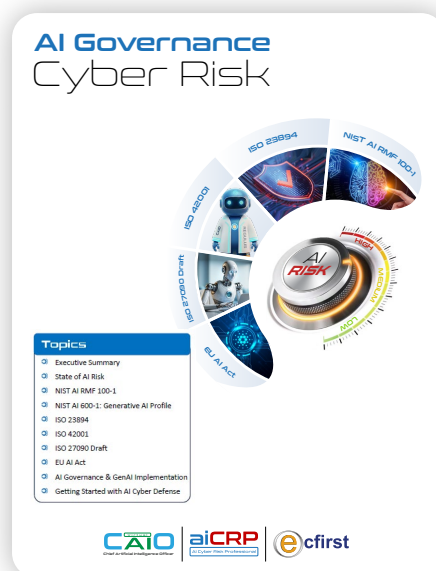




Table of Contents

Why ecfirst for AI.....	2
aiCRP Certification.....	3
AI Governance Executive Bootcamp	4
Virtual CAIO Program	5
AI Risk Management Assessment	6
AI Penetration Test	7
AI Penetration Test Tiers	8
AI Solutions	9
AI Playbook	10



Peter.Harvey@ecfirst.com



www.ecfirst.com

AI | Why ecfirst?



AI Governance Methodology

Virtual AI Governance and Risk Management Program

CAIO
Chief Artificial Intelligence Officer



aiCRP
AI Cyber Risk Professional
Online | Self-Paced

AI Cyber Risk Certification Training

Securing AI
Finding Vulnerabilities

HITRUST and AI



AI Governance Reference

AI and Gen AI Governance Playbook



AI Governance Playbook



Learn More

HITRUST
Authorized External Assessor

AI Risk Management Assessment
AI Cyber Certification

AI Toolkit
www.ecfirst.biz/ai



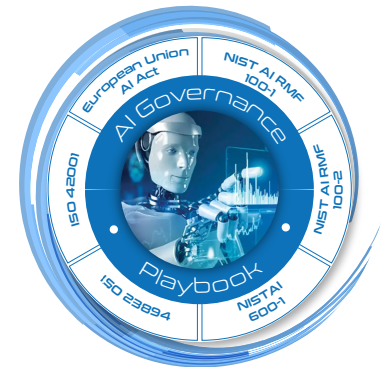
The Industry's First AI Cyber Risk Management Training Program



Unlock the World's First AI Playbook

AI Governance Playbook

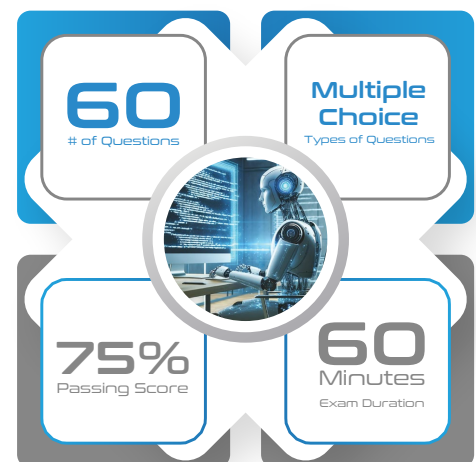
AI Governance Playbook



What's in it for you?

- ✦ Examine the NIST AI Risk Management Framework (RMF)
- ✦ Review valued AI resources for risk management including ISO 23894 and ISO 42001
- ✦ Understand EU AI Act requirements and risk classifications
- ✦ Step through a sample AI risk management policy
- ✦ Identify AI cyber defense controls
- ✦ Determine key phases for an enterprise AI risk assessment

AI Exam Specifications



Digital Badge

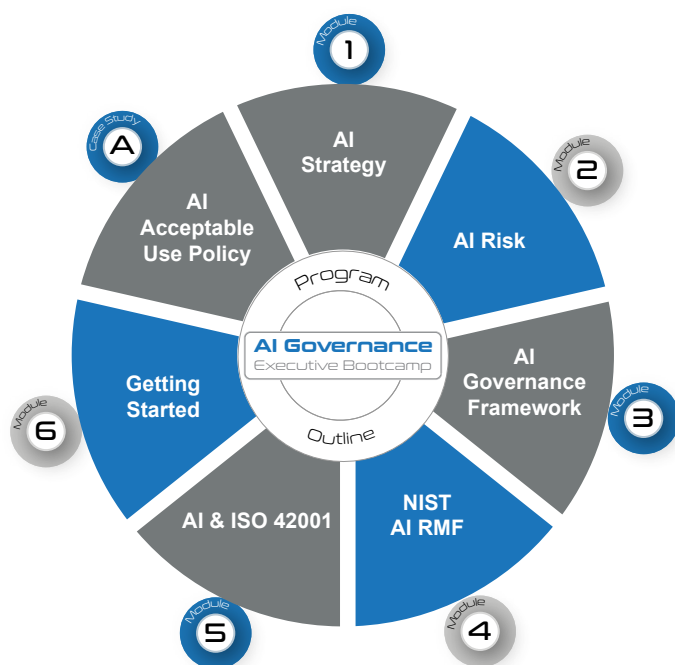
ecfirst also offers a Digital Badge with your certification. There is no fee for this service and acceptance is totally up to you.



Summary

- Practitioner-focused AI governance program for business, compliance, risk, and technology leaders.
- Covers AI governance frameworks, ethics, risk management, and regulatory obligations including NIST AI RMF and ISO 42001, and the European Union AI Act.
- Includes practical governance implementation, policy development, and knowledge-check assessments throughout the program.

Program Outline



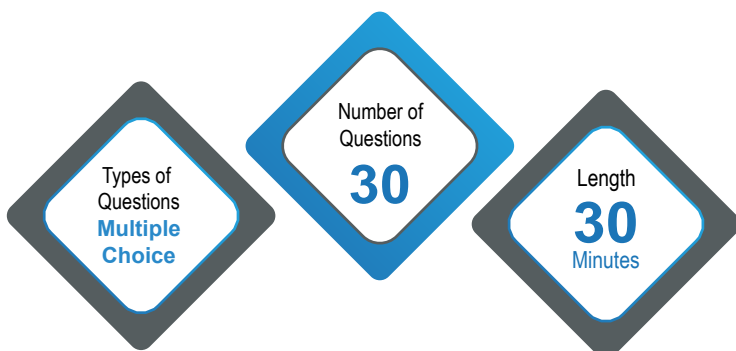
Learning Objectives

- Align AI strategy, governance, and investment planning with enterprise business objectives
- Apply AI governance frameworks including NIST AI RMF and ISO 42001
- Classify and manage AI risks under the European Union AI Act and emerging regulations
- Implement ethical AI principles, governance controls, and responsible AI deployment practices
- Develop AI governance artifacts including AI policies, governance committees, and executive reporting mechanisms

Intended Audience

- C-Suite executives, board members, and AI governance leaders responsible for enterprise AI oversight and strategy.
- Risk, compliance, legal, security, and privacy professionals managing AI risk, governance, and regulatory obligations.
- Technology, data, operations, HR, finance, and public sector leaders overseeing AI development, deployment, and high-risk AI use cases.

Exam Specifications



Module Exam Weight

#	Domain	Exam Weight
Module 1	AI Strategy	10%
Module 2	AI Risk	20%
Module 3	AI Governance Framework	20%
Module 4	NIST AI RMF	25%
Module 5	AI & ISO 42001	15%
Module 6	Getting Started	5%
Case Study	AI Acceptable Use Policy	5%

AI Governance

Establish a customized AI Governance and Risk Management program, tailored for your organization. The virtual CAIO program from ecfirst, provides opportunities in the following areas,

- ❖ Establish an AI Governance program
- ❖ Build a customized AI acceptable use policy
- ❖ Develop an AI risk management policy
- ❖ Access to **aiCRP** an online, self-paced training program (Complimentary)
- ❖ Tailored presentations to senior leadership and the Board
- ❖ Perform an AI cyber risk assessment based on the NIST AI RMF

Customized

Flat Rate

Fixed Cost

Flexible

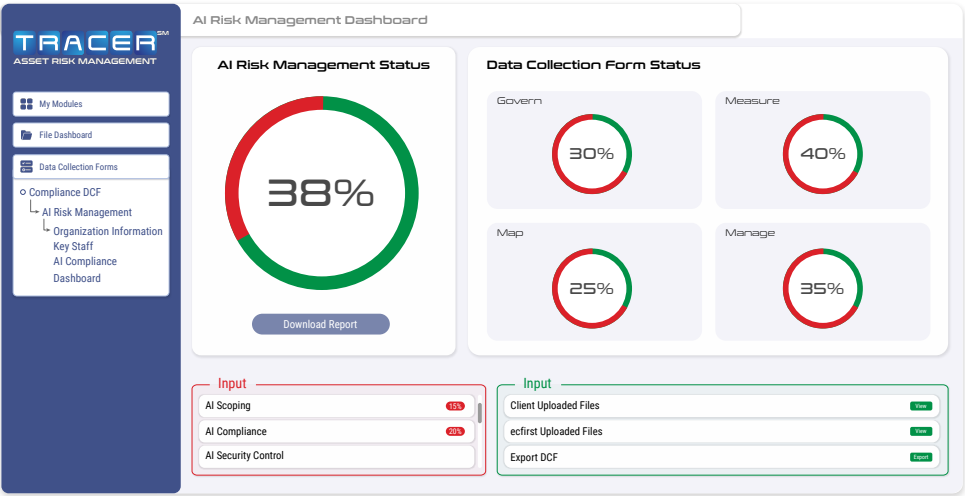
AI Governance Program



AI Risk Management Assessment



AI Risk Assessment



Sources



Purpose

Identify and validate vulnerabilities in AI-enabled systems, including LLM applications, RAG environments, AI agents, custom machine learning models, AI-enabled APIs, and AI-integrated business workflows.

- ✓ Know exactly what gets tested, how we test it, and what you walk away with - before we start.
- ✓ Full transparency on scope, methodology, and outcomes - so there are no surprises.



Your AI Attack Surface



Customized Approach



Our Methodology



Executive Dashboard



AI Penetration Test Service

This assessment is designed to determine whether an AI system can be manipulated, abused, bypassed, or exploited in a way that impacts confidentiality, integrity, availability, privacy, compliance, or business operations.

This is not a traditional pen test run with AI tools - it's a security assessment of your AI itself.



Tests whether your AI can be manipulated, bypassed, or exploited



Combines API pen testing, red team techniques, prompt testing, and ML security



Covers confidentiality, integrity, availability, privacy, and compliance risks

AI Penetration Test Objective



Probes LLMs, agents, RAG pipelines, and ML models for exploitable weaknesses



Tests prompt injection, jailbreaks, data leakage, and privilege escalation



Validates access controls across users, roles, departments, and tenants



Assesses tool integrations and connected business systems for abuse paths



Reviews governance, logging, and alerting against real AI attack frameworks

Why This Matters at the Board Level



Cyber insurers are increasingly asking whether AI systems have been security tested – and some are adding exclusions where they have not.



Regulatory enforcement, including OCR, is extending to AI tools that handle patient and other regulated data.



Your vendor secures its infrastructure – you own how you configure and integrate it. That is where exploitable findings can emerge.

AI Penetration Test Tiers

Tier 1
Bronze

Focus:
Single LLM / Chatbot
Best for:
A single chatbot or customer-facing LLM
Duration: 1-2 Weeks

Tier 2
Gold

Focus:
Multi-component + RAG
Best for:
AI systems with retrieval, memory,
or multiple components
Duration: 2-3 Weeks

Tier 3
Platinum

Focus:
Enterprise AI + Agents + ML
Best for:
Enterprise deployments with agents, tools,
and ML models
Duration: 4-6 Weeks

Key Deliverables by Tier

Deliverable	Tier 1 Bronze	Tier 2 Gold	Tier 3 Platinum
Executive Summary	✓	✓	✓
AI Attack Narrative	✓	✓	✓
Technical Report	✓	✓	✓
Prompt Injection Results	✓	✓	✓
RAG & Vector Security	✗	✓	✓
Agent & Tools Abuse Results	✗	✗	✓
Model Security Results	✗	✗	✓
Framework Mapping Matrix	✓	✓	✓
Findings Matrix	✓	✓	✓
Retest & Attestation Letter	✗	Add-on	✓

Attestation Letter is issued only upon a completed retest. Retesting is not offered at Tier 1, available as a paid add-on at Tier 2, and included at Tier 3.

Framework and Compliance Alignment



AI Specific

OWASP LLM Top 10

OWASP ML Security Top 10

OWASP Top 10 for Agentic Applications

MITRE ATLAS

NIST AI RMF



Regulatory

HIPAA

PCI DSS

SOC 2

GDPR

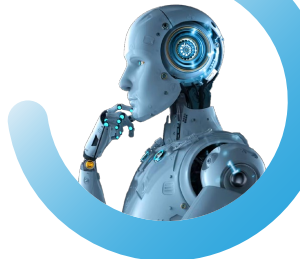
ISO/IEC 42001

EU AI Act

CMMC

NIST SP 800-171

AI Governance Bundle

**CAIO**
Chief Artificial Intelligence OfficerAI Governance
On-Demand ConsultingAI Risk
Assessment
ReportABC
CORP

ecfirst

**aiCRP**AI Cyber Risk Professional
Online | Self-PacedAI Certification
Training Program

HITRUST & AI Solutions

AI Risk Management
Assessment51
Controls

- ✦ Aligned with NIST AI RMF + ISO/IEC 23894:2023
- ✦ Identify gaps and prioritize actions
- ✦ Non-certified; focused on improving AI risk posture

AI Security Assessment
& Certification44
Requirements

- ✦ Formal HITRUST AI Security Certification
- ✦ Standalone or paired with HITRUST e1/i1/r2
- ✦ Designed for AI platforms, developers and deployers

HITRUST
Authorized External Assessor

AI Penetration Test



- Your AI Attack Surface
- Customized Approach
- Our Methodology
- Executive Dashboard

Quick Links

- Home
- AI Guidance
- NIST AI RMF
- Explore the Playbook



AI Guidance



NIST AI RMF



Explore the Playbook

Function	Title	AI Actors	Topics
Govern	GOVERN 1.1	Governance and Oversight	Legal and Regulatory Governance AI Actor Training
Govern	GOVERN 1.2	Governance and Oversight	Trustworthy Characteristics Governance Validity and Reliability Safety Secure and Resilient Accountability and Transparency Explainability and Interpretability Privacy Fairness and Bias
Govern	GOVERN 1.3	Governance and Oversight	Risk Tolerance Governance
Govern	GOVERN 1.4	Governance and Oversight	Risk Management Governance Documentation
Govern	GOVERN 1.5	Governance and Oversight Operation and Monitoring	Monitoring Governance Continual Improvement
Govern	GOVERN 1.6	Governance and Oversight	Risk Management Governance Data Documentation
Govern	GOVERN 1.7	AI Deployment Operation and Monitoring	Decommission Governance
Govern	GOVERN 2.1	Governance and Oversight	Governance Risk Culture
Govern	GOVERN 2.2	Governance and Oversight	Governance AI Actor Training
Govern	GOVERN 2.3	Governance and Oversight	Governance Risk Tolerance

Previous 1 2 3 4 5 ... 8 Next

