David Moskowitz
David M. Nichols

FREE DOWNLOAD

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 Williams Lea company

CHAPTER 1
The journey

1 The journey

"The journey of a thousand miles begins with a single step."
Lao Tzu

Lao Tzu's statement is incomplete. Yes, the journey begins with a single step. However, if your starting point is the New Jersey shore (the beaches of the Atlantic Ocean), and your objective is to get to the Pacific Ocean, your first step should be to the west: walking east will only serve to get you wet. Consequently, we extend Lao Tzu's quote to read, "The journey of a thousand miles begins with a single step *in the right direction*."

Starting a cybersecurity journey in the right direction requires maturing existing organizational capabilities first. Why? Consider that there are cybersecurity control requirements for cybersecurity incidents and configuration management. Instead of adding and supporting these requirements separately, integrate them into existing organizational capabilities. This approach is consistent with the idea that cybersecurity is an organizational responsibility, not something to be siloed in a single department.

This last idea, organizational responsibility, is essential because the actual destination isn't cybersecurity, it's the management of digital business risk. The destination applies a strategy-risk-based approach[1] that creates and protects digital business value, achieving cyber resilience as a by-product.

This book covers this idea in the context of the Digital Value Management System™ (DVMS), which combines a principle-based enterprise risk management framework with a holistic view of the organization in the form of systems thinking. In other words, the cybersecurity journey starts by improving or adding organizational capabilities; the journey addresses expanding existing capabilities rather than adding distinct requirements for cybersecurity segregated from what we might label "business as usual." The initial goal is to be proactive and stabilize existing capabilities before tackling cybersecurity issues. The goal is cyber resilience, not cybersecurity.

As part of stabilizing the environment, understand and document how work flows within the organization: not how it's "supposed" to flow, but the reality. Also, pay attention to how communication, innovation, and improvement flow. Sometimes this will follow an organization (org) chart, but many times it won't. It is essential to understand reality versus assuming. This approach is the only way to leverage the system to make meaningful and long-lasting (i.e., "sticky") changes.

What do we mean by the phrase "leverage the system"? The answer to this question lies in one of our first principles (covered in detail in Chapter 5): "Adopt and apply systems thinking." The principle potentially requires learning to see and perceive the organization differently – see the organization as dynamic and interconnected elements contributing to the value it delivers to stakeholders.

1 We formulated the idea of a single entity "strategy-risk" based on the authors' experience that treating strategy and risk as separate concepts wasn't working. Then a study by North Carolina State University (2022) formally confirmed our approach. Strategy-risk treats the two as inseparable: two faces of the same coin.

The DVMS is neither framework nor method: it is a scalable overlay that applies to any organization. It is composed of three layers:

- The top layer is what the organization already does. It's a black box to the outside world. It could use existing frameworks and methods. These are the organizational capabilities to stabilize
- The middle layer, which we call the *Z-X Model*,[2] provides the seven minimal viable capabilities any organization needs: the capabilities to govern, assure, plan, design, change, execute, and innovate.[3] Every framework or methodology, practice, or process is subsumed by one or more of these minimum viable capabilities
- The bottom layer of a model supports the creation, protection, and delivery (including support) of digital business value. We call the model the *CPD Model*™ (CPD being an abbreviation for "creating, protecting, and delivering" digital business value). It represents an approach to linking strategy and governance with governance and execution to create and protect digital business value.

Cybersecurity is a single aspect of digital business risk management. The overall goal should be cyber resilience that enables the organization to create, and appropriately support and protect, the delivery of digital business value.

There are only two possibilities for adopting and adapting a cybersecurity informative reference. You treat cybersecurity as an organizational responsibility with accountability starting at the top, or you don't. It's a binary choice. If you want to start your cybersecurity journey in the right direction, take the first step to learn to see the whole, not a hole.

One of the themes repeated throughout this book is that value creation and value protection are two sides of the same coin. It's essential to do both: value must be protected appropriately for the organization, understanding that value changes over time. Cybersecurity is an intrinsic aspect of business value.

The idea of a shift in perception is associated with another theme: the need to apply systems thinking, which views cybersecurity as an enterprise responsibility, and not that of a single department (or similar internal organizational unit).

1.1 Using the book

Chapter 2 introduces the key to taking a proactive stance to protect created digital value: anticipating what threat actors will do, requiring asking different questions that have their basis in systems thinking. The purpose of asking questions is twofold:

- The initial questions provide the basis to identify the business systems (and everything that underpins, supports, or enables them), which is essential to the mission to create and protect digital business value
- Additional questions help determine the system weaknesses, allowing probing and proactively determining where and how to direct remediation efforts.

Chapter 3 provides an approach to systems thinking and explains how it differs from traditional thinking. Systems thinking, or thinking in systems, is not something you *do*: it's something you *learn* and *practice*. Systems thinking is similar to agile in that the organization doesn't *do* agile: the organization *becomes* agile. The people in the organization must learn to see the whole (the organization as a whole), not a hole (i.e., the organization viewed as siloed departments). It's critical for everyone in the organization, whether a single-person company or a million-people multinational enterprise, to understand that value created and not appropriately protected has little to no value for stakeholders.

2 The name is derived from the internal solid lines (the Z) and the dotted line (making an X).

3 We apply the term "innovate" to the capability as a superset of "improve." There are four aspects to "innovate" (incremental, sustaining, adaptive, and disruptive) that are covered in more detail later in this book.

The chapter reviews a simple supply chain simulation game and looks at the lessons from gameplay. This discussion provides a basis for understanding how to apply leverage (and at what points) to modify the system. Knowledge management is a critical aspect of human systems. You'll also find this topic covered. Finally, the chapter decomposes the CPD Model, explaining how it supports digital business risk management by creating, protecting, and delivering digital business value.

Chapter 4 provides a detailed link between cybersecurity and the DVMS, starting with an in-depth examination of the Z-X Model capabilities. The chapter introduces the Digital Value Capability Maturity Model (DVCMM) to gauge the organizational ability to use the Z-X Model to create and deliver appropriately protected digital business value. The chapter builds on the systems thinking material in Chapter 3 in the context of the CPD Model.

Chapter 5 covers an adaptive way of working. This is a strategy-risk-informed approach to using cybersecurity to manage digital business risk and create and protect digital business value. It incorporates a principle-based approach to enterprise risk management – the very core of what it takes to manage digital business risk. Why an adaptive approach? It's the best way for the organization to keep pace with the dynamics of the changing environment, including internal and external factors and the constantly evolving threat landscape. The chapter covers organizing to create and protect digital business value – and this isn't an org-chart-based approach. The chapter also covers a generic approach to agile as an essential aspect of an adaptive way of working. The final discussion in the chapter addresses the relationship between agility, resilience, the CPD Model, and managing digital business risk to improve the cybersecurity posture.

Chapter 6 provides detailed information on integrating cybersecurity into the Z-X Model capabilities and resulting practice areas, as distinct from an approach that consigns cybersecurity to technical departments. It details the dependence of cybersecurity on organizational capabilities represented by the Z-X Model – doing so by taking a phased approach that uses the DVMS FastTrack™ model.

Chapter 7 provides a deep dive into strategy-risk in the context of the CPD Model. It highlights the need to consider the material covered previously in this book – specifically regarding the importance of adopting new or different mental models that facilitates asking different questions. The chapter also covers the goal, question, metric (GQM) approach and Question Outcome–Question Metric (QO–QM) to learn to ask better systems-thinking-based questions.

We briefly introduced the idea of the DVMS as a scalable overlay to address the digital business risk management critical to creating and protecting the delivery of digital business value in the first book in the series, *Fundamentals of Adopting the NIST Cybersecurity Framework* (Moskowitz and Nichols, 2022). **Chapter 8** covers how this works, with suggestions that apply to any organization, regardless of size or geography.

1.2 For NIST Cybersecurity Professional students

The material in this book provides the rubric for the NIST Cybersecurity Professional (NCSP) Practitioner and Specialist courses. It presents the narrative that accompanies your course material. The book contains more information than will fit into the course. Consequently, we recommend that you read the whole book rather than focusing on just the material in the syllabus.

The tuition for NCSP students includes the book. For the non-student, because the information in this book is more in-depth, you do not need the *Fundamentals* book to understand the application to an organization.

If you understand the flow of the story in this book, it will be easier to pass the course examination.

1.3 The rest of the story

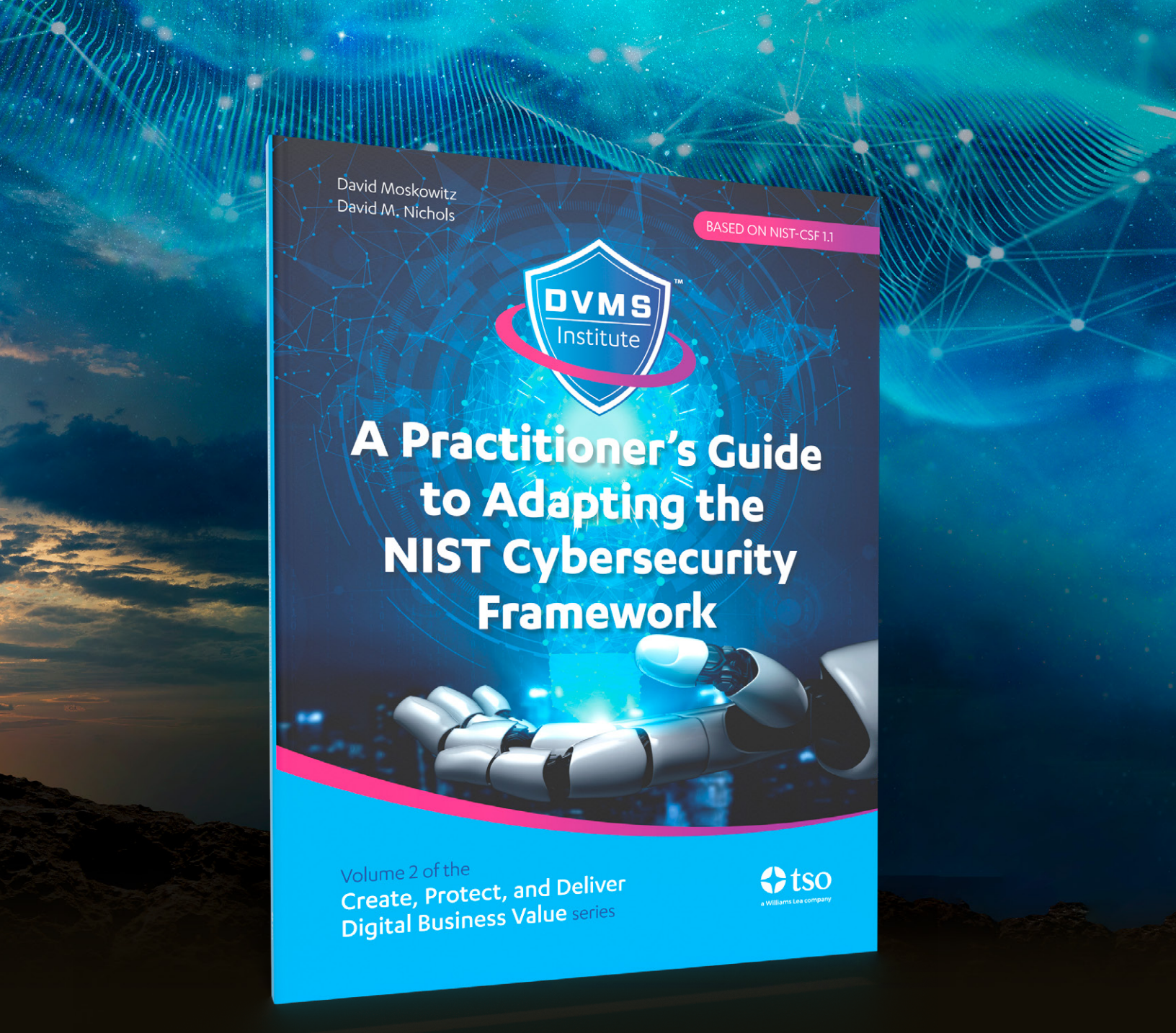
This book continues the story regarding a practical approach to adopting the NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST-CSF) that is covered in the *Fundamentals* book – this time at the practitioner and specialist level. There are several concepts and models introduced in that volume covered in more detail in this volume, including:

- Systems thinking
- The DVMS, and the DVMS as a scalable overlay
- The CPD Model
- The Z-X Model
- Strategy-risk
- The COSO[4] principles.

The *Fundamentals* book is a good place to start if you want guidance in adopting the NIST Cybersecurity Framework.

This book and the rest of the series support the journey in the right direction to build a resilient organization that manages digital business risk. Enjoy the journey.

4 We recommend the Committee of Sponsoring Organizations of the Treadway Commission (COSO) approach because of its principle-based approach to risk management. What is important are the principles, not the specific COSO approach. The source for the COSO principles is the COSO Internal Control Integrated Framework (2013) and is used with permission of AICPA. On the COSO website, you can find the executive summary (COSO, 2017) and a summary of the COSO principles and approach (COSO, 2019).



Purchase the full title now in print or digital formats

dvmsinstitute.com/nist-cybersecurity-professional-training-publications/