Standardization & AI

Archived Working Draft

Authors:

- Login to your Google account to access full editing permission.
- Change from Editing to Suggesting in the upper right of the Google doc for tracking each author's edits.

Please contact research-support@cloudsecurityalliance.org to request full access to author this document.

Reviewers/Visitors:

- If you have a Google Account, please login before commenting. Otherwise, please note your name and affiliation in the comment you leave.
- Use the Comments or Suggesting features on Google docs to leave your feedback on the document. Suggestions will be written in and identified by your Google Account. To use the comments feature, highlight the phrase you would like to comment on, right click and select "Comment" (or Ctrl+Alt+M). Or, highlight the phrase, select "Insert" from the top menu, and select "Comment." All suggestions and comments will be reviewed by the editing committee.

For more information about Google's Comments feature, please refer to http://support.google.com/docs/bin/answer.py?hl=en&answer=1216772&ctx=cb&src=cb&cbid=-rx63b0fx4x0v&cbrank=1

The permanent and official location for the [Insert WG Name] Working Group is https://cloudsecurityalliance.org/research/working-groups/working-group-name

Acknowledgments

Lead Authors

Add Names

Contributors

Add Names

Reviewers

Add Names

CSA Global Staff

Add Names

Table of Contents

STANDARDIZATION & AI

Collaboration in suggestion mode (How to enable: Suggest edits in Google Docs) to facilitate discussion. Add your input into the text, so it becomes one text where we can use the different colors from suggestion mode to trace origin.

Collecting literature around this topic from any field. -> Bibliography section. Please refer by number [1]...[n] to the Bibliography section.

Abstract

Standardization serves as a foundational backbone that enables uniqueness and diversity to flourish within structured environments, akin to the balance of structure and creativity found in language and architecture.

This paper explores the intricate relationship between standardization and uniqueness, emphasizing the necessity of established frameworks in both linguistic and architectural (ETC…) domains to prevent chaos while fostering individual expression. The concept of standardization maturity is examined through three distinct levels: Basic Consistency, where essential rules mitigate chaos; Contextual Adaptation, which allows flexibility within established norms to accommodate diverse needs; and Structural Rigor with Flexibility for Uniqueness, where mature systems enable creative solutions while preserving coherence.

By assessing the maturity of standards based on consistency, recognizability, and adaptability, it can be better understood how to cultivate environments that encourage innovation without sacrificing order. This exploration underscores the vital role of standardization in navigating the delicate balance between uniformity and individuality, ultimately enriching innovation.

Audience

tbd

Why Standardization is Needed for Uniqueness & Diversity

Standardization and uniqueness make such an intriguing pair—like the structure and flair in a great piece of music or architecture: building codes and regulations ensure structures are safe and functional. Yet within those rules, architects can create wildly unique buildings, each with its own personality and purpose, whether it's a sleek skyscraper or a cozy, historic home. Further, standardized language rules, like grammar, provide a framework for clear communication. But then, each person's unique choice of words, tone, and storytelling style add a distinct flavor that makes their speech or writing truly "theirs." Standardization is what keeps us from descending into utter linguistic chaos, while uniqueness and diversity is what makes conversations interesting and memorable.

Standardization is like the hidden backbone that makes space for uniqueness to shine without devolving into sheer confusion. Though it appears to be counterintuitive to uniqueness and diversity, it actually plays a crucial role by providing:

- A framework for comparison that allows meaningful comparison across diverse entities.
- Inclusivity and Accessibility by establishing common standards ensuring diverse groups have equal access to resources and opportunities.
- A certain level of security,

1. *AI driven still and motion image detection used by security and law enforcement services.*This consistent internal structure, allows for safe building blocks to creatively add to, whilst fitting within the defines of the standard

and materials and innovation

Bibliography / Literature

1. https://noahpgordon.github.io/composely-articles/AIGovernanceMaturityModels101.pdf
2. https://innovalor.nl/dam/jcr:9e941add-a590-4525-a9bd-ec482708f48f/AI%20ethics%20maturity%20model%20-%20Krijger%20et%20al..pdf
3. https://www.microsoft.com/en-us/research/uploads/prod/2023/05/RAI_Maturity_Model_Aether_Microsoft_whitepaper.pdf
4. https://www.mitre.org/news-insights/publication/mitre-ai-maturity-model-and-organizational-assessment-tool-guide
5. Cybersecurity Capability Maturity Model (C2M2) | Department of Energy
6. FedER: Federated Learning through Experience Replay and privacy-preserving data synthesis - ScienceDirect
7. Discover Your AI-Maturity Index

8. https://www.gov.uk/cma-cases/ai-foundation-models-initial-review

9. https://iapp.org/media/pdf/resource_center/global_ai_legislation_tracker.pdf

AICert v1.0 - Open-Source AI Traceability Tool for Verifiable Training
10. https://www.researchgate.net/publication/341616218_Is_Artificial_Intelligence_Ready_for_Standardization
11. https://www.forbes.com/advisor/business/software/ai-in-business/

Appendix

Side-Topics removed from the original document

A standard training data format

The rapid evolution of artificial intelligence (AI) has brought about opportunities as well as challenges. One pressing issue is the lack of standardization in AI training data. This hinders collaboration, reproducibility, and ethical development. This paper proposes a standardized data format, called .ai-data, designed to address the fragmentation and inconsistencies that currently plague the AI landscape. Thise .ai-data format aims to establish a universal framework for managing and sharing AI training data, promoting consistency, transparency, and security across platforms and industries.

This paper examines the critical need for standardization, highlighting challenges posed by diverse and often incompatible data formats. It will outline key components of ta common format for AI-related datahe .ai-data format, which encompasses:

- Data content - structured and unstructured
- Metadata Tags - ensuring transparency and traceability
- File format - leveraging existing formats (HDF5, JSON,etc), with AI specific extensions for compatibility and efficiency.

The paper will discuss benefits of this new formatthe .ai-format and explore practical implications for specific sectors, including law enforcement, critical infrastructure, and cybersecurity. Additionally, It will discuss real world use cases, and challenges of implementing a ncommon .ai-data format.

A common.ai-data format can provide:

- Consistency and Reusability - data sharing and collaboration
- Transparency and Trust - clear documentation of data origins
- Privacy and Compliance - adherence to privacy regulations using metadata
- Methods to minimize or overcome inconsistent labeling, misclassification, bias and subjectivity, and data integration issues.
- Measures for cross-validation and reliability checks.
- Scalability to label large data sets

Connecting Maturity Levels of Standardization to AI Data

At the first level of maturity, the focus for a common format for AI data would be establishing basic consistency in data structure and essential metadata tags. This would involve defining fundamental elements like:

- Data content - Clear guidelines for handling of structured and unstructured data.
- Mandatory Metadata Tags: Essential tags for data source, type, preprocessing, privacy, and compliance.
    - File Format: Choosing a base format and creating extensions for AI-specific needs.Removing noisy data outliers and duplicates
    - Creating data labels and categories of datasets

This initial level would ensure AI Data is recognizable and shares a common structure, promoting basic interoperability and understanding across different AI platforms. It would also allow for testing and refinement of the format under real-world conditions.

The second maturity level would involve adapting an AI Data format to accommodate specific needs of different AI domains and tasks that might include:

- Specialized Metadata tags: Specific to data type, like image annotations or threat intelligence sources.
- Domain Specific Extensions: Extending the format to handle unique data structures or requirements in fields like law enforcement, healthcare, or finance.

Contextual adaptation ensures that the AI Data format remains relevant and useful across a diverse range of applications while still adhering to the core principles of standardization.

The third level represents a mature and robust AI Data standard that provides both structural rigor and the flexibility to support innovation and unique solutions. This would involve:

- Robust Governance: Establishing clear governance processes for evolving the standard and incorporating community feedback.
- Extensibility Mechanisms: Providing well-defined mechanisms for extending the format without breaking backward compatibility.
- Advanced Features: Integrating support for cutting edge AI technologies and practices, such as federated learning or differential privacy.

This final level would enable the AI community to develop and share diverse AI solutions while ensuring consistency, interoperability, and trust in the underlying data.

Challenges in Reaching Higher Maturity Levels

Reaching the higher levels of maturity for an AI Data format presents various challenges, these challenges involve gaining industry wide support, creating a format that can handle diverse data types, and striking a **balance** between enforcing standardization and **encouraging** innovation in AI development.

Brainstorming

James Morgan-Jones

As part of my role I have to assess what products and services are acceptable in our environment. As we are a police force, we clearly hold sensitive data so my thoughts below for the paper come from that side of things.

Why we need standardisation:

- Time efficiencies - Without a level of standardisation in the industry it is time consuming for organizations cyber security advisors to review/evaluate different offerings to ensure that they meet the requirements of their organisation, be it legal, regulatory or industry standards. This leads to slower adoption and inefficient practices.
- Compatibility - Another thing we have to evaluate in my practice is ensuring that whatever AI products we utilise are compatible with our existing systems. Standardisation could help this. Things like MS CoPilot are clearly going to be popular in many Windows based organizations due to it's deep integration and compatibility with Windows products. In a world of standardised AI, those evaluating products would have a good idea how a product would act in it's environment and have a level of confidence in its interoperability with other main stream systems
- Compliance - Many industries and public sector organizations have compliance standards that they must meet. The standardisation of AI would help create a level of confidence that a product or service meets these standards. Many organizations must be able to prove they meet things such as ISO standards or follow NIST standards, their adoption of AI is no exception to this, so it is important for AI developer to ensure their products and services follow wider industry best practices in the same way that other technical products are required to, to be considered for wider adoption.
- Sensitivity - Most organizations hold data at differing levels of sensitivity. It is important to know which systems are assured to store and process data at which sensitivity level. An example may be information considered "Official" (UK classification system) can be stored in the cloud in approved vendor data centres. Data labelled as Secret must remain on the secure organisational network on-prem. Data labelled Top Secret must be physically segregated in an air-gapped network with no external network connectivity. With AI standardisation it would be possible to assure different AI products for different information - though it's highly unlikely many agencies are going to consider Top Secret information being put into public cloud LLMs!
- Ethics - My Masters Dissertation was on the privacy considerations of Autonomous Vehicles. As part of this formed an ethics discussion. At the moment there is still a sense of distrust from the wider public around AI in all of its forms. Standards for the ethical production and use of AI are imperative for the industry to grow.

Some notes I made that I feel are relevant to help with further reasons for standardisation - hopefully it's fairly clear how it fits into the conversation:

According to the National Audit Office, AI is not widely used in the UK Government with approximately a third of respondents using one or two use cases. 70% of respondents, however, were planning or piloting the use of AI (NAO, 2024). As many government departments work towards adoption of AI, a level of standardisation would help with the adoption as it would make it easier and more efficient to evaluate AI products and systems.

Further to that a risk based approach to AI, with AI systems fitting into different standardised categories, would also assist organizations in their adoption of AI. Each organisation will have it's own risk acceptance levels or policy, however, standardisation would help them fit AI into the correct risk level to help decide whether the system is a fit for their risk appetite.

The EU AI Act, signed in June 2024 (Madiega, 2024) acknowledges the benefits of AI, whilst recognising that a risk based framework is needed.The new act, would apply to all AI systems on the market or used within the EU, so it's application spans far wider to organizations within the EU, but also to anyone wishing to sell AI products within it, or even use them in the EU. The EU AI Act (Madiega, 2024) looks to categorise based upon risk, outright banning the most harmful applications of AI, regulating high risk uses and ensuring that transparency controls were applied to AI use that is deemed medium-low risk. If we consider the impact of GDPR on organizations world-wide, I think it helps to show how impacting this act could potentially be.

Dimitri Vekris

On the incredibly broad topic of AI Standardization, I would like to provide some suggestions in order to "narrow down" and "further define" **The Importance of Standardization for Further AI Developments.** I believe that any paper we (via CSA) author should have some real-world, objective value to the (corporate or governmental) reader, either in terms of solving a problem, or providing best-practices guidance.

1. Interoperability and Collaboration

AI systems are deployed across a variety of platforms, industries, and regions. For these systems to communicate, share data, and collaborate effectively, standard protocols must be established. Interoperability standards enable AI models, tools, and systems to integrate seamlessly with each other, regardless of the platform or developer. This is essential for large-scale applications such as autonomous vehicles, healthcare diagnostics, and smart cities, where multiple AI systems need to work in unison. *<generated by ChatGPT in order to accurately define areas and aspects of AI standardization>*

2. Ethical Considerations and Trust
3. Safety and Reliability
4. Fair Competition and Innovation

5. Global Harmonization

AI is a global phenomenon, with research, development, and implementation happening across the world. However, each country or region might have different regulations, priorities, and ethical concerns related to AI. Without global standards, this can lead to fragmentation, with conflicting regulations that hinder the growth of the AI industry. International standardization bodies like the International Organization for Standardization (ISO) and the Institute of Electrical and Electronics Engineers (IEEE) play a crucial role in creating globally accepted AI standards. These standards ensure that AI systems can operate consistently across borders, promoting smoother international collaborations, trade, and regulation alignment. *<generated by ChatGPT in order to accurately define areas and aspects of AI standardization>*

6. Data Management and Privacy

7. Quality Control and Benchmarking

As AI systems are integrated into more industries, there is a growing need for performance benchmarking and quality control. Standards can provide clear criteria for evaluating the accuracy, efficiency, and robustness of AI models. This is particularly important for sectors like finance, healthcare, and law enforcement, where errors can have severe consequences. Benchmarking AI performance against standardized tests helps ensure that systems meet certain thresholds of reliability before being deployed. This is also crucial for regulators, who need consistent metrics to evaluate the effectiveness and safety of AI solutions in various industries. *<generated by ChatGPT in order to accurately define areas and aspects of AI standardization>*

Reworked Outline Draft

- **Why Standardization is Necessary**
  - **The risk of Noncompliance and Immature AI**
- AI Standardization Maturity Model – Not just a RMF
  - **Maturity Levels of Standardization (1-3 bad > great)**
  - **How would you rate or test maturity?**
- Comparing your RMFs – Pros and Cons
  - **We have a very basic table, but could do MUCH more here**
- Implementation Challenges & Recommendations
  - **Applied standards audit**
- Conclusion
  - **Adherence to standards: an AI maturity discipline**
- Annex: Maturity Questionnaire

Remove: AI Use case section, unless we are going to get far more specific on standardization for each use case
Remove: Risk and threat examples for immature AI agents and immature users – this has been covered in several other CSA papers