

NCSP[®]

PRACTITIONER CERTIFICATION

COURSE OUTLINE



Course Introduction

Instructor Introduction
Course Introduction
Course Introduction

Chapter 01 - Course Introduction

Course Introduction

Lesson: Course Organization

Learning Outcomes
Welcome to the Course!
Why Are You Here?
Using Bloom's Taxonomy
What do you Expect?
Housekeeping Online
Daily Routine, Quizzes & Exercises
NCSP Practitioner Exam
NCSP Bootcamp Exam
Getting Started in the Classroom
Agenda

Lesson: Setting the Stage

Constantly Evolving Threat Landscape
Adopt the NIST-CSF & Adapt an Informative Reference
Cybersecurity Adopt & Adapt - Governance & Management
Use an Adaptive Way to Work
Rapid Adoption & Rapid Adaption FastTrack
Continual Improvement & Implementation of Cybersecurity

Chapter 02 - Digital Transformation & Cybersecurity

Digital Transformation & Cybersecurity

Digital Transformation & Cybersecurity
Learning Outcomes

Lesson: DX as a Practitioner

The Industrial Era & the Digital Era
Entering the Digital Era
Unique Strategic Challenges of the Digital Era
Digital Strategy Concepts
Organizational Culture Defined
The Need for a Digital Culture
Get Your Culture READY to Transform!
Digital Transformation Readiness Framework

Framework Structure
Operational Sustainability - Principle Themes
Attributes of Operational Sustainability
Organizational Agility - Principle Themes
Attributes of Organizational Agility
Strategic Agility - Principle Themes
Attributes of Strategic Agility
Disruptive Culture - Principle Themes
Disruptors are NOT Loose Cannons
Digital Readiness Framework

Lesson: DX in the Context of Cybersecurity

More about Culture Than Technology
Adopt & Adapt - DX & Cybersecurity
Agility Demands
Shared Aspects
Different Sides of the Same Coin

Lesson: Cybersecurity as a DX Catalyst

Start with Operational Sustainability
Becoming Agile
Establish a Strategic Approach

Summary: Digital Transformation & Cybersecurity

Becoming Digital Ready
Interdependencies - DX/Cybersecurity
Checkpoint

Chapter 03 - Threat Landscape

Threat Landscape

Learning Outcomes
Introduction

Lesson: Threat Actors: Agile & Creative

Take Advantage of Everything: All Information Has Value
Threat Actor Creativity
Threat Actors Agile & Adaptive
Threat Actors Exploit Vulnerabilities

Lesson: Attacks

Generic Attack Types
Typical Attack Profile
Lockheed-Martin Cyber Kill Chain
Typical Mitigation Controls
External Attacks
Insider Attacks
Verizon 2019 Data Breach Investigation* Report (DBIR)*

Verizon 2019 DBIR Summary*

Lesson: Challenges

Vulnerability Contributors
Indicators for Cybersecurity Issues
Most Prevalent Deficiencies
IT & Cybersecurity
Organizational Challenges
Lack of Cybersecurity Budget/Funding
Cybersecurity Funding Impacts All Organizations
Increased Threat Sophistication
CISO Actions

Lesson: Organizational Response to Threat Landscape

New Approach to Information Security Management (ISM)
Understand Cyber Risk
Understand Importance of Controls
Breaches - Lessons Learned
Analysis of Target Breach - Background
Analysis of Target Breach - Threat Actor Reconnaissance Phase
Analysis of Target Breach - Threat Actor Infection & Infiltration Phases
Analysis of Target Breach - Threat Actor Data Collection & Exfiltration Phases
General Lessons from Target Breach
Lessons from Target Breach for each Attack Phase (1)
Lessons from Target Breach for each Attack Phase (2)
Analysis of Home Depot Breach - Background
Lessons from Home Depot Breach
Analysis of Sony Breach - Background
General Lessons from the Sony Breach
Lessons from the Sony Breach - Infection & Infiltration
Lessons from the Sony Breach - Data Collection & Exfiltration

Lesson: Absolute Prevention Not Possible

Ongoing Improvement is Critical
Cybersecurity Isn't Implemented & Done
Make Strategic Commitment to Inculcate Cybersecurity into Culture
Trust & Verify
Not Just Awareness & Training - Deterrence
What Is Cybersecurity Deterrence
Start with Program to Raise Awareness
Make CS Training & Awareness Critical Part of Organizational DNA
Training Alone Insufficient

Summary: Threat Landscape

Threat Actors
Attacks

Challenges
Organizational Response to Threat Landscape
Absolute Prevention Not Possible
Checkpoint

Chapter 04 - The Controls

The Controls

Learning Outcomes
Overall Approach & Control Selection
Control Selection Rationale
Introduction to Cybersecurity Controls

Lesson: Initiation & Basic Controls

Controls Phased Adoption
Controls – Order of Precedence (Initiation & Basic [Startup])
CIS Control 17 - Implement a Security Awareness & Training Program
CIS Control 17 - Implement a Security Awareness & Training Program Sub Controls
CIS Control 19 - Incident Response & Management
CIS Control 19 - Incident Response & Management Sub Controls
CIS Control 1 - Inventory & Control of Hardware Assets
CIS Control 1 - Inventory & Control of Hardware Assets Sub Controls
CIS Control 2 - Inventory & Control of Software Assets
CIS Control 2 - Inventory & Control of Software Assets Sub Controls
CIS Control 3 - Continuous Vulnerability Management
CIS Control 3 - Continuous Vulnerability Management
CIS Control 4 - Controlled Use of Administrative Privileges
CIS Control 4 - Controlled Use of Administrative Privileges
CIS Control 5 - Secure Configurations
CIS Control 5 - Secure Configurations
CIS Control 6 - Maintenance, Monitor & Analysis of Audit Logs
CIS Control 6 - Maintenance, Monitor & Analysis of Audit Logs

Lesson: Foundation Controls

CIS Control 7 - Email & Web Browser Protections
CIS Control 7 - Email & Web Browser Protections
CIS Control 8 - Malware Defenses
CIS Control 8 - Malware Defenses
CIS Control 9 - Limitations & Control of Network Ports, Protocols & Services
CIS Control 9 - Limitations & Control of Network Ports, Protocols & Services
CIS Control 10 - Data Recovery Capabilities
CIS Control 10 - Data Recovery Capabilities
CIS Control 11 - Secure Configurations for Network Devices
CIS Control 11 - Secure Configurations for Network Devices
CIS Control 12 - Boundary Defenses

CIS Control 12 - Boundary Defenses
CIS Control 13 - Data Protection
CIS Control 13 - Data Protection
CIS Control 14 - Control Access Based on the Need to Know
CIS Control 14 - Control Access Based on the Need to Know
CIS Control 15 - Wireless Access Control
CIS Control 15 - Wireless Access Control
CIS Control 16 - Account Monitoring & Control
CIS Control 16 - Account Monitoring & Control
Lesson: Organizational & Recovery Controls
CIS Control 18 - Application Software Security
CIS Control 18 - Application Software Security
CIS Control 20 - Penetration Tests & Red Team Exercises
CIS Control 20 - Penetration Tests & Red Team Exercises
Recovery NIST-CSF - NIST 800-53
Summary: Controls
Controls – Order of Precedence (Initiation & Basic ((Startup)))
Checkpoint

Chapter 05 - Adopt & Adapt

Adopt & Adapt

Learning Outcomes

Lesson: The Context of Adopt & Adapt

Introduction to Adopt & Adapt

Adopt: What's Included in Governance for Cybersecurity?

Adapt: What's Included in Management for Cybersecurity?

Lean Thinking Applied

Cybersecurity Adopt & Adapt - Governance & Management

Management: Operationalization of Cybersecurity

Lesson: Cybersecurity & Culture

Culture Defined & Thoughts About Culture

Cultural Patterns

Characteristics of Culture Types: How They Process Information

How to Change Your Culture

Culture & Cybersecurity

Final Thoughts on Culture

Lesson: Where We Are

Determine Current State

Determinative Model

Flow of Improvement

Flow of Communication

Flow of Work

3D Knowledge Flow Model
Consultant's View of the Flows
Summary: Adopt & Adapt
The Context of Adopt & Adapt
Cybersecurity & Culture
Where We Are?
Checkpoint

Chapter 06 - Adaptive Way of Working

Adaptive Way of Working

Learning Outcomes

Lesson: Introduction to Adaptive Way to Work

Adaptive Approach Reduces Waste, Delivers Value
Little Gap & Big Gap
Quick Review
Approach
Leverage Cross-functional Teams
Lots of small projects
Work Structure
Facilitate Learning
Everything is Subject to Improvement
Try Something New in "the Small"
Be Proactive
Organizational Change
Change Requires Engagement
Focus on Small Steps Toward a Goal, Not the Whole

Lesson: How to Get Started

Adaptive Approach
Work in phases
Ask Questions: Method (How), Not Capability (Binary Choice)
Develop Small Requirements
Prioritize Based on Most Valuable Thing to do "Next"
Focus on Value, Outcomes, Costs & Risks
Develop Different Flow Patterns

Summary: Adaptive Way of Working

Introduction to Adaptive Way to Work
How to Get Started
Checkpoint

Chapter 07 - Rapid Adoption & Rapid Adaptation FastTrack

Rapid Adoption & Rapid Adaptation FastTrack

Learning Outcomes
Rapid Adoption & Adaptation Using FastTrack

Lesson: Rapid Adoption

Determine Risk Appetite
Establish Cybersecurity Governance
Assess Cybersecurity Capabilities
Balance Resources & Risks
Balance Resource Optimization Model
Optimized Resources

Lesson: Rapid Adaptation

Cybersecurity Assessment
Impact on People, Practice & Technology
Impact Flows
Implementation Groups
Review Center for Internet Security Controls*
Take a Phased Approach
Phase 0: Initiation
Phase 1: Establish Cybersecurity Beachhead
Phase 2: Expand Defensible Perimeter
Phase 3: Refine & Tailor
FastTrack - Implement/Improve Cycles

Summary: Rapid Adoption & Rapid Adaptation FastTrack

Rapid Adoption & Adaptation Using FastTrack
Rapid Adoption
Rapid Adaptation
FastTrack - Implement/Improve Cycles
Checkpoint

Chapter 08 - CIIS Practice

CIIS Practice

Chapter: CIIS Practice
Learning Outcomes

Lesson: Ongoing Practice of Cybersecurity

Set the Stage for Continual Improvement
Build a Learning Organization
How to Scope Ongoing Improvement
Identify Business Systems Most at Risk
Verify or Create Inventory of Hardware & Software Assets
Think Like A Threat Actor
Mitigate & Protect
Learn & Improve
Embed

Overall Flow

Lesson: NIST 7-step Improvement

NIST 7-step

Step 1: Prioritize & Scope

Step 2: Orient

Step 3: Create Current Profile

Step 4: Conduct Risk Assessment

Step 5: Create Target Profile

Step 6: Determine, Analyze & Prioritize Gaps

Step 7: Implement action plan

Lesson: Cybersecurity Maturity Model Certification CMMC

Origins of CMMC

CMMC Model Framework

CMMC Model Level Descriptions - 1 & 2

CMMC Model Level Descriptions - 3 & 4

CMMC Model Level Descriptions - 5

Examples of Level 1 to 3 Practices

Examples of Level 4 & 5 Practices

Lesson: Integrate Cybersecurity

Balancing Loop

Escalation (Archetype)

People, Practice & Technology: Improvement Cycle

Assess Cybersecurity Posture: Implementation Cycle

FastTrack - Combined Implement/Improve Cycles

Summary: CIIS Practice

Set the Stage for Continual Improvement

Overall Flow

NIST 7-step

Origins of CMMC

FastTrack - Combined Implement/Improve Cycles

Checkpoint

Chapter 09 - Course Summary

Course Summary & Wrap Up