AI Cyber Defense Academy

Risk Management

One-Day Training Virtual

ecfirst

> "AI will change the world more than anything in the history of mankind. More than electricity!"
>
> Kai-Fu Lee

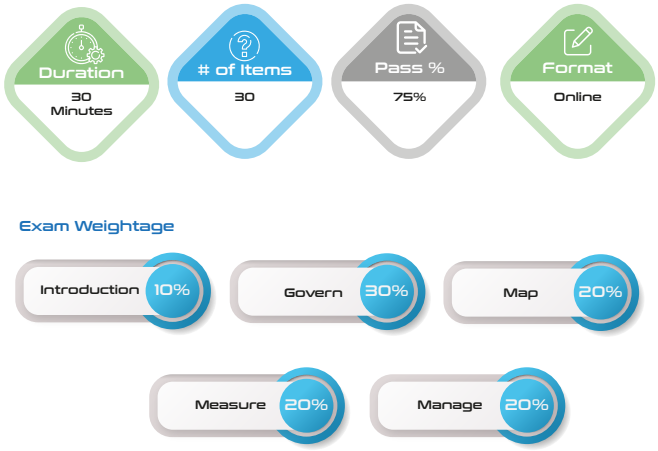
> "AI deployment will add $15.7 trillion to the global GDP by 2030."

Learning Objectives

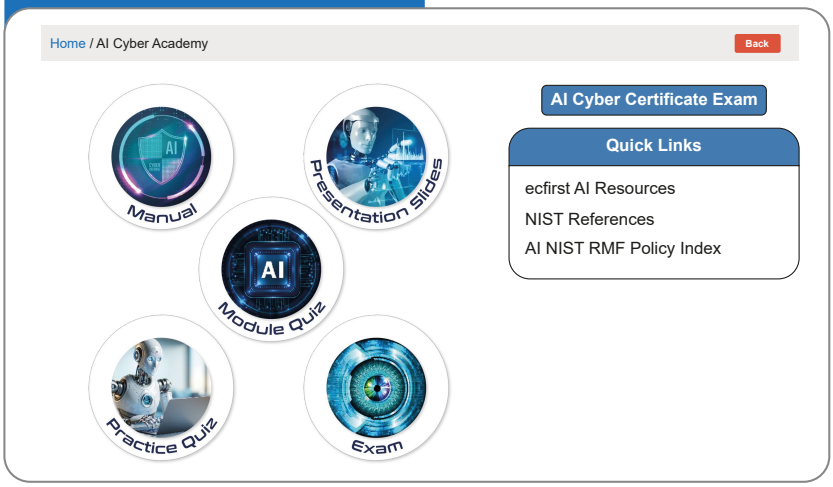
In this AI cyber defense training program,

- Examine the NIST AI Risk Management Framework (RMF)
- Review valued AI resources for risk management
- Step through a sample AI risk management policy
- Identify AI cyber defense controls
- Determine key phases for an enterprise AI risk assessment

AI Cyber Certificate Exam



AI Academy Portal



Takeaways

AI Cyber Defense Academy

Risk Management

One-Day Training Virtual

ecfirst

Course Outline

Module 1 Introduction

- Basics of AI
- Ethical and societal impacts
- Development process, limitations, and challenges
- Attack vectors and risk assessment
- Countermeasures and secure development practices

Module 2 AI RMF Resources

- Tailoring organization-specific AI RMF
- Developing an effective Risk Management Framework for AI
- Resources for managing IT and AI system risks

Module 3 Govern

- Overseeing AI systems' lifecycle
- Infusing risk management in AI processes
- Ensuring responsible and ethical AI use
- Regulatory alignment and trust building

Module 4 Map

- Framing AI risks
- Understanding the AI ecosystem
- Identifying opportunities for informed decision-making

Map
Context is recognized and risks related to context are identified

Module 5 Measure

- Analyzing and monitoring AI risks
- Assessing AI project success and areas for improvement
- Implementing testing, assessment methodologies, and documentation

Measure
Identified risks are assessed, analyzed, or tracked

Module 6 Manage

- Strategic AI initiative planning
- Executing, controlling, and optimizing AI activities
- Resource allocation and performance monitoring
- Data management for AI project integrity

Manage
Risks are prioritized and acted upon based on a projected impact

Module 7 Getting Started

- Setting up AI governance structures
- Prioritizing and aligning cyber and AI capabilities
- Building AI RMF policies
- Establishing ecfirst AI Defense methodology

Module 8 AI Assessment Lab

- Structured environment for AI assessment
- Addressing compliance and cyber priorities
- RMF scoping to maximize AI benefits
- Optimizing AI solutions for business value

AI Defense, *Beyond Cyber*