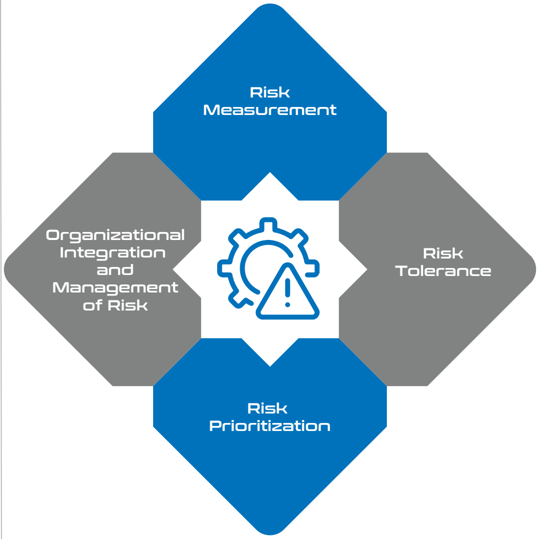
An Infographic

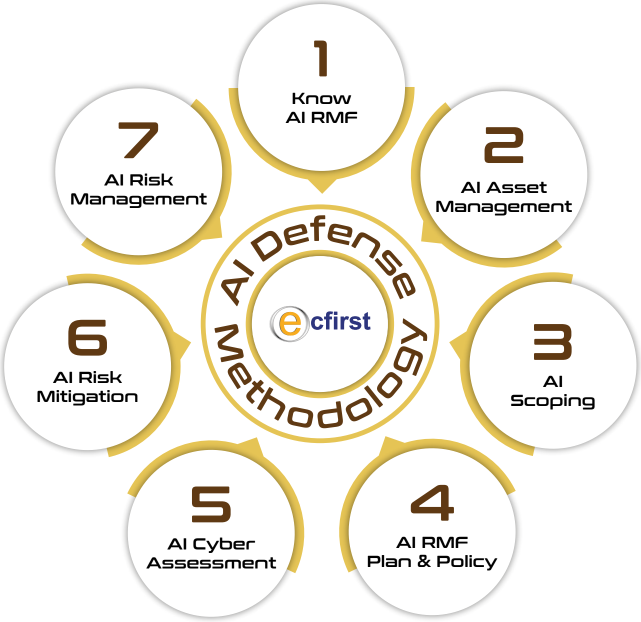
AI Cyber Risk

NIST Risk Management Framework

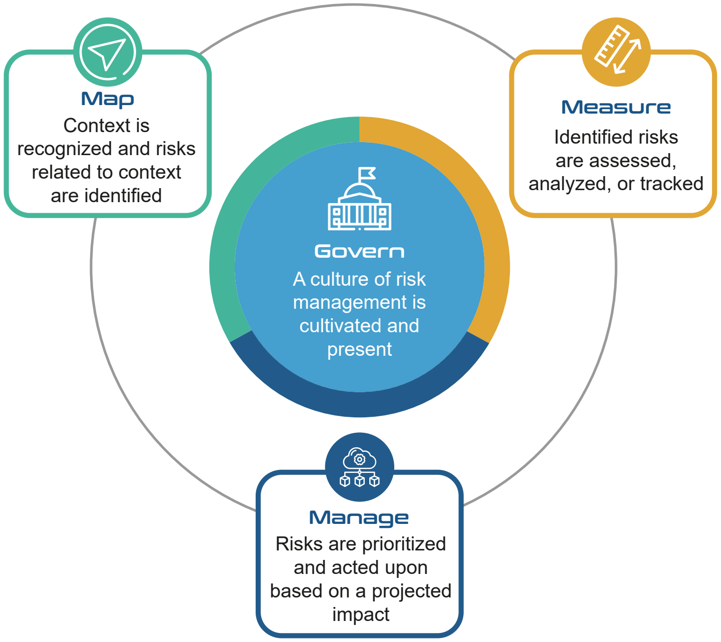
Challenges for AI Risk Management

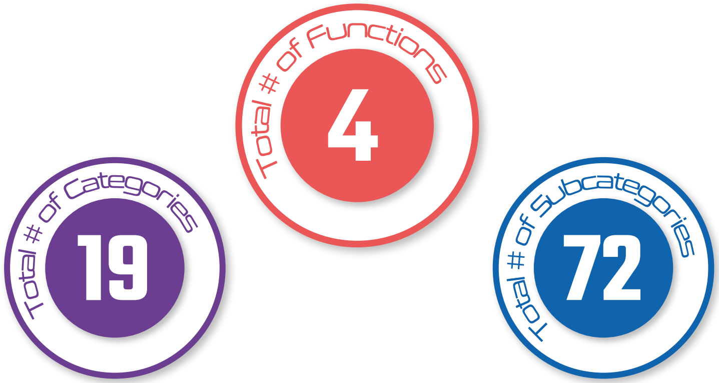


AI Risk Management



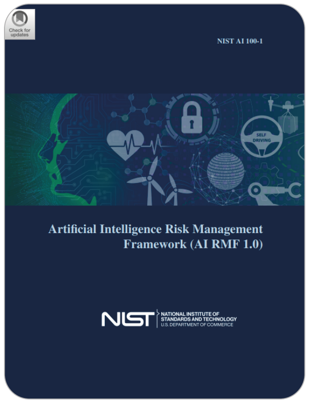
AI NIST RMF


Map
Context is recognized and risks related to context are identified
Measure
Identified risks are assessed, analyzed, or tracked
Govern
A culture of risk management is cultivated and present
Manage
Risks are prioritized and acted upon based on a projected impact



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

Source

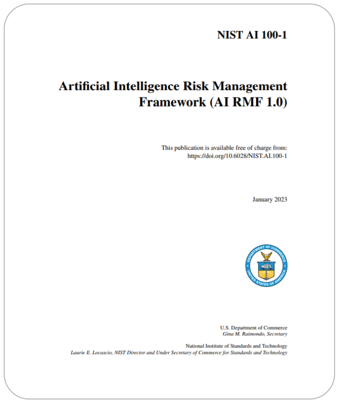


Check for updates

NIST AI 100-1

Artificial Intelligence Risk Management Framework (AI RMF 1.0)

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE



NIST AI 100-1

Artificial Intelligence Risk Management Framework (AI RMF 1.0)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.AI.100-1

January 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

aiCRP AI Cyber Risk Professional | ecfirst

AI Defense, *Beyond Cyber*

Uday Ali Pabrai

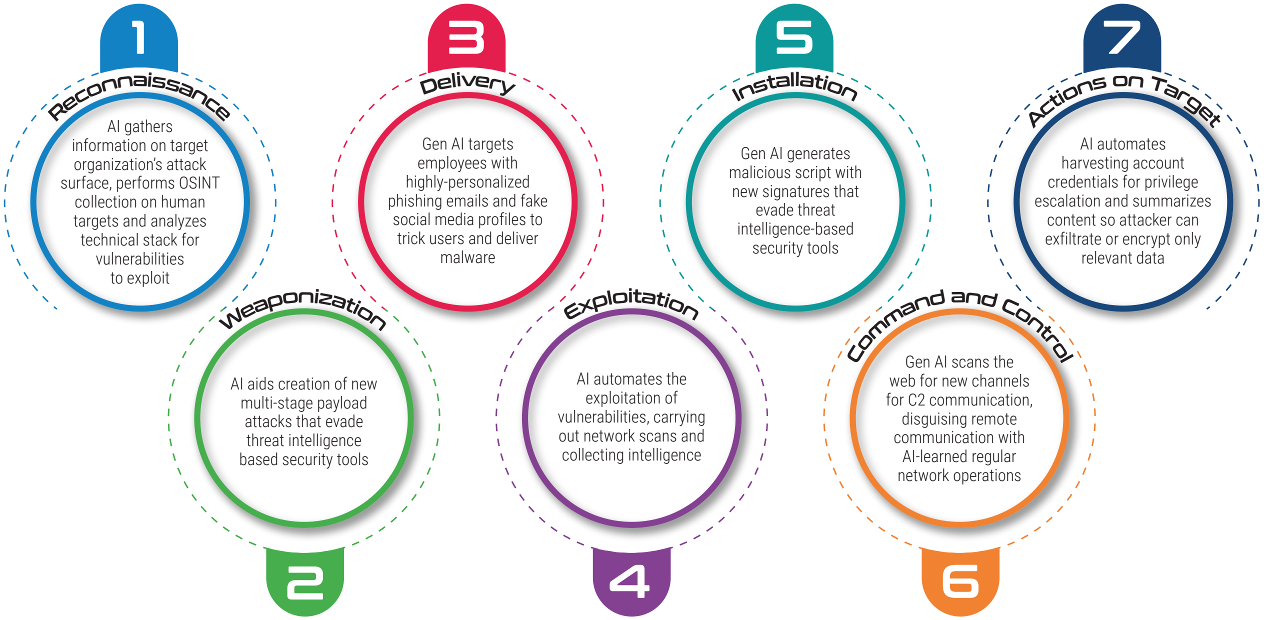
Global AI Cyber Defense Thought Leader

An Infographic

AI Cyber Risk

NIST Risk Management Framework

AI Cyber Kill Chain



1 Reconnaissance

AI gathers information on target organization's attack surface, performs OSINT collection on human targets and analyzes technical stack for vulnerabilities to exploit

2 Weaponization

AI aids creation of new multi-stage payload attacks that evade threat intelligence based security tools

3 Delivery

Gen AI targets employees with highly-personalized phishing emails and fake social media profiles to trick users and deliver malware

4 Exploitation

AI automates the exploitation of vulnerabilities, carrying out network scans and collecting intelligence

5 Installation

Gen AI generates malicious script with new signatures that evade threat intelligence-based security tools

6 Command and Control

Gen AI scans the web for new channels for C2 communication, disguising remote communication with AI-learned regular network operations

7 Actions on Target

AI automates harvesting account credentials for privilege escalation and summarizes content so attacker can exfiltrate or encrypt only relevant data

> “In deep learning, there's no data like more data. The more examples of a given phenomenon a network is exposed to, the more accurately it can pick out patterns and identify things in the real world.”
>
> Kai-Fu Lee

Getting Started with AI

Organization aligns the AI system with the organization's objectives.

Organization maintains an inventory of AI data, models, and systems that it uses and/or develops.

Organization conducts BIA on AI systems at least annually, considering the criticality of the impact, tangible and intangible impacts, and criteria used to establish the overall impact.

Organization maintains documentation of consideration for stakeholders in the context of the risk management process for AI systems.

Organization defines the scope of its risk management activities, taking into consideration the objectives and purpose of the AI systems.

Dr. Lee cautions us about the truly dramatic upheaval that AI will unleash and how we need to start thinking now on how to address these profound changes that are coming to our world.

Kai-Fu Lee

aiCRP AI Cyber Risk Professional | ecfirst

AI Defense, *Beyond Cyber*

Global AI Cyber Defense Thought Leader

An Infographic

AI Cyber Risk

NIST Risk Management Framework

AI Function - GOVERN

Govern
A culture of risk management is cultivated and present

- GOVERN is a cross-cutting function that is infused throughout AI risk management and enables the other functions of the process.
- Attention to governance is a continual and intrinsic requirement for effective AI risk management over an AI system's lifespan and the organization's hierarchy.
- Senior leadership sets the tone for risk management within an organization.
- Documentation can enhance transparency, improve human review processes, and bolster accountability in AI system teams.

6 # of Categories

19 # of Subcategories

Govern 1
Policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks are in place, transparent, and implemented effectively

Govern 2
Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks

Govern 3
Workforce diversity, equity, inclusion, and accessibility processes are prioritized in the mapping, measuring, and managing of AI risks throughout the lifecycle

Govern 4
Organizational teams are committed to a culture that considers and communicates AI risk

Govern 5
Processes are in place for robust engagement with relevant AI actors

Govern 6
Policies and procedures are in place to address AI risks and benefits arising from third-party software and data and other supply chain issues

aiCRP
AI Cyber Risk Professional

ecfirst

AI Defense, *Beyond Cyber*

Global AI Cyber Defense Thought Leader

An Infographic

AI Cyber Risk

NIST Risk Management Framework

AI Function - MAP

Map

Context is recognized and risks related to context are identified

- The MAP function establishes the context to frame risks related to an AI system. The AI lifecycle consists of many interdependent activities involving a diverse set of actors.
- AI actors in charge of one part of the process often do not have full visibility or control over other parts and their associated contexts.
- Outcomes in the MAP function are the basis for the MEASURE and MANAGE functions. Without contextual knowledge and awareness of risks within the identified contexts, risk management is difficult to perform.

5 # of Categories

18 # of Subcategories

Map 1

Context is established and understood

Map 3

AI capabilities, targeted usage, goals, and expected benefits and costs compared with appropriate benchmarks are understood

Map 5

Impacts to individuals, groups, communities, organizations, and society are characterized

Map 2

Categorization of the AI system is performed

Map 4

Risks and benefits are mapped for all components of the AI system including third-party software and data

aiCRP AI Cyber Risk Professional | ecfirst

AI Defense, *Beyond Cyber*

Global AI Cyber Defense Thought Leader

An Infographic

AI Cyber Risk

NIST Risk Management Framework

AI Function - Measure

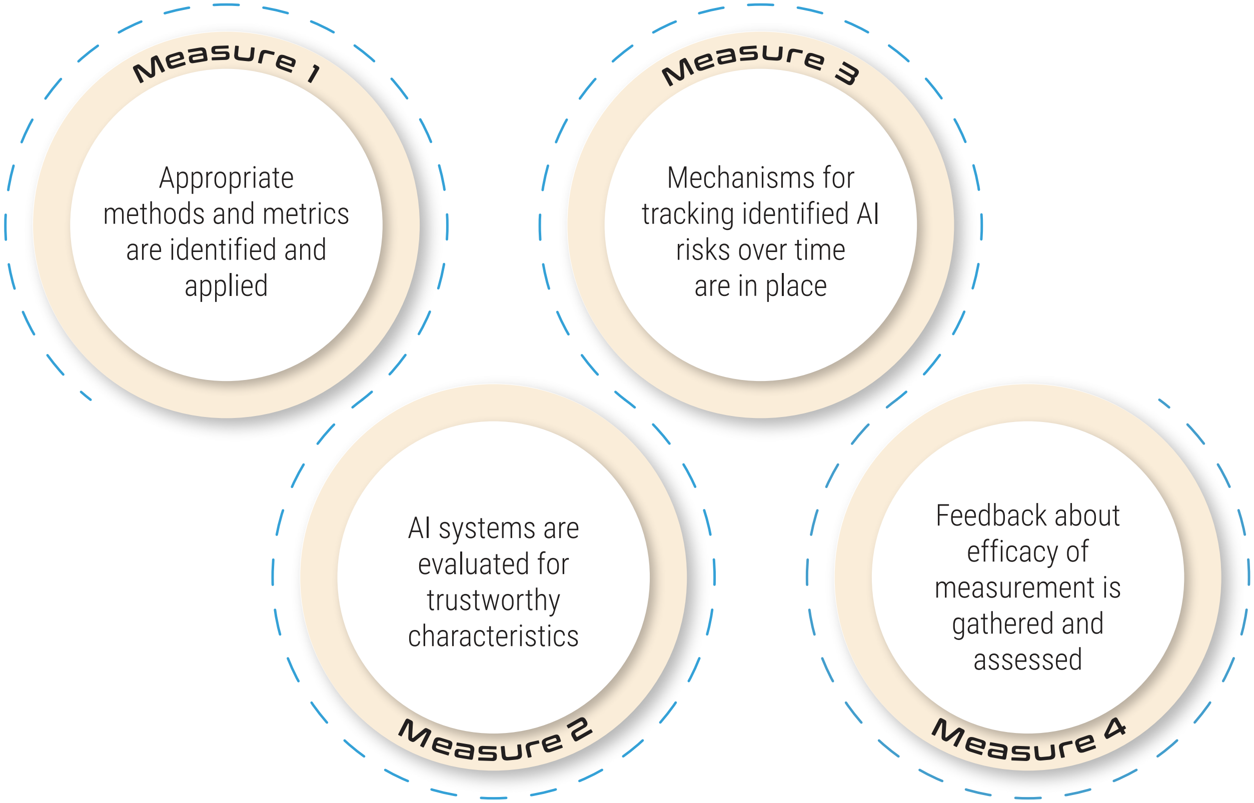
Measure

Identified risks are assessed, analyzed, or tracked

- The Measure function employs quantitative, qualitative, or mixed-method tools, techniques, and methodologies to analyze, assess, benchmark, and monitor AI risk and related impacts.
- It uses knowledge relevant to AI risks identified in the MAP function and informs the MANAGE function.
- AI systems should be tested before their deployment and regularly while in operation.
- Processes developed or adopted in the MEASURE function should include rigorous software testing and performance assessment methodologies with associated measures of uncertainty, comparisons to performance benchmarks, and formalized reporting and documentation of results.

5 # of Subcategories

22 # of Subcategories



Measure 1: Appropriate methods and metrics are identified and applied

Measure 3: Mechanisms for tracking identified AI risks over time are in place

Measure 2: AI systems are evaluated for trustworthy characteristics

Measure 4: Feedback about efficacy of measurement is gathered and assessed

aiCRP AI Cyber Risk Professional | ecfirst

AI Defense, *Beyond Cyber*

Uday Ali Pabrai

Global AI Cyber Defense Thought Leader

An Infographic

AI Cyber Risk

NIST Risk Management Framework

AI Function - Manage

Manage

Risks are prioritized and acted upon based on a projected impact

- The MANAGE function entails allocating risk resources to mapped and measured risks on a regular basis and as defined by the GOVERN function.
- Contextual information gleaned from expert consultation and input from relevant AI actors – established in GOVERN and carried out in MAP – is utilized in this function to decrease the likelihood of system failures and negative impacts.
- Systematic documentation practices established in GOVERN and utilized in MAP and MEASURE bolster AI risk management efforts and increase transparency and accountability. Processes for assessing emergent risks are in place, along with mechanisms for continual improvement.

4 # of Categories

13 # of Subcategories

Manage 1

AI risks based on assessments and other analytical output from the MAP and MEASURE functions are prioritized, responded to, and managed

Manage 3

AI risks and benefits from third-party entities are managed

Manage 2

Strategies to maximize AI benefits and minimize negative impacts are planned, prepared, implemented, documented, and informed by input from relevant AI actors

Manage 4

Risk treatments, including response and recovery, and communication plans for the identified and measured AI risks are documented and monitored regularly

aiCRP AI Cyber Risk Professional | ecfirst

AI Defense, *Beyond Cyber*

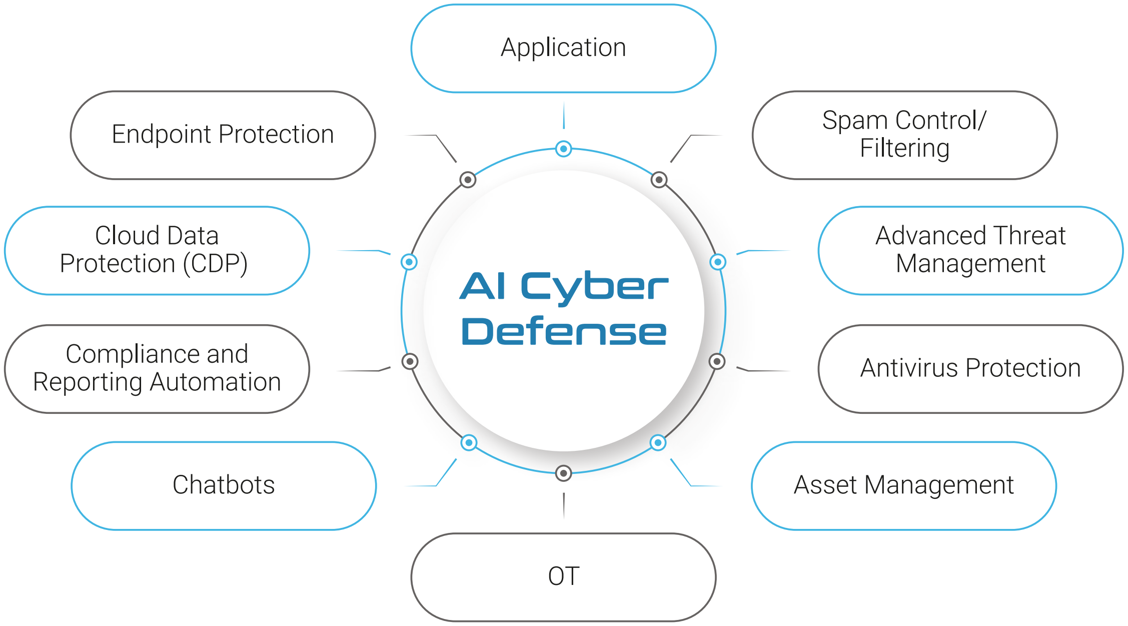
Global AI Cyber Defense Thought Leader

An Infographic

AI Cyber Risk

NIST Risk Management Framework

AI Cyber Controls



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

PricewaterhouseCoopers

$3.05 Million

Average reduction in data breach costs for organizations with fully deployed security AI and automation - by far the leading factor in reducing the overall costs of a data breach.

84%

of executives plan to prioritize generative AI cybersecurity solutions over conventional cybersecurity solutions.

Generative AI won't replace people, but people who use generative AI will replace people who don't.

> The transformation to AI is already happening all around us, whether we are aware of it or not.

Kai-Fu Lee

aiCRP AI Cyber Risk Professional | ecfirst

AI Defense, *Beyond Cyber*

Global AI Cyber Defense Thought Leader

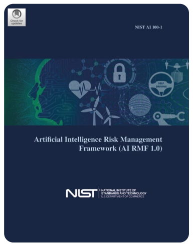
An Infographic

AI Cyber Risk

NIST Risk Management Framework

AI RMF Resources

AI RMF 1.0



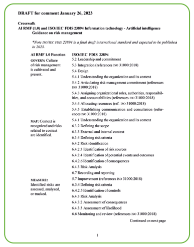
NIST AI 100-1

Artificial Intelligence Risk Management Framework (AI RMF 1.0)

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

January 26, 2023

AI RMF Crosswalks



DRAFT for comment January 26, 2023

Crosswalk
AI RMF (1.0) and ISO/IEC FDIS 23894 Information technology - Artificial intelligence
Guidance on risk management

**Note ISO/IEC FDIS 23894 is a final draft international standard and expected to be publishea in 2023.*

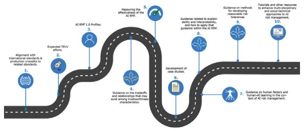
AI RMF 1.0 Function	ISO/IEC FDIS 23894
GOVERN: Culture of risk management is cultivated and present.	5.2 Leadership and commitment 5.3 Integration (references ISO 31000:2018) 5.4 Design 5.4.1 Understanding the organization and its context 5.4.2 Articulating risk management commitment (references ISO 31000:2018) 5.4.3 Assigning organizational roles, authorities, responsibilities, and accountabilities (references ISO 31000:2018) 5.4.4 Allocating resources (ref. ISO 31000:2018) 5.4.5 Establishing communication and consultation (references ISO 31000:2018)
MAP: Context is recognized and risks related to context are identified.	5.4.1 Understanding the organization and its context 6.3.2 Defining the scope 6.3.3 External and internal context 6.3.4 Defining risk criteria 6.4.2 Risk identification 6.4.2.3 Identification of risk sources 6.4.2.4 Identification of potential events and outcomes 6.4.2.6 Identification of consequences 6.4.3 Risk Analysis 6.7 Recording and reporting
MEASURE: Identified risks are assessed, analyzed, or tracked.	5.7 Improvement (references ISO 31000:2018) 6.3.4 Defining risk criteria 6.4.2.5 Identification of controls 6.4.3 Risk Analysis 6.4.3.2 Assessment of consequences 6.4.3.3 Assessment of likelihood 6.6 Monitoring and review (references ISO 31000:2018)

Continued on next page

1

January 26, 2023

AI RMF Roadmap



1. Alignment with international standards & production crossalks to related standards.
2. Expanded TEVV efforts.
3. AI RMF 1.0 Profiles.
4. Guidance on the tradeoffs and relationships that may exist among trustworthiness characteristics.
5. Measuring the effectiveness of the AI RMF.
6. Development of case studies.
7. Guidance on human factors and human-AI teaming in the context of AI risk management.
8. Guidance related to explainability and interpretability, and how to apply that guidance within the AI RMF.
9. Guidance on methods for developing reasonable risk tolerances
10. Tutorials and other resources to enhance multi-disciplinary and social-technical approaches to AI risk management.

January 26, 2023

NIST SP 1270

NIST Special Publication 1270

Towards a Standard for Identifying and Managing Bias in Artificial Intelligence

Reva Schwartz
National Institute of Standards and Technology
Information Technology Laboratory

Apostol Vassilev
National Institute of Standards and Technology
Information Technology Laboratory
Computer Security Division

Kristen Greene
National Institute of Standards and Technology
Information Technology Laboratory
Information Access Division

Lori Perine
National Institute of Standards and Technology
Information Technology Laboratory
& The University of Maryland

Andrew Burt
Patrick Hall
BNH.AI

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1270

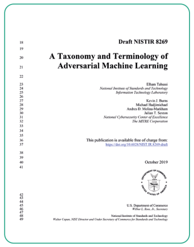
March 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

March 16, 2022

NISTIR 8269



Draft NISTIR 8269

A Taxonomy and Terminology of Adversarial Machine Learning

Elham Tabassi
National Institute of Standards and Technology
Information Technology Laboratory

Kevin J. Burns
Michael Hadjimichael
Andres D. Molina-Markham
Julian T. Sexton
National Cybersecurity Center of Excellence
The MITRE Corporation

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8269-draft

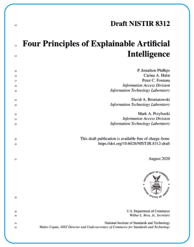
October 2019

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Draft

NISTIR 8312



Draft NISTIR 8312

Four Principles of Explainable Artificial Intelligence

P. Jonathon Phillips
Carina A. Hahn
Peter C. Fontana
Information Access Division
Information Technology Laboratory

David A. Broniatowski
Information Technology Laboratory

Mark A. Przybocki
Information Access Division
Information Technology Laboratory

This draft publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8312-draft

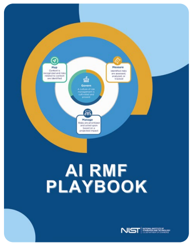
August 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

Draft

NIST AI RMF Playbook



Map
Context is recognized and risks related to context are identified

Measure
Identified risks are assessed, analyzed, or tracked

Govern
A culture of risk management is cultivated and present

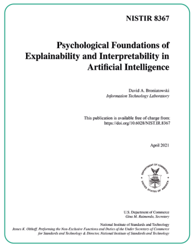
Manage
Risks are prioritized and acted upon based on a projected impact

AI RMF PLAYBOOK

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

March 30, 2023

NISTIR 8367



NISTIR 8367

Psychological Foundations of Explainability and Interpretability in Artificial Intelligence

David A. Broniatowski
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8367

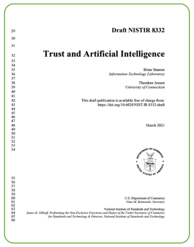
April 2021

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

April 2021

NISTIR 8332



Draft NISTIR 8332

Trust and Artificial Intelligence

Brian Stanton
Information Technology Laboratory

Theodore Jensen
University of Connecticut

This draft publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8332-draft

March 2021

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

Draft

aiCRP
AI Cyber Risk Professional

ecfirst

AI Defense, *Beyond Cyber*

Global AI Cyber Defense Thought Leader

An Infographic

AI Cyber Risk Management

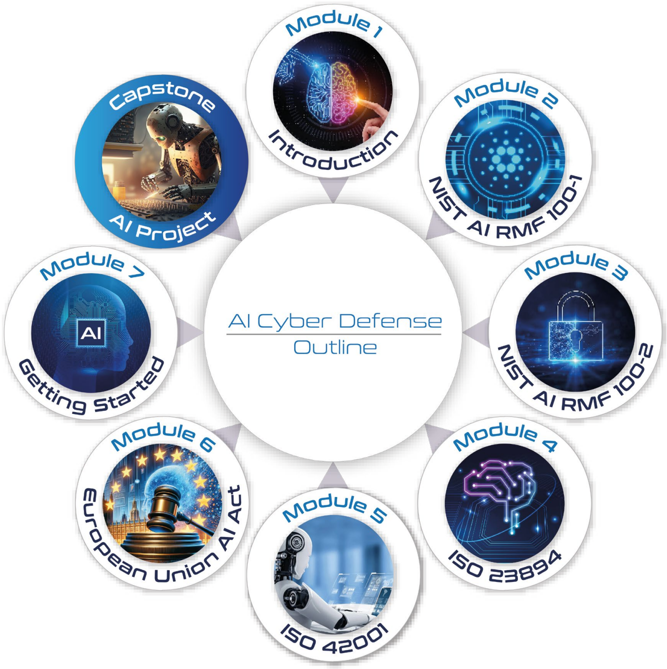
One-Day Training | Virtual

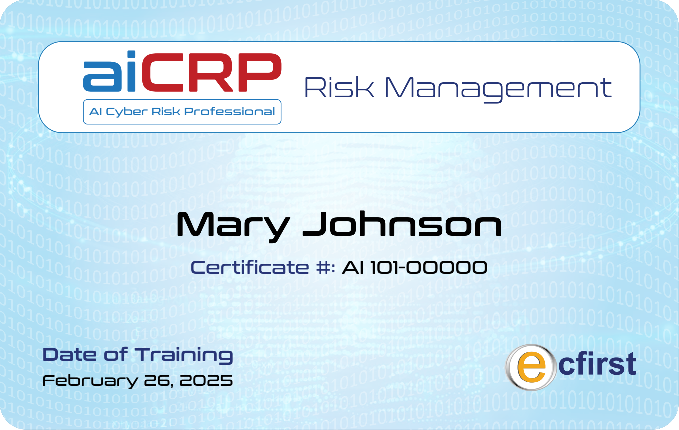
Learning Objectives

In this AI cyber defense training program:

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

Program





aiCRP Risk Management

AI Cyber Risk Professional

Mary Johnson

Certificate #: AI 101-00000

Date of Training
February 26, 2025

ecfirst

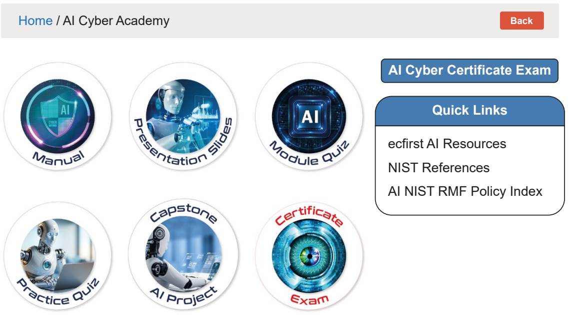
AI Cyber Certificate Exam

Duration	# of Items	Pass %	Format
30 Minutes	30	75%	Online

Exam Weightage

Introduction	25%
NIST AI RMF 100-1	25%
NIST AI RMF 100-2	25%
ISO AI	25%

AI Academy Portal



Takeaways

- AI RMF Policy Template
- AI Cyber Defense Infographic
- AI Cyber Training Certificate

aiCRP AI Cyber Risk Professional | ecfirst

AI Defense, *Beyond Cyber*

Global AI Cyber Defense Thought Leader