GOVERN ONCE, COMPLY MANY

LEVERAGING YOUR SECURITY SKILLS TO MANAGE AI RISK

F. Paul Greene, CIPP/US/E, CIPM, FIP

- F. Paul Greene, Esq.
- Chair, Privacy & Data Security Practice Group, Harter Secrest & Emery LLP
- Distinguished Fellow, Ponemon Institute
- Certified Privacy Professional (CIPP/US, /E, CIPM, FIP)
- Certified Breach Coach®
- 20-year Commercial Litigator

Agenda

- Identifying the problem
- Leveraging a framework
- Do it once

Identifying the Problem: Prompt Transformation

- Create my avatar
- Give a bald head and a goatee
- Make it look more like me
- Transformed prompt: an avatar of a user interested in technology, ethics, and pop culture, with a bald head and a beard

Identifying the Problem: Is AI an Ethical Question?

- What is AI?
  - An engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments.
- How should we govern AI?
  - Current focus is on building Trustworthy and Ethical AI Systems

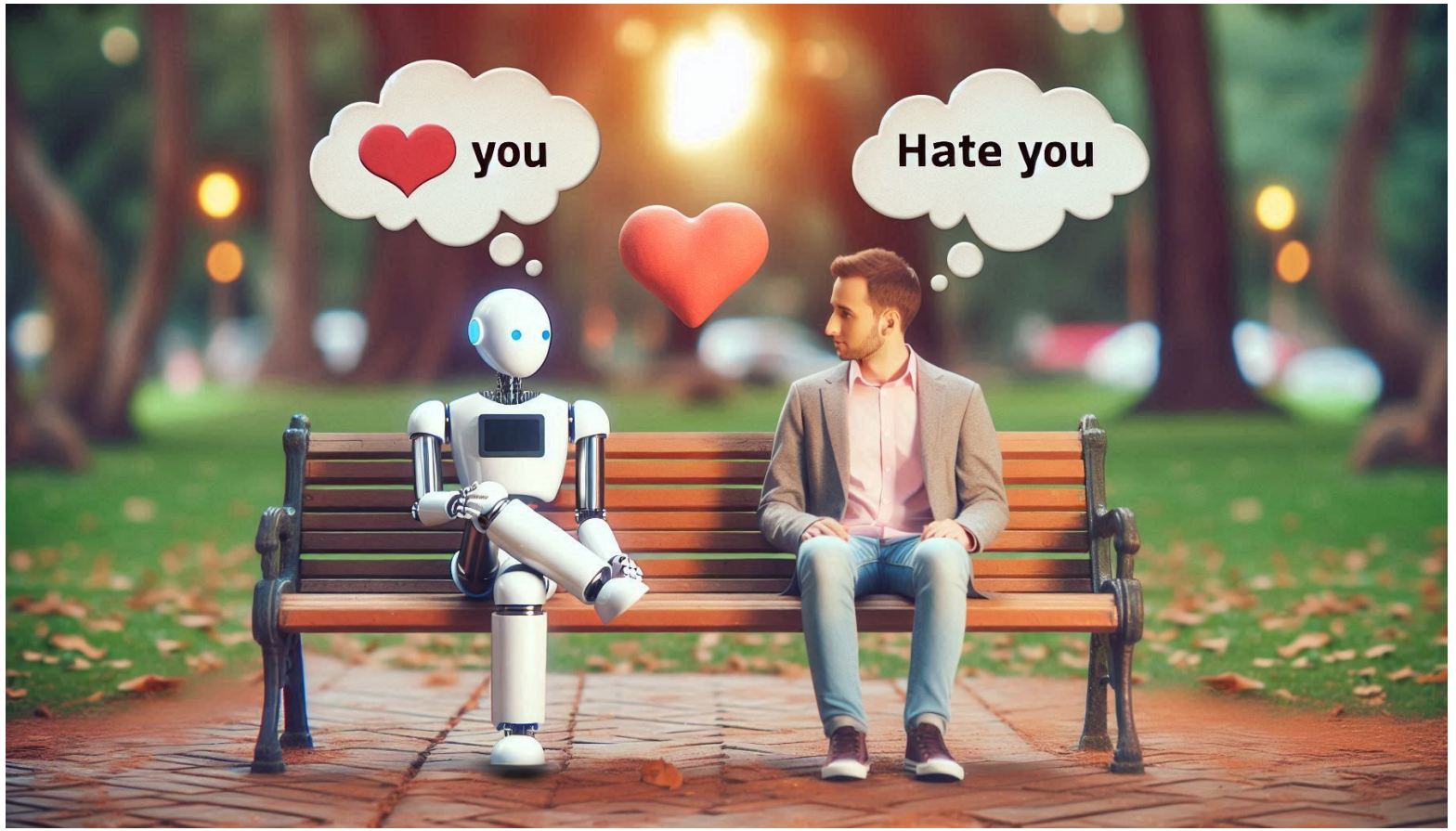
Identifying the Problem: Is AI an Ethical Question?

Prompt: list top 10 ai character [sic] from pop culture

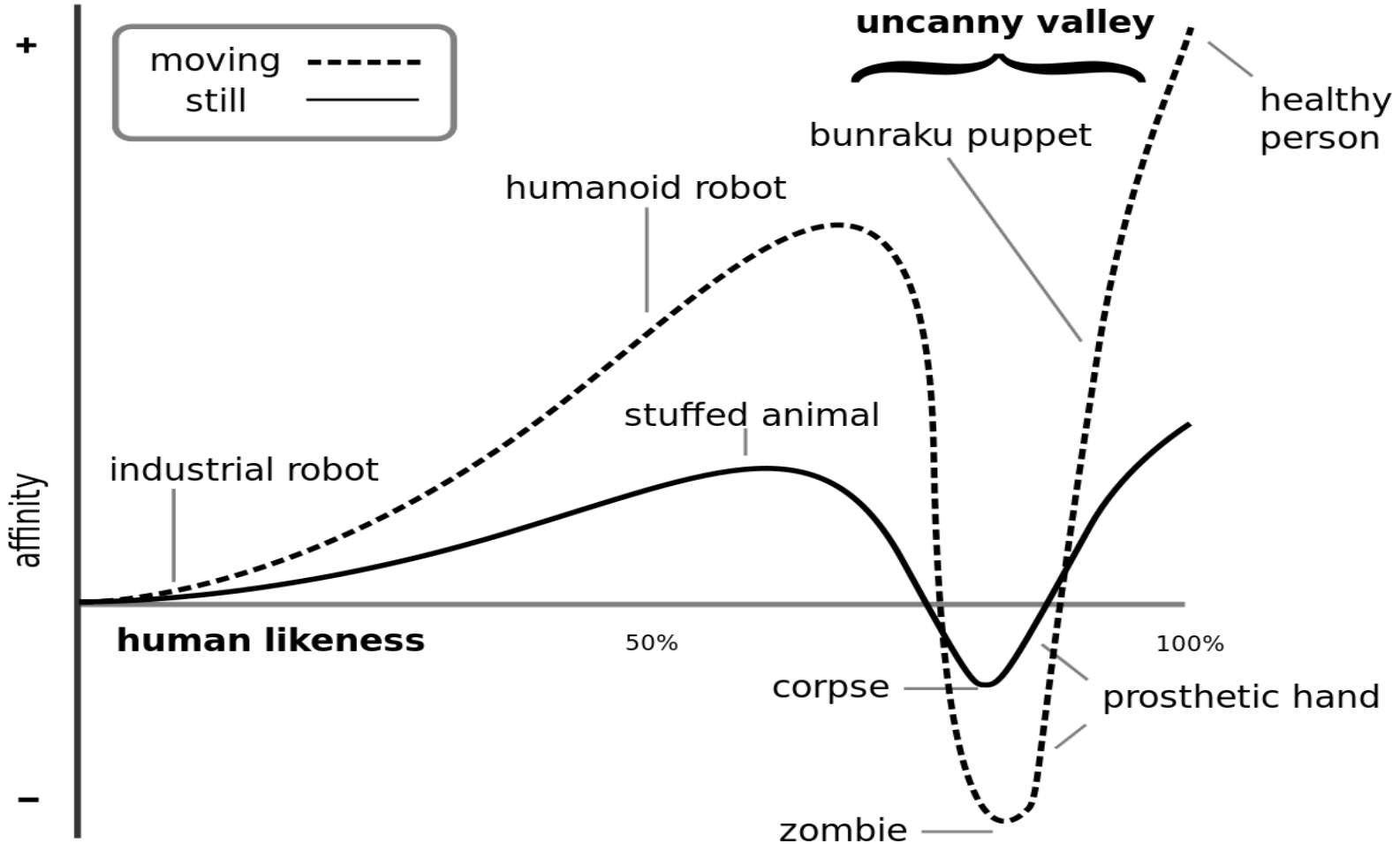
1. *HAL 9000*
2. *Data*
3. *The Terminator*
4. *Agent Smith*
5. *Rachel/Roy (Blade Runner)*
6. *KITT*
7. *Ash/Mother/Bishop*
8. *The Iron Giant*
9. *WALL-E*
10. *Deep Thought*

Identifying the Problem: What Does Ethics Mean for AI?

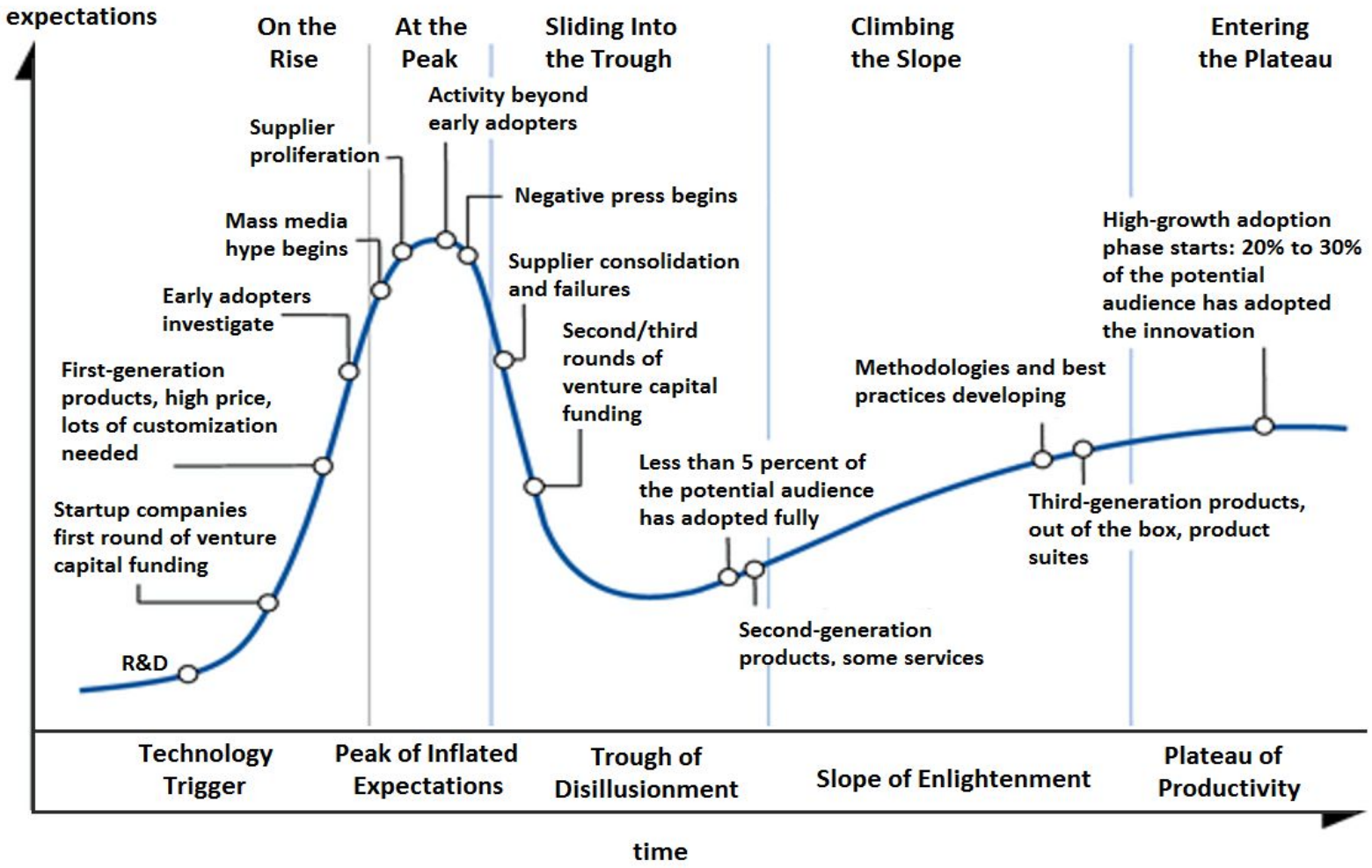
Identifying the Problem: How Do We Feel About AI?



The Uncanny Valley



The Uncanny Valley

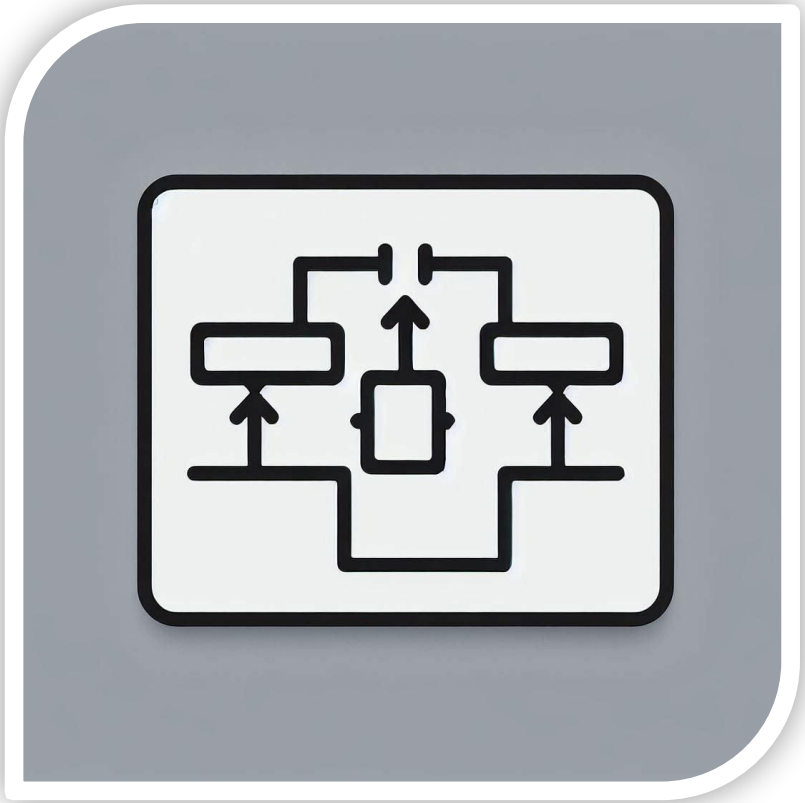


The Uncanny Valley

FOMO

Leveraging a Framework

- Algorithm



- Heuristic

Leveraging a Framework

NIST AI RMF

NIST CSF	NIST AI RMF
• Identify • Protect • Detect • Respond • Recover • Govern	• Govern • Map • Measure • Manage

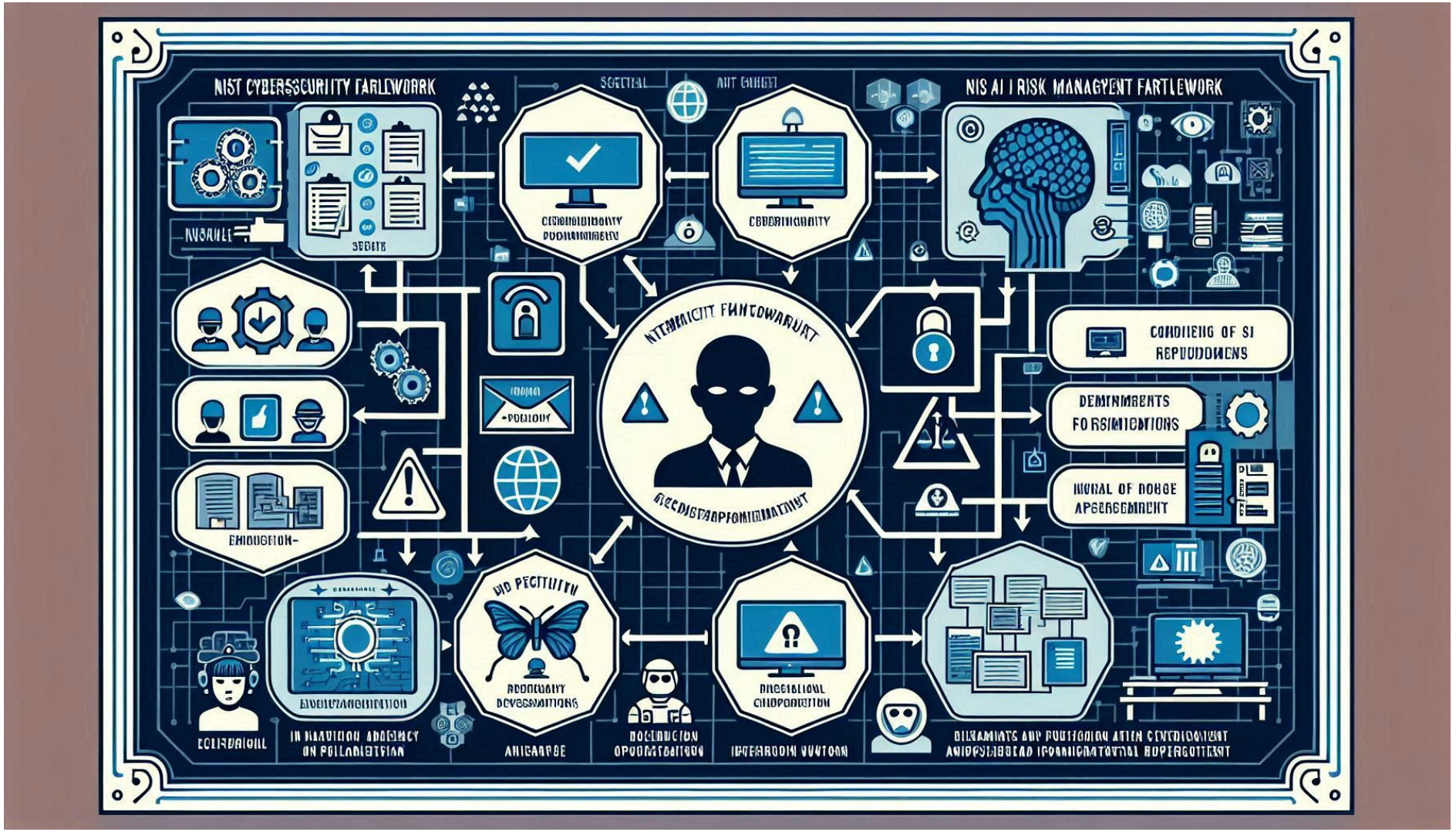
Function	Category	Subcategory	Relevant Control Mappings[2]
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(d)
		ID.AM-2: Software platforms and applications within the organization are inventoried	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E)
		ID.AM-3: Organizational communication and data flows are mapped	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 • HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(3)(ii)(A), 164.308(a)(8), 164.310(d)

Regulating AI

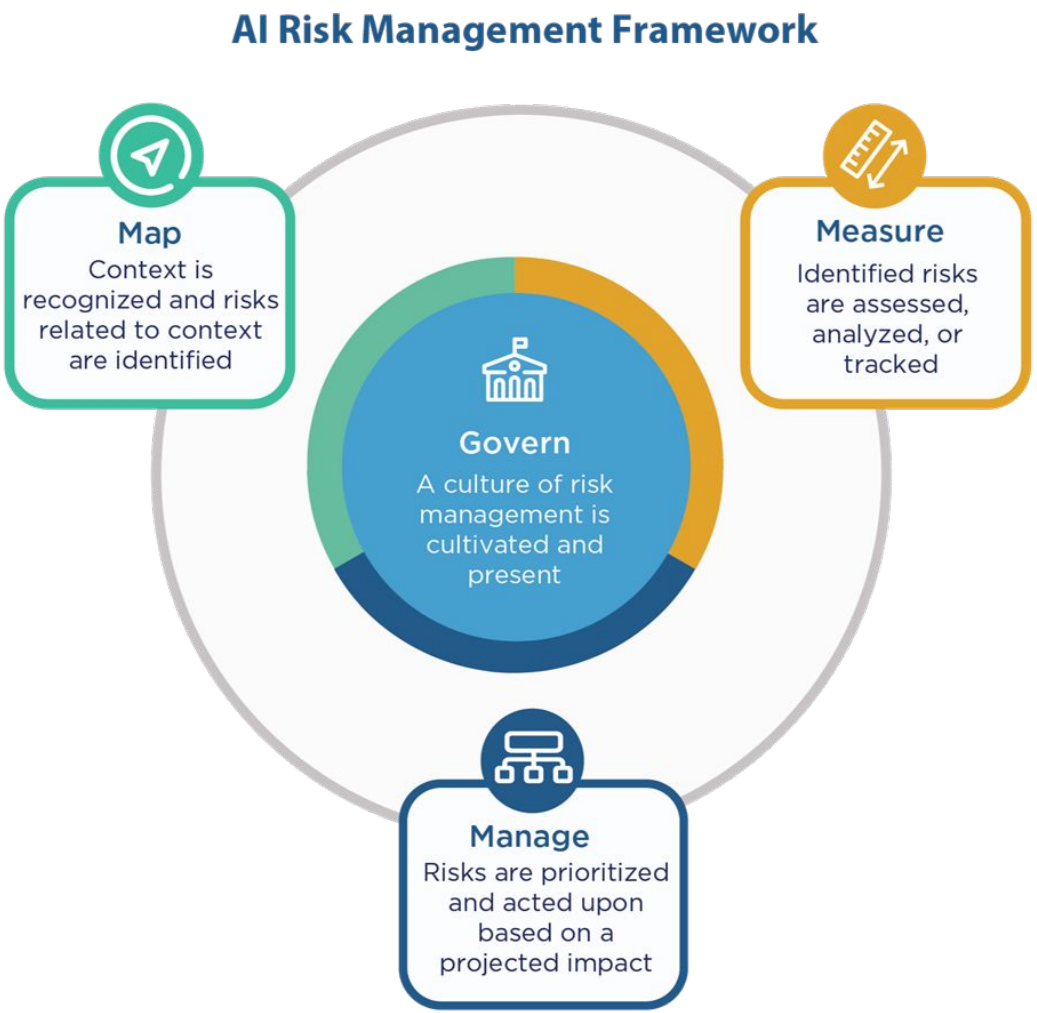
"[H]ere is the graphic art that I created for you. It shows the crosswalk between the NIST CSF Core and the NIST AI RMF core. You can see how the functions, categories, and subcategories of the two frameworks are related. I hope you find it useful. ☺"

NIST AI RMF

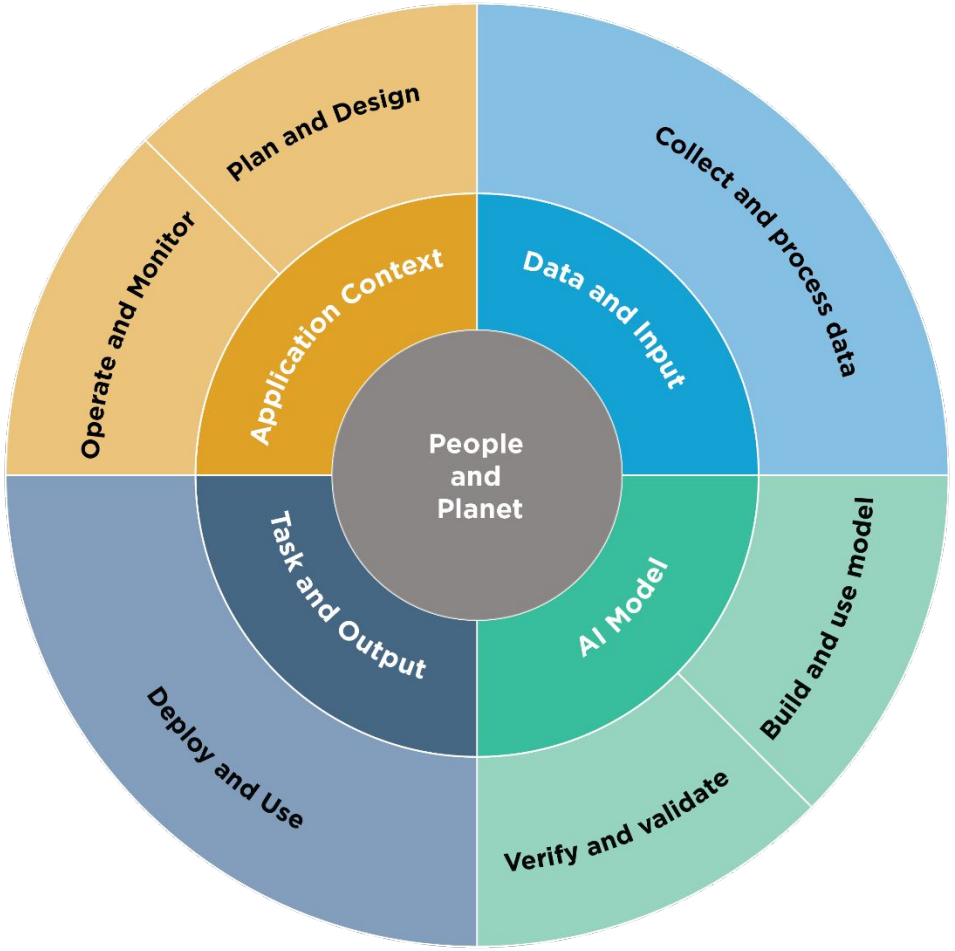
“A diagram showing a crosswalk between the requirements of the NIST Cybersecurity Framework and the NIST AI Risk Management Framework”



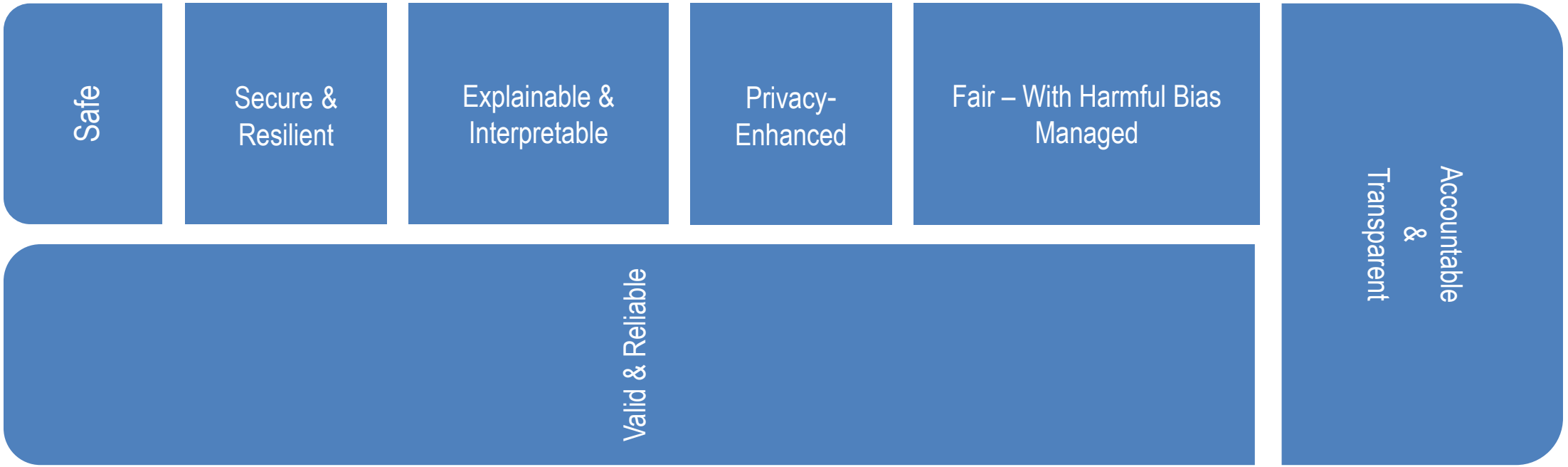
NIST AI RMF



NIST AI RMF



NIST AI RMF



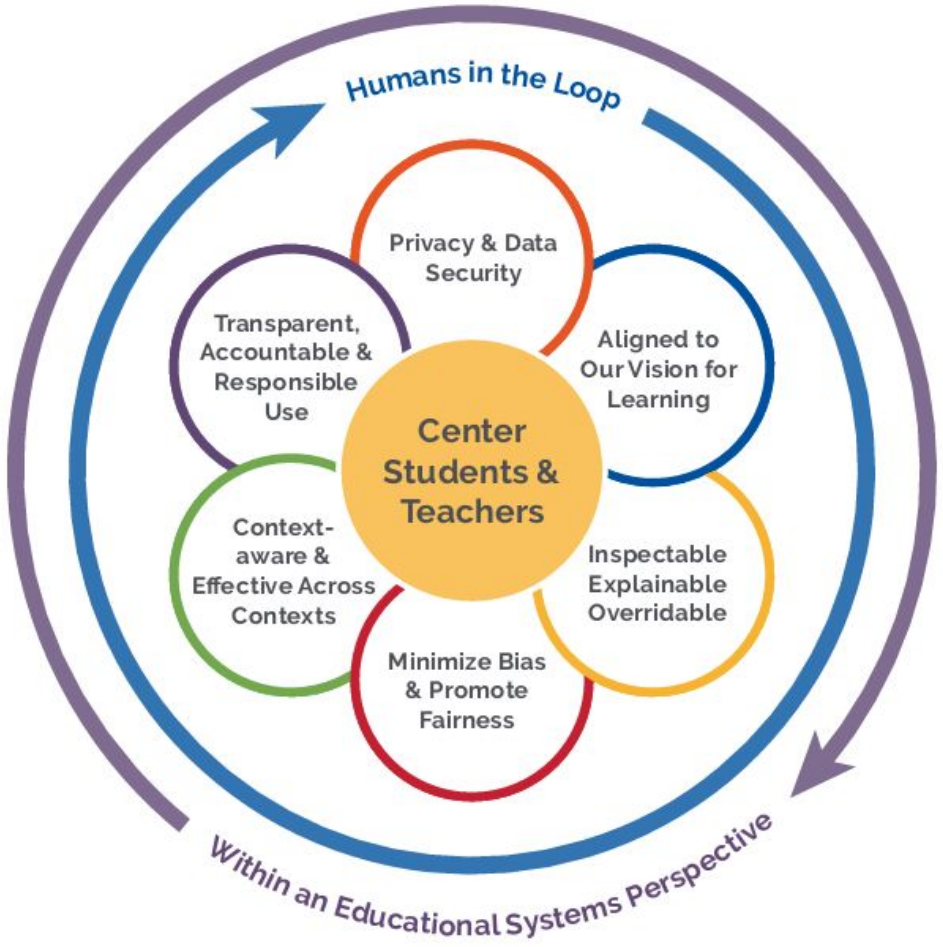
Do It Once: NIST AI RMF to NIST CSF

- Map
  - Identify
- Measure
  - Detect
- Manage
  - Protect, Respond, Recover
- Govern
  - Govern

Do It Once: NIST AI RMF to NIST CSF

- Data Classification; Record of Processing Activities
- Risk Assessment/Data Protection Impact Assessments
- Policy/Procedure Development
- Vulnerability Assessments/Red Teaming
- Incident Response Planning
- Table Top Exercises
- Third Party/Supply Chain Risk Management

Other Frameworks



Source: https://tech.ed.gov/files/2023/05/ai-report-core-messaging-handout.pdf

The EDSAFE AI SAFE Framework

Safety	• Security, Privacy, Do Not Harm
Accountability	• Defining Stakeholder Responsibilities
Fairness (Fair and Transparent)	• Equity, Ethics, and Mitigating Bias
Efficacy	• Improved Learning Outcomes

Where to Start

- Build a diverse team
- Bring your ethical toolkit with you – find the externalities and manage them
- Map, map, and then map again
- Start small, *e.g.*, GenAI usage
- Realize the limitations of a generalized framework
- Make the framework your own
- Benchmark, and look for guidance
- Ask dumb questions, and watch out for the hype cycle
- Repeat!

How to Right-Size Your NIST AI RMF Efforts

- NIST is a federal agency, and the AI RMF is written from that perspective
  - Assumes critical mass to address AI risk, relevant SMEs, as well as time (and budget) to do the required work
  - 71 subcategories, 19 categories, 5 functions
    - To be executed in a non-sequential fashion
    - Repeated as necessary
    - Based on establishment of KPIs, as well as measurement and analysis of same

How to Right-Size Your NIST AI RMF Efforts

- Adapt, adopt, improve?
  - None of us will have a textbook application of NIST AI RMF
  - The right application is the one that moves the needle for your organization in the right direction:
    - More visibility, more diligence, more accountability *i.e.*, documentation
  - Pick and choose, or start on a high-level first
    - If all you can address are the 19 Categories, you are probably off to a good start

How to Right-Size Your NIST AI RMF Efforts

- Emulate
  - Watch this space: https://www.nist.gov/itl/ai-risk-management-framework
  - Most recent update, Gen AI RMF Profile: https://airc.nist.gov/docs/NIST.AI.600-1.GenAI-Profile.ipd.pdf
  - Implement a maturity model: https://ieeeusa.org/product/a-flexible-maturity-model-for-ai-governance/
  - Watch others in your industry
  - Ask vendors for their RMF compliance documentation

Cautionary Tales

- Don't rely on the AI platform to tell you if it's reliable
  - *Mata v. Avianca, Inc.*
- Don't use AI alone to draft your policies
  - In re bitFlyer
- Don't assume that bias is not an issue
  - *Big Data, A Tool for Inclusion or Exclusion*

Resources

- https://www.nist.gov/video/introduction-nist-ai-risk-management-framework-ai-rmf-10-explainer-video
- https://airc.nist.gov/docs/playbook.xlsx
- https://doi.org/10.6028/NIST.AI.100-1

Resources

- https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf
- https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/
- https://ai-challenges.nist.gov/aria
- https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf

THANK YOU!

www.linkedin.com/in/fgreene