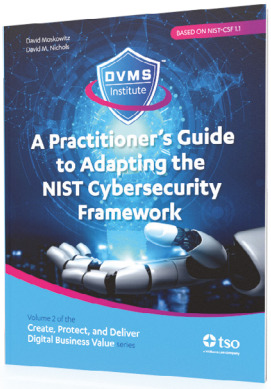
The first book from the Institute's, Create, Protect, and Deliver (CPD) digital business value series. It takes business leaders and stakeholders on a journey into the world where the ever-changing cyber threat landscape intersects with digital business risk.

Print: 9780117093706

eBook: 9780117093713

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

---



A Practitioners Guide to Adapting the NIST Cybersecurity Framework

This publication provides practitioners with detailed guidance on creating a NIST Cybersecurity Framework risk management program using NIST Special Publication 800-53, the DVMS Institute's CPD Model, and existing digital business systems.

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

Cybersecurity Culture Assessment Tool

People usually pose the highest risk regarding cybersecurity breaches, and this is hard to measure. There is no single behaviour that will keep individuals and organizations secure online. The ability to create and adequately protect digital business value requires multiple interrelated behaviours, and each one is potentially influenced by different factors.

Digital business risk is usually measured around process and technology, without factoring in human behaviour. Understanding individual behaviour is an important component to evaluate effective digital business risk management within business. Many businesses believe they are safe from cyberthreats, but they have no ways of knowing if this is the case. What users say they understand and do, is not necessarily the same as what they actually do. Users may report awareness in surveys but might not have the skills or inclination to carry out the associated actions and this poses a real challenge to organizations.

Therefore, DVMS and partners have created a survey tool that provides a snapshot of the organizational cyber culture to understand if improvements could be made and highlight best practice to protect digital business value.

Once the survey has been completed, the tool will generate an automated report and score the organization against the following factors:

- **individual commitment to managing digital business risk**
- **organizational commitment to digital business risk (team)**
- **training and education**
- **policies and procedures**
- **workplace culture**
- **commitment to learning**

The report will provide actionable insights and advisable next steps based on the results. You can then perform in-depth data analysis and filtering to get a better understanding for what's happening across the organization.

To find out more and to register your interest:
https://dvmsinstitute.com/

"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

DVMS's exclusive global publishing partner