Creating Trust in AI Through Standards: A Management System Approach

Kimberly Lucy
Director, GRC Standards
Microsoft
Introduction

Artificial intelligence has the power to affect virtually every aspect of human life, from work to healthcare to leisure. At the same time, the damage that can be created by such powerful systems is immense if left unchecked. **How can AI be developed and used in a way that is responsible and that leads to trust and assurance for consumers and other stakeholders? And what is the role of standards in creating this trust and assurance?**
Two components of this presentation—both critical aspects of management systems standards that create trust in AI

The “traditional” approach

The AI Management System (AIMS, ISO/IEC 42001) as central component of a governance, risk, and compliance ecosystem

The “novel” approach

Conformity assessment/certification of management systems + products/service certification that can lead to a joint certification model for AI
Background: What is a management system standard? What is ISO/IEC 42001 (AIMS)?

- Management System Standard:
  - Based on a common “High-Level Structure” with required management clauses (all MSS have these)
  - Focused/scoped to a particular domain or sector (e.g. information security, privacy, AI)
  - Stresses an iterative process of continuous improvement for an organization
  - Risk-based
  - Organizations can be certified by a third-party to the applicable MSS

Current AIMS Structure

- Management Clauses
  - Context of the organization
  - Leadership
  - Planning
  - Support
  - Operation
  - Performance Evaluation
  - Improvement

- Annex A Controls + Annex B Guidance
  - Policies related to AI
  - AI management framework
  - Resources for AI
  - Assessing impacts of AI systems
  - AI system life cycle
  - Data for AI systems
  - Information for interested parties of AI systems
  - Use of AI systems
  - Third-party Relationships

ISO / IEC AI Workshop | 24 – 25 May 2022
AIMS “fast facts”

• Scope of standard allows organizations to define what “responsible AI” means for them, depending on the context of their organization—want organizations to think about responsible AI, with the flexibility to address this within their own operational environment

• System level controls (Annexes A and B) align well with requirements in draft EU AI Act

• Controls are written at an abstract level to allow organizations the flexibility to add more granular detail depending on their context (particularly regulatory context); they are not meant to cover regulatory requirements 1:1

• Written with a strategic approach to other SC42 standards, particularly governance, risk, and compliance (next slide), which complement AIMS and can be used by organizations to help implement a GRC ecosystem of standards to enable trust and assurance
The governance, risk, and compliance (GRC) ecosystem approach

Hypothetical AI MSS Ecosystem use in an organization

ISO / IEC AI Workshop | 24 and 25 May 2022
How can AIMS/management systems certification lead to customer/public trust?

- Management systems certifications, particularly those for IT products or “digital services” have a history of being the primary international certification mechanism (e.g. ISO/IEC 27001)

- Customers have come to recognize and rely on management system certification for assurance and trust that organizations are doing the right thing, and that products/services can be trusted

- Supply chains heavily rely on management system certifications as methods of mutual trust and assurance
Will management system certification alone be enough, particularly for higher risk AI systems?

- Potentially not—but it will be a key component!

- AI will likely be highly regulated in many cases (e.g., EU AI Act)

- “Productization” of intangible/digital services like AI—expectations by regulatory authorities and others for certification “equal” to that of tangible manufactured products
  - Accreditation of certification takes place under ISO/IEC 17065 for products/services rather than ISO/IEC 17021 for management systems in this case

- There are several problems to be solved in this space—primarily that digital services/intangible products have not historically been certified under 17065. However, there is a potential solution...
Novel approach to using management system for trust and assurance in a changing regulatory landscape: Joint certification

For more information on the joint certification topic, see the following whitepaper:

A Joint Certification Approach for Digital Services and Regulatory Compliance
Summary

An AI management system will be a key component for providing trust and assurance for users of AI systems. Whether in a more traditional form via an organization’s GRC ecosystem and MSS certification, or as part of the novel approach to joint certification for management system and digital services, AIMS will be the foundation on which trust is created.
Thank you
Kimberly Lucy
kilucy@microsoft.com