CSET CENTER for SECURITY and EMERGING TECHNOLOGY

Key Takeaways from "Harmonizing AI Guidance: Distilling Voluntary Standards and Best Practices into a Unified Framework"

In this report, we present a harmonized framework for how an organization should govern, manage, and protect its technology—and how to integrate emerging technologies like artificial intelligence (AI) into its existing practices. Using a harmonization process developed by researchers at CSET, this work distills the collective knowledge of over 7,000 recommended practices collected from 52 different reports into a condensed set of 258 recommendations. As such, this framework covers a far more comprehensive set of topics—including governance, safety, cybersecurity, privacy, and detection and response practices—than any single existing report, a scope that organizations would otherwise need seven or more different frameworks to approximate. In addition, we use the results of the harmonization process to provide an "AI score" alongside each harmonized recommendation to help illustrate how and where new AI guidance overlays with existing organizational practices.

For Practitioners:

This framework outlines a comprehensive approach that your organization can take to manage its technological assets and integrate AI systems. Use this report as a resource to:

- Understand how best practices from a wide variety of disciplines fit together.
- Identify recommendations pertinent to specific topics of interest.
- Prioritize practices that were most salient across existing guidance documents.
- Assess the applicability of recommendations to the adoption of AI systems.

For Policymakers:

This report provides insight into the breadth of practices—and required expertise—that organizations are being asked, at least voluntarily, to implement. Use this framework to:

- Understand the approach organizations use to develop and deploy AI systems.
- Identify practices that are most important to the public interest.
- Assess how ecosystem-wide infrastructure and policies can connect to and support these internal efforts.
- Evaluate the potential impact of regulation on an organization's operations.

To facilitate the identification and prioritization of relevant guidance, this framework is organized into 34 topic areas, grouped into 5 overarching categories as outlined below:

Governance: Defining and implementing the overarching organizational strategy for managing technology and its associated risks.	
Topics:	*Strategy & Leadership*, *Management*, *Risk Management*, *IT Management*, *Supply Chain*, *Workforce & Training*, *Inventory*, *Audit & Compliance*

Safety: Responsibly developing and evaluating the organization's technology, assessing the impact it has on society, and engaging with stakeholders to foster trust.	
Topics:	*Responsible Business Conduct*, *Stakeholders*, *Societal Impact*, *Impact & Trust*, *Fairness & Synthetic Content*, *Test & Evaluation*, *Performance Monitoring*, *Traceability*, *Transparency & Oversight*, *Model Safeguards*

Security: Developing and deploying secure systems, managing access to facilities and assets, and implementing security controls.	
Topics:	*Security Management*, *Design & Development*, *Vulnerabilities*, *Identity & Authentication*, *Access Control*, *Network Security*, *Information Security*, *Endpoint Security*, *Personnel & Media Security*, *Physical Security*

Privacy: Managing data, particularly personally identifiable information (PII), and protecting the privacy and confidentiality of data throughout its life cycle.	
Topics:	*Privacy Program*, *Handling PII*

Detection & Response: Identifying threats and incidents, responding when these events occur, and building greater operational continuity.	
Topics:	*Audit Logging*, *Monitoring*, *Incident Response*, *Resilience & Recovery*

For more information:

- Download the report: https://cset.georgetown.edu/publication/harmonizing-ai-guidance-distilling-voluntary-standards-and-best-practices-into-a-unified-framework/
- Contact Us: cset@georgetown.edu