The Industry Leader in NIST Cybersecurity Framework Cyber Resilience Certified Training

tso
a Williams Lea company

The Mission

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.

To achieve this, the DVMS Institute offers a series of in-depth accredited training courses to enable stakeholders to 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.

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.

NIST-CSF Awareness Course

Purpose: General Introduction

Course participants 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.

The course is based on the NIST Cybersecurity Framework and the DVMS Institute's Fundamentals of Adopting the NIST Cybersecurity Framework Publication.

This DVMS® NIST Cybersecurity Framework Foundation certification training course is accredited by APMG International, assured by NCSC/GCHQ in the UK, and recognized by DHS-CISA in the U.S.

Target Audience

The NIST-CSF Awareness course is designed for:

- Executives seeking to further understand digital business, digital business risk and how the NIST Cybersecurity Framework can help manage those risks and ensure improved governance.
- Organisations of all sizes seeking to begin changing the cybersecurity culture within an organisation enabling employees to understand why and how digital business and associated cybersecurity risk materialises and what can be done about it.
- Individual students seeking to enter the NIST training program

Delivery Format

The course is offered in the following formats:

- 1/2-Day In-Person or Virtual, Open Enrollment, Instructor-Led Classroom
- 1-Day In-Person or Virtual, Private, Instructor-Led Classroom Workshop
- Self-Paced Video Learning (1.2 Hours for Completion)

Course Modules

Module 1: Digital Business Evolution

- Understanding Cyber Risk – Key concepts and the impact on digital business.
- Strategic Leadership – Cybersecurity responsibilities of executives and decision-makers.
- Implementation & Compliance – Risk management, regulatory adherence, and security frameworks.
- Business Integration – Embedding cybersecurity into operations and digital transformation.

Module 2: Introducing Cyber Risk

- Cyber Risk Fundamentals – Exploring key concepts, threat actors, and the risk equation (threat x vulnerability x impact).
- Threat Analysis & Response – Understanding cyber-attack methods and the Lockheed Martin Cyber Kill Chain.
- Risk Assessment & Management – Identifying, analyzing, and prioritizing threats, and implementing mitigation strategies.
- Cybersecurity Strategy & Defense – Embedding security controls, employee education, and creating response plans for incidents.

Module 3: Adopting and Adapting NIST-CSF

- Adopting the NIST Cybersecurity Framework – Steps to implement and adapt the NIST-CSF for optimized cyber risk management.
- Shifting Cybersecurity Philosophy – Moving from a reactive, IT-centric approach to a proactive, strategic business capability.
- Strategic Integration – Aligning cybersecurity risk management with organizational goals and enterprise risk management.
- Cybersecurity as a Business Imperative – Emphasizing cybersecurity as a core, ongoing business and governance concern.

Certification

Upon completion, course participants will gain:

- Professional Development Credits
  - 8 CEU Credits for the Instructor-Led Workshop
  - 1 CEU Credit for the Self-Paced Video program
- Digital Badge
- Certificate of Completion

General Information

Included within the course is the following:

- Access to an eBook version of “Fundamentals of Adopting the NIST Cybersecurity Framework”
- Learners receive 50% discount on the printed version of Fundamentals of Adopting the NIST Cybersecurity Framework

NIST-CSF Foundation Course

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.

This DVMS® NIST Cybersecurity Framework Foundation certification training course is accredited by APMG International, assured by NCSC/GCHQ in the UK, and recognized by DHS-CISA in the U.S.

Target Audience

The NIST-CSF Foundation Certificate course is targeted at individuals or teams looking to learn the fundamentals of Digital Transformation, Cybersecurity Risk Management, NIST Cybersecurity Framework and NIST-CSF Management Systems.

IT, Business and Cyber Security professionals who will play an active or passive role in engineering, operationalising and continually improving an organizations NIST-CSF programme and those looking for a baseline knowledge of the NIST-CSF who are considering a career in cyber security.

Delivery Format

The course is offered in the following formats:

- 2-Day In-Person or Virtual, Open Enrollment, Instructor-Led Classroom
- 2-Day In-Person or Virtual, Private, Instructor-Led Classroom
- Self-Paced Video Learning, (5 Hours for Completion)

Course Modules

Module 1: Looking Through the Wrong End of the Telescope

- Introductory NIST Cybersecurity Framework Course – Outlining the structure of the NIST framework and how to use it for identifying and prioritizing cybersecurity risk management in an organizational setting.
- Practitioner Program – Exploring implementing or auditing cybersecurity controls based on the NIST Cybersecurity Framework and other standards.

- Advanced Specialist Courses – Focus on specific informative references such as NIST 853 or 171, ISO 27001, CIS Controls, and others, tailored for both auditors and implementers seeking specialized skills.

Module 2: A Clear and Present Danger

- Understanding Digital Transformation – Grasp what it truly means to become digital, distinguishing between digital evolution and the more hyped concept of digital transformation.
- Navigating the Threat Landscape – Learn how the global threat landscape shapes the need for coherent cybersecurity responses to manage threats and vulnerabilities.
- Expanding the Threat Surface – Understand how digital evolution leads to an expanded threat surface and what that means for cybersecurity strategy.

Module 3: Cybersecurity and business risk

- Understanding Cyber Risk – Examine how the NIST Cybersecurity Framework helps in identifying and assessing cyber risks.
- Key Aspects of Cyber Risk – Discuss the different elements of cyber risk, including vulnerabilities, threats, risks, controls, and critical assets.
- Risk Assessment Approach – Introduce the risk assessment process used in the NIST Cybersecurity Framework to evaluate relevant risks.
- Informed Decision-Making for Controls – Use the risk assessment findings to guide decisions about the types and levels of cybersecurity controls needed to protect assets effectively.

Module 4: Introduction to the NIST-CSF

- Introduction to the NIST Cybersecurity Framework – Provide an overview of the NIST Cybersecurity Framework and its relevance to cybersecurity management.
- Understanding the Framework's Structure – Discuss the core components of the framework, including its structure and main functions.
- Exploring the Tiers and Profiling Capabilities – Explain the different tiers and profiling capabilities of the NIST framework, and how they help organizations assess their cybersecurity posture.

Module 5: Introduction to the NIST-CSF and the CPD Model

- Detailed Exploration of the NIST Cybersecurity Framework – Delve into the five core functions of the framework: identifying assets, protecting assets, detecting anomalies, establishing response procedures, and recovering capabilities.
- Risk-Based Approach – Emphasize that the framework is designed as a risk-based approach, not just a compliance-driven one, helping organizations optimize resource allocation to manage cyber risk effectively.
- Core, Tiers, and Profiles – Introduce the core, tiers, and profiles of the framework, outlining how they guide organizations in planning cybersecurity activities.
- Informative References – Provide an overview of informative references linked to the framework, offering further guidance on activity planning and specific cybersecurity objectives.

Module 6: Implementation Tiers and profiles

- Building on the Framework Core – Expand on the foundational understanding of the NIST Cybersecurity Framework by introducing the concepts of tiers and profiles.
- Assessing Risk Management Rigor – Explore how tiers help assess the relative rigor of an organization's risk management approach and evaluate the extensibility of cybersecurity capabilities into supply chains.
- Assessing Current and Future Capabilities – Discuss how profiles are used to assess current cybersecurity capabilities and serve as the basis for a risk assessment to inform future requirements.

Module 7: Beyond the Framework

- Adopting and Adapting the Framework – Explore how organizations can leverage the framework to drive continuous improvement in managing digital business capabilities.
- Supporting Organizational Initiatives – Discuss how the framework can be used to align with broader organizational goals and support initiatives for delivering sustainable digital business value.
- A Holistic Approach – Introduce a model that helps organizations think about how they create, protect, and deliver reliable digital business value while ensuring cybersecurity is integrated into these processes.

Examination

DVMS® NIST Cybersecurity Framework Foundation Exam

- 60-minute Closed-book exam
- 40 x Multiple choice questions
- Blooms Level 1 & 2
- Pass Mark: 60% or 24 marks
- Paper-based & online availability (including ProctorU)

Certification

Upon completion, course participants will gain:

- Professional Development Credits
  - 8 CEU Credits for the Instructor-Led Workshop
  - 1 CEU Credit for the Self-Paced Video program
- Digital Badge
- Certificate of Completion

General Information

Included within the course is the following:

- Access to an eBook version of "Fundamentals of Adopting the NIST Cybersecurity Framework" and "A Practitioner's Guide to Adapting the NIST Cybersecurity Framework".
- Learners receive 50% discount on the printed version of the abovementioned DVMS books.

NIST-CSF 800-53 Practitioner Course

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.

Note: Candidates must have attended and completed the NIST Cybersecurity Framework Foundation course and exam to participate in this course.

Target Audience

For IT, Business and Cyber Security professionals who will play an active or passive role in engineering, operationalising and continually improving an organisations NIST-CSF programme and those looking for a baseline knowledge of the NIST-CSF who are considering a career in cybersecurity.

Delivery Format

The course is offered in the following formats:

- 5-Day In-Person or Virtual, Open Enrollment, Instructor-Led Classroom
- 5-Day In-Person or Virtual, Private, Instructor-Led Classroom
- Self-Paced Video Learning, 16 Hours

Course Modules

Module 1: Course Introduction

- Understanding Cyber Risk – Exploring threats, risks, and systems thinking to enhance cybersecurity decision-making.
- Strategic Leadership – Aligning cybersecurity risk management with governance, assurance, and organizational capabilities.
- Implementation & Compliance – Adapting the NIST Framework 800-53 and other references for effective cybersecurity risk management.
- Business Integration – Leveraging digital value management and continual improvement models to embed cybersecurity into operations.

Module 2: Be the Menace - A Proactive Approach

- Threat Landscape Assessment – Identifying and prioritizing business systems, including hardware, software, people, and processes.
- Proactive Risk Management – Establishing controls to prevent, detect, respond to, and recover from cyber threats.
- Business Resilience – Strengthening defenses across internal operations, suppliers, and partners to mitigate risks.

Module 3: Systems: Simply, Complex, Complicated, and Resilient

- Systems Thinking – Applying a holistic approach to understanding digital business and the delivery of digital value capabilities.
- Complex Systems – Exploring the interconnectedness of organizational culture, knowledge, and information flows in supporting systems.
- Points of Leverage – Identifying opportunities to experiment and adapt systems for improved results.
- Continuous Improvement – Using systems thinking to enhance performance and drive organizational change.

Module 4: Cybersecurity and the DVMS

- Digital Value & Cybersecurity Integration – Aligning digital value management systems with cybersecurity risk management through the Z-X Model and gap analysis.
- Capability Maturity & Systems Thinking – Using a digital value capability maturity model to assess and enhance organizational capabilities for creating, protecting, and delivering business value.
- CPD Model Application – Applying systems and complex models to integrate cybersecurity risk management into organizational strategies through the create, protect, and deliver framework.
- Strategic Alignment – Employing the goal/question/metric methodology and extensions like QO-QM to align strategic goals with operational intent and define key metrics for success.

Module 5: Adapting the Way We Work

- Adaptive Work in Cybersecurity – Adapting cybersecurity capabilities in response to evolving vulnerabilities, threats, and asset values.
- Coherent & Principled Approach – Establishing structured, principled strategies to create, protect, and deliver value within an organization.
- Organizational Structure Support – Creating appropriate structures to support ongoing adaptation and risk management efforts.
- Fast Track Approach – Implementing a phased strategy to stabilize, optimize, and innovate for continuous improvement in the CPD capability.

Module 6: Cybersecurity Within a System

- Cybersecurity & Organizational Integration – Exploring how to integrate cybersecurity risk management with your organization's existing capabilities.
- Phased Approach – Implementing cybersecurity risk management through a structured, phased approach to ensure sustainability over time.
- Sustaining Capabilities – Developing strategies to maintain and evolve cybersecurity risk management capabilities to address changing threats and organizational needs.
- Program Implementation – Walking through the process of embedding cybersecurity risk management into the organization's ongoing operations and growth.

Module 7: Digital Business Risk Management

- Organizational Perspective – Examining previous concepts from the viewpoint of the organization as a whole.
- Mental Models – Exploring new mental models that individuals within the organization may need to adopt for successful integration.
- Capabilities & Practice Areas – Understanding the organization's capabilities and practice areas in the context of cybersecurity risk management.
- Dynamic Integration – Defining the dynamics needed to effectively integrate cybersecurity risk management into the processes of creating, protecting, and delivering digital capabilities and value.

Module 8: DVMS as a Scalable Overlay

- Digital Value Management System Layers – Exploring how the system operates in layers to scale according to the organization's size and needs.
- Adaptability to Business Context – Tailoring the Digital Value Management System to fit the nature, scope, governance requirements, and regulatory constraints of the organization.
- Resource Alignment – Ensuring the system aligns with resource needs to address specific threats and risks effectively.
- Governance & Risk Management – Integrating legal, regulatory, and governance considerations into the system's design to optimize cybersecurity and risk management.

Examination

Implementer vs Auditor

800-53 Practitioner Certification training – Implementer Exam:

The 800-53 Practitioner Implementer exam evaluates one's knowledge of operationalizing a NIST Cybersecurity Framework program that is fit for use within an organization and is aligned with organizational strategic policies.

800-53 Practitioner Certification training – Auditor Exam:

The 800-53 Practitioner Auditor exam evaluates one's knowledge of ensuring that a NIST Cybersecurity Framework program delivers the desired business and regulatory outcomes expected by executive leadership and government regulators.

The DVMS™ 800-53 Practitioner Implementer or Auditor Exams:

- 65 multiple-choice questions per exam
- 150-minute exam
- Pass Mark – 50% (33 marks)
- Open book
- Blooms Level 3,4, & 5
- Paper-based & online availability (including ProctorU)

Certification

Upon completion, course participants will gain:

- 32 CEU credits
- Digital Badge
- Certificate of Completion

General Information

Included within the course is the following:

- Access to an eBook version of "Fundamentals of Adopting the NIST Cybersecurity Framework" and "A Practitioner's Guide to Adapting the NIST Cybersecurity Framework".
- Learners receive 50% discount on the printed version of the abovementioned DVMS books.

tso
a Williams Lea company