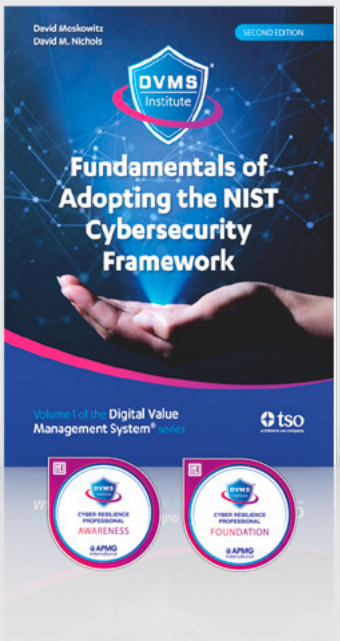
The Market Leader in NIST Cybersecurity Framework (NISTCSF) and Digital Value Management System (DVMS) Publications, Certification Training, Assessments, and Expert Mentoring Services.

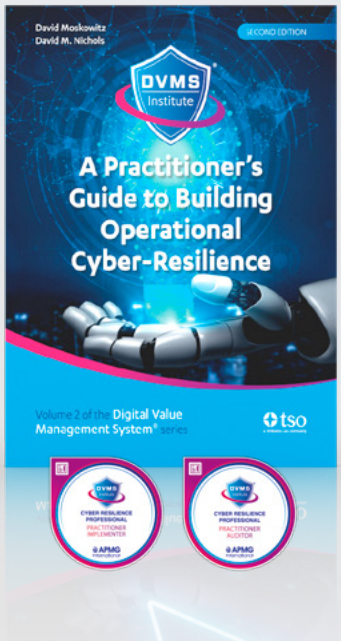
williams lea | tso
An RRD Company

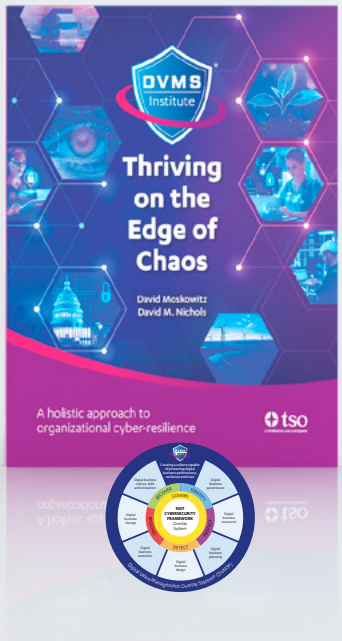
Introducing the DVMS Institute

The DVMS Institute assists organizations in operationalizing the NIST Cybersecurity Framework (NISTCSF) by utilizing a Digital Value Management System® (DVMS) to transform it from a static compliance reference framework into a dynamic operating system of Governance, Resilience, and Assurance.

The DVMS Institute's **Accredited Publications** and **Certified Training Courses** offer a structured pathway for mastering the integration of governance intent, operational execution, and assurance evidence, enabling organizations to demonstrate measurable resilience, regulatory alignment, and stakeholder confidence in a rapidly evolving digital landscape.







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

DVMS Cyber Resilience Professional - Awareness

Version: 4.0

Course Overview

The DVMS Cyber Resilience Professional Awareness course teaches employees the fundamentals of digital business, its risks, and their role in creating, protecting, and delivering resilient digital business value. This investment builds durable capability within the organization and creates a workforce culture prepared to transform systemic cyber risks into operational resilience.

Who Should Attend

This course is designed for employees at all levels who:

- Contribute to the creation, protection, or delivery of digital services
- Need a practical understanding of cybersecurity as business risk
- Want to become part of a culture of resilience within their organization

Learning Objectives

By the end of the course, participants will be able to:

- Explain what it means to "become digital" and how digital evolution increases risk.
- Recognize the components of cyber risk—threats, vulnerabilities, assets, and controls.
- Understand the basics of risk assessment and the role of frameworks like NIST CSF.
- Describe how cybersecurity enables business value rather than restricts it.
- Appreciate the importance of culture and leadership in building resilience.

Course Structure

Chapter 1 – Digital Business Evolution

- From industrial to digital enterprise
- The digital mindset and expanding threat surface
- How leadership must adapt in the digital age

Chapter 2 – Digital Business Risk & Cybersecurity

- What cyber risk is and why it matters to business
- Threats, vulnerabilities, assets, and controls
- Basics of risk assessment and the Cyber Kill Chain™
- Why cybersecurity is a business opportunity, not just an IT challenge

Chapter 3 – Adopting & Adapting the NIST Cybersecurity Framework

- Role of NIST CSF in digital evolution
- The six functions: Govern, Identify, Protect, Detect, Respond, Recover
- Adoption as a strategic decision; adaptation as a cultural discipline
- How to embed continual improvement into the organization

Materials & Resources

- Course Text: Fundamentals of Adopting the NIST Cybersecurity Framework
- Mentoring Community: Access to the DVMS NIST Cybersecurity Framework Community of Practice on LinkedIn
- Digital Badge: Earn your DVMS Professional® recognition and share your achievement

Key Takeaways

- Digital evolution is both an opportunity and a source of risk.
- Cybersecurity must be reframed as a business enabler.
- The NIST Cybersecurity Framework provides a common language for resilience.
- Culture, leadership, and practice—not technology alone—drive organizational protection of digital value.

DVMS Cyber Resilience Professional Foundation Certification Training

Version: 4.0

Course Overview

The DVMS Cyber Resilience Professional Foundation certification training course teaches ITSM, GRC, Cybersecurity, and Business professionals a detailed understanding of the NIST Cybersecurity Framework (NISTCSF) and its role as part of an integrated, adaptive, and culture-driven governance and assurance Digital Value Management System® capable of delivering resilient, compliant, and trusted digital outcomes.

Learning Objectives

By the end of the course, participants will be able to:

- Explain fundamental cybersecurity and risk management concepts.
- Understand the structure, components, and relationships within the NIST-CSF.
- Apply concepts of organizational culture, privacy, and resiliency to cybersecurity programs.
- Describe how to adopt and adapt the NIST-CSF within a digital enterprise.
- Recognize how the DVMS (Digital Value Management System) overlay extends and integrates with the NIST-CSF to drive digital business performance and resilience.

Course Modules and Content Outline

Module 1: Imperative & Origin

- Explain the concept of risk.
- Differentiate between threats and vulnerabilities.
- Understand cybersecurity risk.
- Review the NIST-CSF timeline and its origins.
- Identify the benefits of adopting the NIST-CSF.

Module 2: Framework Structure

- Explain the structure of the NIST-CSF Core.
- Understand profiles and tiers and their relationships.
- Learn to use the NIST-CSF Online Reference tool.

Module 3: Framework Core

- Describe the structure and outcomes of the CSF Core.
- Understand category-level objectives within the framework.

Module 4: CSF Profiles & CSF Tiers

- Explain the use of CSF Profiles.
- Describe CSF Tiers and their applications.

Module 5: COSO Enterprise Risk Management (ERM)

- Understand COSO's 20 principles in the context of the NIST-CSF.
- Discuss how culture influences organizational risk.

Module 6: NIST CSF & NIST Privacy Framework

- Describe the role of a privacy framework.
- Understand how the NIST Privacy Framework integrates with the CSF.

Module 7: NIST-CSF and Resiliency

- Define organizational resiliency in the context of NIST-CSF.

Module 8: Adopt and Adapt the NIST-CSF

- Describe the strategic importance of adopting the NIST-CSF.
- Explain leadership's role in commitment and culture curation.
- Define organizational commitment to adoption.

Module 9: Adopt the NIST-CSF

- Define "Informative References" (IRs).
- Describe how to adapt IR controls to suit organizational needs.
- Understand how adaptation enhances organizational resiliency.

Module 10: Beyond the Framework – DVMS Overlay

- Explain DVMS overlay concepts.
- Understand the DVMS Z-X Model and its seven capabilities.
- Learn to identify performance gaps using the DVMS overlay.
- Explore the DVMS FastTrack™ approach.

Examination Details

Parameter	Details
Duration	60 minutes
Format	40 multiple-choice questions (4 options each)
Delivery	Paper-based or online, proctored
Bloom's Levels	Level 1 – Knowledge; Level 2 – Comprehension
Scoring	1 point per question; 60% to pass (24/40)
Closed Book	Yes

DVMS Cyber Resilience Professional Practitioner

Version: 4.0

Course Overview

The DVMS Cyber Resilience Professional Practitioner certification training course teaches practitioner-level competencies in building a Digital Value Management System® (DVMS) that transforms systemic cyber risk into operational resilience by uniting **Fragmented Frameworks and Standards**—such as NIST, ITSM, GRC, and ISO—into a single, adaptive **Governance, Resilience, and Assurance** (GRA) operating system that keeps your digital business running, no matter the disruption. The course builds progressively from mindset and models to systems thinking, governance integration, and continuous improvement, culminating in a capstone synthesis project.

Learning Objectives

By the end of the course, participants will be able to:

- Develop practitioner-level competencies in building and operating a **Digital Value Management System® (DVMS)**.
- Transform **systemic cyber risk** into **operational resilience** through an integrated Governance, Resilience, and Assurance (GRA) operating system.
- Unify fragmented frameworks (NIST, ITSM, GRC, ISO, etc.) into a cohesive, adaptive system of governance and assurance.
- Demonstrate the ability to align **strategy, risk, and performance** for sustained cyber operational resilience.

Course Modules and Content Outline

Module 1 – Practitioner Foundations

1.1 Transitioning to a Practitioner's Mindset

- Differentiate between compliance-driven and practitioner (strategy-risk-aligned) mindsets.
- Understand adaptive, proactive decision-making in cybersecurity operations.
- Identify behaviors and mindsets that enable value creation.

1.2 The 3D Knowledge Model

- Describe X and Y axes of the model for mapping knowledge and dependencies.
- Apply both axes to enhance decision-making and resilience.

1.3 3D Knowledge Model: Z-Axis

- Explore culture and leadership as drivers of practitioner effectiveness.
- Evaluate how culture influences resilience and governance.
- Develop strategies for building generative culture.

1.4 The Role of Questions

- Formulate practitioner-level diagnostic and strategic questions.
- Use inquiry to uncover hidden risks, dependencies, and assumptions.
- Embed questioning as a foundation for proactive cybersecurity.

1.5 Strategy-Risk

- Explain the unity of strategy and risk.
- Apply the space-time analogy to decision-making.
- Evaluate the consequences of siloed strategy and risk management.

Module 2 – Systems Thinking and Operational Integration

2.1 Systems Thinking Fundamentals

- Understand system structure, behavior, and culture in cybersecurity.
- Apply systems tools (causal loops, iceberg, BOT graphs).
- Identify feedback loops and leverage points for resilience.

2.2 Strategy-Risk: Reinforce & Operationalize

- Integrate strategy-risk thinking into daily cybersecurity practices.
- Design cross-functional collaboration processes for alignment.

2.3 Deep Dive into the CPD Model

- Analyze workflows through the CPD (Create-Protect-Deliver) Model.
- Map assurance loops and feedback mechanisms.

2.4 MVC Operationalized by CPD

- Describe how CPD loops enable Minimum Viable Capabilities (MVC).
- Map NIST CSF core functions to CPD and MVC for execution alignment.

2.5 Be the Menace

- Apply use and misuse cases to anticipate threats.
- Integrate adversarial modeling into assurance and measurement planning.

Module 3 – Governance, Capabilities, and Measurement

3.1 DVMS as a Governance Overlay

- Understand DVMS as a system overlay linking governance, strategy, and execution.
- Map workflows to MVCs and assess governance loops.

3.2 Minimum Viable Capabilities (MVC)

- Explain and apply the seven MVCs across workflows.
- Use the 3D Knowledge Model (Z-axis) to identify cultural barriers.

3.3 QO–QM Validation & Metrics

- Apply GQM (Goal–Question–Metric) and QO–QM frameworks.
- Align metrics with strategic outcomes and continuous improvement.

3.4 FastTrack™ Approach

- Sequence capability deployment based on maturity and culture.
- Use governance feedback and cultural diagnostics for dynamic adaptation.

3.5 Risk Team Structure & Collaboration

- Design and assess cross-functional risk teams.
- Integrate DVMS, MVC, and QO–QM in governance and decision-making.

Module 4 – Innovation, Maturity, and Adaptation

4.1 The Four Aspects of Innovation

- Distinguish incremental, sustaining, adaptive, and disruptive innovation.
- Apply systems thinking to identify innovation leverage points.
- 4.2 Nonlinear Adoption – Revisiting Phases
- Contrast linear and nonlinear adoption models.
- Map feedback loops that drive adaptation and cultural learning.

4.3 DVCMM (Digital Value Capability Maturity Model)

- Define DVCMM levels (0–3) across MVCs.
- Benchmark maturity and link Govern/Assure to capability deployment.

4.4 Bridge to Day 5 – Synthesis Preparation

- Integrate systems thinking, governance, culture, and measurement.
- Formulate a capstone action plan for cyber resilience improvement.

Module 5 – Integration, Improvement, and Mastery

5.1 Continual Improvement & Innovation Loops

- Design feedback mechanisms for single- and double-loop learning.
- Embed continuous improvement into operations and culture.

5.2 Integrating Governance, Measurement, and Culture

- Unify DVMS governance, GQM/QO–QM measurement, and cultural diagnostics.
- Design feedback loops for adaptive improvement and resilience.

5.3 Capstone Synthesis & Practitioner Reflection

- Apply all course models to a real-world cybersecurity challenge.
- Develop an actionable improvement plan aligned with strategy-risk priorities.
- Reflect on practitioner growth and continuous learning.

Assessment and Examination

Parameter	Details
Duration	150 minutes (2.5 hours).
Format	Online, proctored, open-book examination.
Questions	65 multiple-choice (1 correct answer each)
Weighting	5 total points; passing score = 39 (60%)
Focus	Application, analysis, and evaluation (Bloom's Levels 3–5)
Resources	Book, slides, and case study materials (unaltered)
Outcome	Pass/Fail

Capstone

Learners synthesize course concepts—DVMS overlay, CPD, MVC, 3D Knowledge Model, DVCMM, and governance frameworks—into a strategic practitioner plan demonstrating cyber-resilience maturity, cultural awareness, and measurable improvement.

williams lea | tso
An RRD Company