NCP 010

DVMS Cyber Resilience Professional – Practitioner

Syllabus

Version 4.0

September 2025

tso
a Williams Lea company

Contents

Introduction

This document provides the learning outcomes for the course and the assessment criteria used. It also provides an overview of the examination design regarding the types of questions asked.

The syllabus table below shows the learning outcomes for each module and the related sections, the exam marks allocated to each module, and the Bloom's level associated with the module.

The examinable materials include the relevant books in the DVMS series, the course materials, the course workshops, the lecture notes, and the exercises. Unless otherwise noted in the syllabus, the book sections are from

The Marks column applies to the Implementor and the Assessor examinations. The notation in the Book Sections column refers to the Practitioner's Guide sections. The notation "ff" refers to all subsections inclusively (e.g., 2.3ff means section 2.3 and all subsections through to 2.3.3.7). Any figures, tables, or callouts (i.e., text in dark blue boxes) within the sections listed below are also part of the study material. A reference to a chapter introduction is shown as X.0 (e.g., 5.0 in Module 1.1).

You might notice that the number of marks allocated to each module doesn't always align with the number of learning outcomes within that module. This is because the last word in "Digital Value Management System®" suggests that the DVMS is a system that requires us to think systematically—a concept we'll dive into on Day 2.

Also, remember that some questions may touch on multiple learning outcomes and even overlap between different modules. For example, the idea of "strategy-risk" is discussed in several sections, each offering a unique viewpoint. Similarly, there are parts of the book that reference material that may not directly link to one specific learning outcome (LO) but might be relevant for understanding later ones.

There isn't always an exclusive mapping between the learning outcomes and the book sections. While we've tried to map the modules to the book, concepts and models appear in multiple places in the course (and the book), making it difficult to say "read this and you'll get everything you need." Your best approach is to read the entire book; by all means, use the syllabus as a guide with the understanding that you'll miss the nuances and connections that are examinable if you're not familiar with the whole.

Note: The order of presentation in the course intentionally differs from that of the book. The course starts with the fundamentals and builds with each module.

Syllabus

Module	Title	Learning Outcomes	Book Sections	Marks	Bloom's Level
1.1	**Transitioning to a Practitioner's Mindset**				3-4
		• Differentiate foundational (compliance-driven) and practitioner (strategy-risk-aligned) mindsets • Explain the importance of proactive, strategic, and adaptive thinking in cybersecurity, operations, and decision-making • Identify key behaviors, decision-making processes, and value creation mindset	2.4.2.4, 2.5.2, 4.4.3, 5.0, 5.3, 5.3.1, 5.3.1.4, 5.4.2.6	1	
1.2	**The 3D Knowledge Model**				3-4

		• Describe the components and purpose of the 3D Knowledge Model X and Y axes.
		• Apply the X-axis to map knowledge over time.
		• Analyze the Y-axis to uncover structural and cross-functional dependencies that affect knowledge flow and decision-making.
		• Evaluate how integrating both axes:
		  ○ Improves resilience
		  ○ Enables better decisions
		  ○ Supports practitioner-level governance and assurance
		  ○ Breaks down siloes
			2.2ff, 2.3, 2.3.1	2	

1.3	**3D Knowledge Model: Z-axis**				3-5
		• Apply the Z-axis and understand its role in practitioner effectiveness. • Analyze how culture and leadership shape cybersecurity decision-making, resilience, and assurance outcomes • Evaluate how cultural alignment or misalignment impacts organizational resilience and governance. • Identify strategies for fostering a generative culture.	2.2ff, 2.3, 3.4.1ff, 3.4.2, 3.4.3, 4.2.2.3, 5.4.1	2	
1.4	**The role of questions**				3-5
		• Explain the importance of practitioner-level questioning in uncovering cybersecurity risks, dependencies, and assumptions.	2.3ff	2	

		• Formulate diagnostic, strategic, and operational questions that challenge assumptions and reveal hidden systems, workflows, and cultural vulnerabilities. • Apply structured inquiry techniques to identify root causes and guide more adaptive, risk-informed decisions. • Use scenario-based questioning to prioritize risks and clarify practitioner decision points. • Recognize how a questioning culture underpins proactive cybersecurity and sets the foundation for measurement and continuous improvement			
1.5	**Strategy-risk**				3-5
		• Explain the inseparability of strategy and risk in modern cybersecurity • Apply the space-time analogy to understand the dynamic relationship between strategic goals and risk decisions. • Analyze how integrating strategy and risk improves decision-making, prioritization, and resilience. • Evaluate the consequences of siloed strategy and risk management using real-world scenarios	2.4.2.2, 2.5ff, 5.3.1.4, 5.4.2.5, 5.4.2.6	2	
2.1	**Systems Thinking Fundamentals**				3-5
		• Define and distinguish system structure, behavior, and culture in cybersecurity contexts. • Analyze how these system elements interact to create feedback loops, delays, and unintended consequences. • Apply systems thinking tools (e.g., causal loops, iceberg, behavior-over-time graphs) to identify risks and leverage points. • Evaluate how targeted structure, behavior, or culture interventions can improve system resilience. • Recognize the importance of whole-system visibility to minimize system blindness and siloed thinking.	3.0, 3.2ff, 3.2.3, 3.2.4, 6.3.7	2	

2.2	**Strategy-Risk, Reinforce & Operationalize**				4-5
		• Reinforce the inseparability of strategy and risk as a single entity in cybersecurity • Apply the strategy-risk lens to analyze how business decisions create both opportunity and exposure • Develop operational approaches for integrating strategy-risk thinking into daily cybersecurity practices • Design processes that enable cross-functional teams to collaborate on strategy-risk alignment • Evaluate existing organizational structures and workflows for strategy-risk integration gaps	2.5ff, 3.3.2, 3.4.1.2, 3.4.2, 5.4.2.5, 5.4.2.6, 5.4.2.7, 5.4.3	3	
2.3	**Deep Dive into the CPD Model**				4-5

		• Explain how the CPD Model integrates value creation, protection, delivery, and assurance
		• Use the CPD Model to analyze workflows and supply chains, identifying assurance mechanisms.
		• Map real-world processes to CPD loops with embedded assurance feedback.
		• Apply CPD to design workflows that answer:
		  ○ "How do you know?"
		  ○ "How can you be sure?"
		• Evaluate CPD interventions using feedback loops, leverage metrics, and 3D Knowledge Model insights.
			4.3ff, 5.4.2.7	2	

2.4	**MVC Operationalized by the CPD Model**				3-5
		• Describe how the CPD loops activate and align with the MVC overlay to support digital business value and resilience. • Identify how each MVC is operationalized through CPD-based workflows. • Map NIST-CSF core functions to CPD and MVC to bridge high-level strategy with operational execution. • Analyze organizational workflows for alignment gaps or reinforcements between CPD and MVC. • Evaluate how CPD and MVC integration promote adaptive, scalable, and culture-aware practices within cybersecurity ecosystems.	3.4.2, 4,2,1ff, 4.3ff, 4.4ff, 5.4.2.6, 5.4.2.7	3	
2.5	**Be the Meance**				4-5
		• Apply use case and misuse case to anticipate threats and surface systemic vulnerabilities. • Develop scenario-based adversarial models that expose blind spots in digital workflows and cultural practices • Integrate misuse case thinking into risk discovery, assurance planning, and future measurement design. • Explain the behavioral and cultural implications of the "be the menace" mindset across teams and systems.	2.5ff, 2.6ff, 3.3 through 3.3.2, 3.3.4ff, 8.3ff	3	

3.1	**DVMS as a Governance Overlay**				3-5
		• Describe the DVMS as a governance overlay and differentiate it from traditional frameworks, particularly aligning digital value management, strategy, and risk appetite with operational execution. • Map existing organizational workflows, structures, and practices to the seven Minimum Viable Capabilities (MVC) to identify gaps and improvement opportunities. • Analyze how the DVMS overlay supports governance and assurance through its iterative feedback loops: Governance/Assurance, Strategy/Governance, and Governance/Execution. • Evaluate how organizational culture and leadership influence the success or failure of governance and assurance mechanisms. • Assess governance gaps and recommend improvements using DVMS overlay principles, emphasizing scalability, cultural alignment, and sustainable innovation.	3.4ff, 4.2 ff, 5.4.2.5 through 5.4.2.7, 5.4.3, 8.2ff	2	
3.2	**Minimum Viable Capabilities (MVC)**				4-5
		• Explain the seven Minimum Viable Capabilities (MVC) as universal, non-optional activities that underpin cybersecurity effectiveness and business value delivery. • Map real-world workflows and operational processes to the MVC to identify strengths, silos, and improvement opportunities. • Analyze how MVC integration within the CPD Model's Governance-Execution loop enables scalable, adaptive cyber-resilience. • Evaluate cultural and structural barriers to MVC effectiveness using the 3D Knowledge Model's Z-axis (culture and leadership). • Recommend prioritized interventions that strengthen MVC performance and alignment with strategic goals and risk posture.	4.2ff, 4.3ff, 5.7ff, 6.3ff, 8.2.2, 8.2.3, A-ff	3	

3.3	**QO-QM Validation & Metrics**				4-5
		• Explain the GQM (Goal-Question-Metric) approach as a method for turning goals into operational measurement. • Apply the QO-QM (Question-Outcome–Question-Metric) framework to align strategy-risk with practitioner-relevant outcomes. • Build GQM trees and QO-QM mappings using role-based and event-based templates. • Validate metrics using the 3D Knowledge Model's behavioral (X), structural (Y), and cultural (Z) lenses. • Use GQM and QO-QM to audit and refine existing measurement systems for strategic alignment and continual improvement.	2.2ff 2.4ff, 3.4.2 5.4.2.5, 5.4.2.7, 8.2.2, 8.2.3,	3	
3.4	**FastTrack™ Approach**				3-4
		• Sequence and justify the deployment of cybersecurity capabilities across the FastTrack phases based on organizational maturity, risk posture, and cultural readiness. • Adapt FastTrack progression dynamically using governance feedback loops, incident post-mortems, and Z-axis cultural diagnostics. • Diagnose cultural and structural barriers to capability adoption and propose targeted interventions using surveys, interviews, and focus groups. • Integrate incident response, contingency planning, and governance feedback into phase transitions for continual resilience. • Contrast linear and nonlinear deployment models and explain when phase reordering or looping is appropriate. • Justify capability investment at each phase using cost-of-failure and risk-based analysis aligned with strategic priorities.	2,2ff, 2.5ff 3,3,2, 3.4.2, 5.4.2.7, 5.5ff, 6.2ff 8.2.2, 8.2.3	3	

3.5	**Risk Team-structure & Collaboration**				3-4
		• Describe the roles, responsibilities, and structural configuration of an effective cross-functional Risk Team. • Analyze how the Risk Team operationalizes the DVMS, MVC, and QO-QM approaches to inform governance, assurance, and decision-making. • Evaluate the influence of leadership modeling and culture on the success or failure of risk-informed collaboration. • Design a Risk Team configuration and communication plan that supports continual resilience and cultural transparency. • Recommend improvements to Risk Team operations based on scenario-driven diagnostics of structural and cultural breakdowns.	2.2ff, 3.3.2, 3.4.2, 4.2.1ff, 5.4.2.1, 5.4.3, 6.2ff 6.5.1.1, 8.2.1, 8.2.2, 8.2.3	2	
4.1	**The Four Aspects of Innovation**				3-5
		• Define and distinguish incremental, sustaining, adaptive, and disruptive innovation in cybersecurity contexts. • Analyze how each innovation type leverages low- or high-order systemic influence: • e.g., process tweaks vs. cultural shifts. • Evaluate how culture, leadership, and feedback loops enable or block innovation success. • Apply systems thinking tools to diagnose innovation barriers and opportunities. • Recommend targeted strategies to close value/capability gaps through innovation.	2.2ff 3.4ff, 3.5ff, 4.3 5.6.1.1, 8.3ff	4	

4.2	**Nonlinear Adoption – Revisiting Phases**				4-5
		• Explain the concept of nonlinear adoption in cybersecurity and digital value management, contrasting it with linear, phase-gate models. • Describe how organizations "adopt and adapt" by revisiting and iterating on earlier capability improvement and deployment phases in response to incidents, feedback, or changing business needs. • Analyze real-world scenarios in which adaptation versus strict adherence to a plan improved resilience, learning, or innovation. (inline case study) • Apply systems thinking tools to map feedback loops that trigger adaptation, including cultural, technical, and leadership drivers. (tools from the book) • Recommend strategies for fostering a culture and governance environment that encourages adaptive practice, psychological safety, and continuous improvement. (inline case study)	3.3ff, 4.2ff, 4.3ff, 5.2.2, 5.4ff 5.5ff, 5.6ff, 6.5ff, 8.2.3, 8.2.4	4	
4.3	**DVCMM**				3-4
		• Define the four DVCMM maturity levels (0–3) and their characteristics for each MVC. • Benchmark organizational maturity by mapping existing practices to DVCMM criteria for Govern (policy alignment, oversight) and Assure (performance validation, gap identification). • Align DVCMM maturity assessments with FastTrack phases, demonstrating how Govern and Assure enable scalable capability deployment. • Analyze the impact of organizational culture (Z-axis) on Govern (leadership accountability) and Assure (transparency in audits) maturity. • Advise leadership on closing gaps in Govern (e.g., outdated policies) and Assure (e.g., ineffective metrics) to	2.2ff, 3.3.4, 4.2.3 4.3.3.6 5.5ff, 5.6ff, 6.5.4, 8.2ff, A.1, A.2, B-ff	3	

		advance maturity, and explore how this impacts the other five MVC.			
4.4	**Bridge to Day 5 – Synthesis Preparation**				4-5
		• Synthesize key insights from Days 1–4, connecting systems thinking, governance, measurement, capability maturity, innovation, and culture into a cohesive understanding of organizational cyber-resilience. • Evaluate organizational readiness to integrate DVMS overlay, MVC, FastTrack, 3D Knowledge Model, CPD Model, DVCMM, and cultural diagnostics into real-world improvement efforts. • Formulate an initial action plan for the capstone application, identifying leverage points, maturity gaps, and cultural enablers/barriers using course concepts and models. • Reflect on personal and team learning, pinpointing areas of strength and growth opportunities to inform capstone strategy and continuous improvement.	2.2ff 3.3ff 3.4ff 3.5ff 4.2ff, 4.3ff 8.2ff, A-ff B-ff D-ff	5	

5.1	**Continual Improvement & Innovation Loops**				4-5
		• Explain the principles and value of continual improvement and innovation loops in cybersecurity and digital value management, distinguishing between single-loop (incremental) and double-loop (transformational) learning. • Analyze how feedback mechanisms, measurement, and reflection drive ongoing adaptation and resilience in organizational capabilities, practices, and culture. • Apply systems thinking tools to design and map feedback loops that support continual improvement and innovation within cybersecurity workflows and cross-functional teams. • Evaluate the impact of organizational learning, experimentation, and knowledge sharing on the effectiveness of continual improvement and innovation initiatives (in the context of the 3D Knowledge Model). • Recommend strategies for embedding continual improvement and innovation practices into daily operations, leveraging metrics, feedback, and cultural enablers to sustain adaptive, resilient performance.	2.2ff, 3.2.4, 3.3ff, 3.4ff, 3.5ff, 4.2ff, 4.3ff, 5.5ff, 5.6ff, 8.2.3, 8.3ff, A-ff, B-ff	5	

5.2	**Integrating Governance, Measurement, & Culture**				4-5
		• Integrate DVMS governance overlay, measurement (GQM/QO-QM), and culture (3D Knowledge Model Z-axis) into a unified approach for managing and improving cybersecurity and digital value management. • Analyze how cultural factors (leadership behavior, psychological safety, communication) affect the effectiveness of governance and measurement systems. • Design feedback loops that connect governance decisions, measurement practices, and cultural diagnostics to drive adaptive improvement and resilience across organizational systems. • Evaluate the impact of integrated governance, measurement, and culture on organizational maturity, capability deployment, and risk management, referencing DVCMM and FastTrack models. • Recommend actionable strategies for aligning and sustaining governance, measurement, and cultural practices to support continuous improvement and cyber-resilience.	2.2ff, 3.4ff, 3.5ff, 4.2ff, 6.4ff, 6.5ff, 8.2ff, A-ff, B-ff, D-ff	5	

5.3	**Capstone Synthesis & Practitioner Reflection**				4-5
		• Synthesize course approaches and models (3D Knowledge Model, CPD Model, DVMS overlay, MVC, FastTrack, DVCMM) into a unified strategy for addressing a complex cybersecurity challenge, demonstrating mastery of systems thinking, governance, and cultural alignment. • Design and defend a practitioner-level action plan that integrates leverage points, maturity benchmarks, feedback loops, and cultural diagnostics to achieve measurable improvements in cyber-resilience and digital value delivery. • Evaluate the effectiveness of proposed interventions using scenario-based outcomes, stakeholder impact analysis, and alignment with organizational strategy-risk priorities. • Reflect on personal growth as a cybersecurity practitioner, identifying strengths, gaps, and strategies for continuous learning and leadership development.	Everything excluding Chapter 1 and Appendix C.	5	

Examination structure and assessment

The course assessment consists of a comprehensive online examination to evaluate your mastery of course content at advanced cognitive levels. The examination emphasizes application, analysis, and evaluation skills (Bloom's Taxonomy Levels 3-5) rather than simple recall of facts.

Examination structure

Duration

150 minutes

Format

The **open-book** examination has 65 multiple-choice questions with a single correct answer from four choices (A, B, C, D).

Delivery

Online, proctored

Prerequisites: Successful completion of the NCP010 Practitioner course

Resources

You may reference the book and unaltered class materials (i.e., slides and case study without annotation)

Assessment approach

Questions test your ability to apply concepts, analyze scenarios, and evaluate information rather than memorize content. Each question has one correct answer that is worth one point.

Scoring and requirements:

- Total Points: 65 points possible
- Passing Score: 39 points (60%)
- Grading: Pass/Fail based on achieving the minimum threshold

The open-book format reflects the real-world nature of professional practice, where information access is available, but critical thinking and application skills are essential for success.

Examination voucher distribution

Upon completing the course, students will be given a voucher for the examination to use at their discretion and timing.