A Standards Story: AI

Jason Matusow
General Manager, Corporate Standards Group

Microsoft

Act 1:
Learning The Ropes

Scale

Shared Obligations

Privacy

Act 2:
The Regulatory Tsunami

Horizontal Global Non-Coherent

Act 3:
Separating Signal From Noise

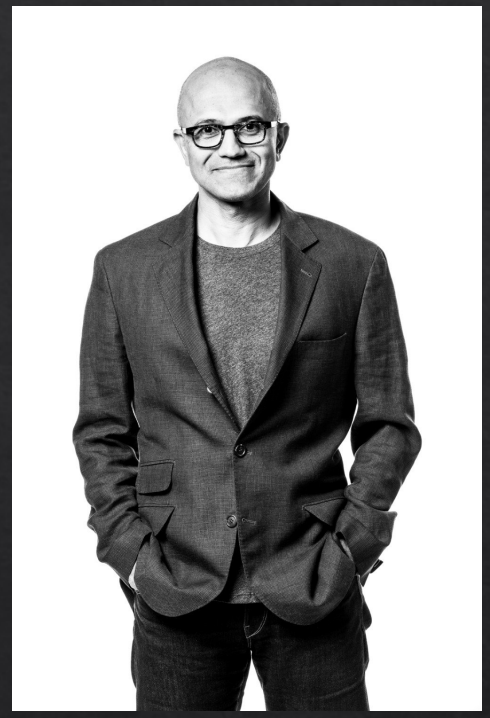
Microsoft

Culture

Strategy

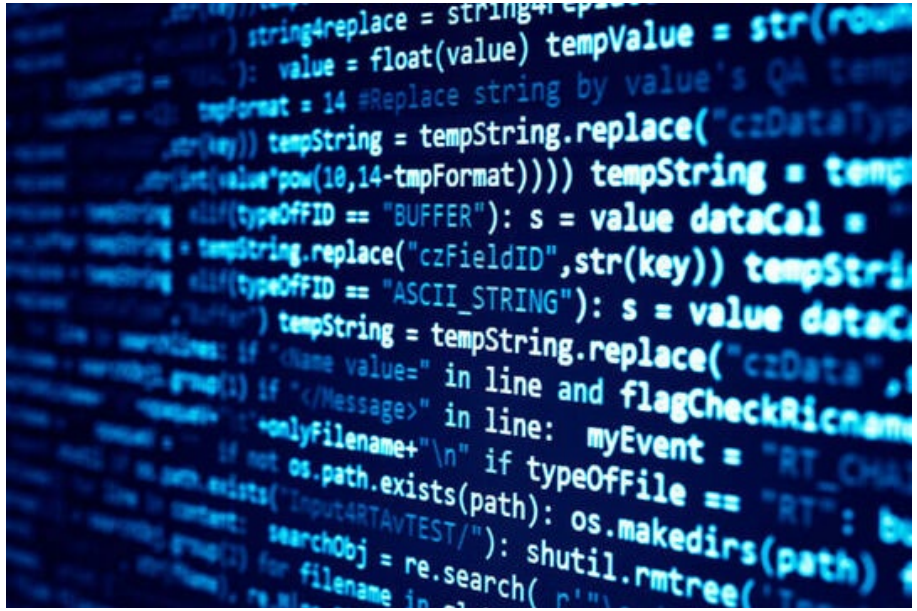
Commitment

Trust



Cloud + Data + Research

Marketplace Competition

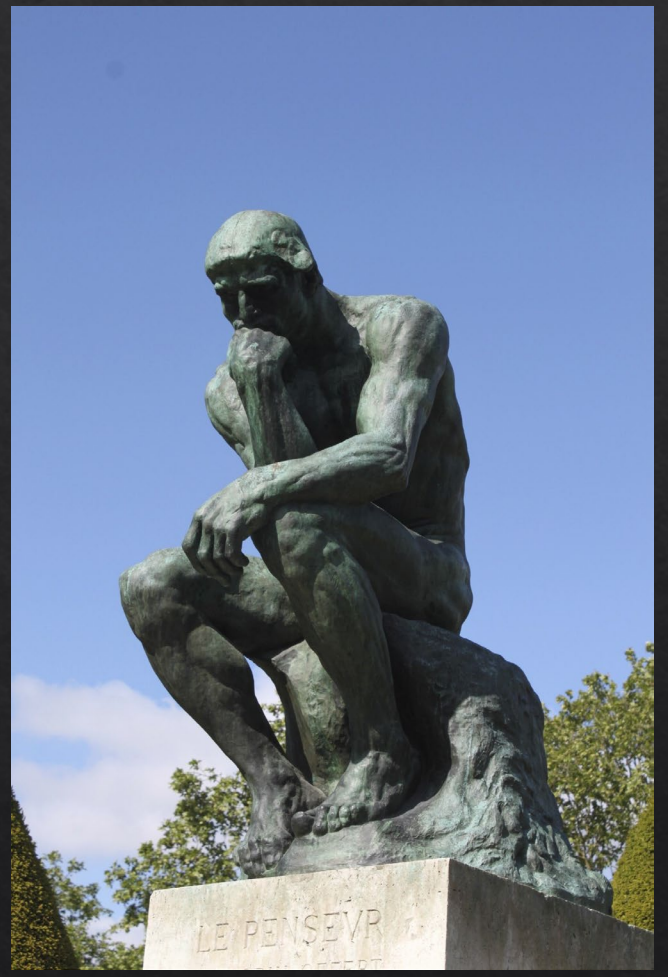

string4replace = string4
value = float(value) tempValue = str(
tmpFormat = 14 #Replace string by value's QA
tempString = tempString.replace("czDataTyp
value*pow(10,14-tmpFormat)))) tempString = temp
typeOfFID == "BUFFER"): s = value dataCal =
tempString.replace("czFieldID",str(key)) tempStri
typeOfFID == "ASCII_STRING"): s = value dataC
tempString = tempString.replace("czData",
if "<Name value=" in line and flagCheckRicname
if "</Message>" in line: myEvent = "RT_CHA
+onlyFilename+"\n" if typeOfFile == "RT": b
if not os.path.exists(path): os.makedirs(path)
exists("Input4RTAvTEST/"): shutil.rmtree(
searchObj = re.search(
for filename in

Act 4:
We Don’t’ Know $#@!
How Cool is That?

Ubiquitous

Regulated

Concepts & Behaviors



Establishment of organization's **principles**
Definition of **risk criteria** and "**appetite**"

Organization's Governance

[Drafted in 2018]

Identification of concerns to **stakeholders** →

Organization | Customers / Partners/ 3rd Parties | End Users | Society

→ as related to their **assets** or **values**

Viability | Reputation/ Trust | Safety | Privacy/ Confidentiality | Fairness | Transparency

Risk assessment of **control objectives** (i.e., **threats** and **vulnerabilities**)

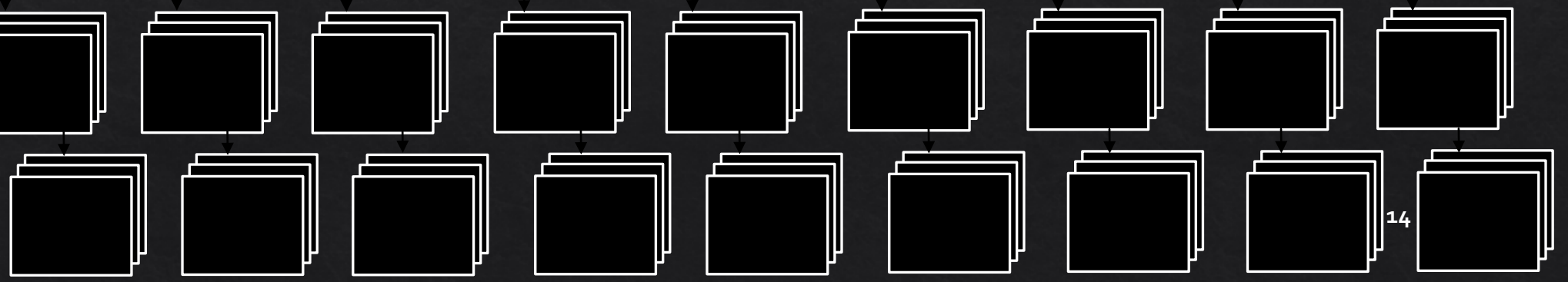
Creation of power of **data** | Complications to **accountability** | New **security** threats | New **privacy** threats (e.g., hidden patterns) | **Improper specification** | **Deficient implementation** | **Incorrect use** | Different sources of **biases**

Risk treatment through **controls**

Non-technical measures | AI system **repeatability** | Approaches to **transparency** | New **security** controls | New **privacy** controls | **Resilience/ Robustness** controls | Choices and configuration of **ML algorithms** | Considerations related to **data** | AI system **controllability**

Implementation **guidelines**

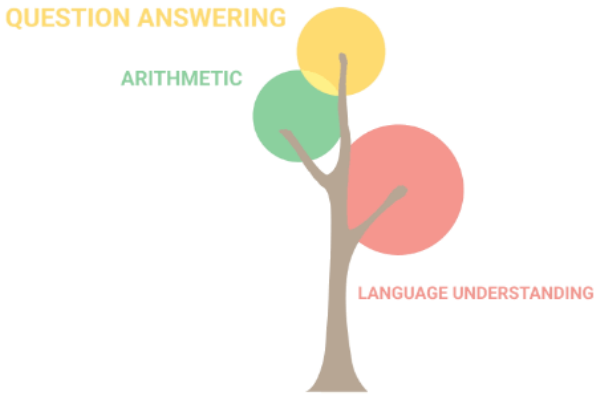
Evaluation of **characteristics** using qualitive or quotative **metrics**



Specific AI

General AI

Generative Transformers



8 billion parameters

Tools

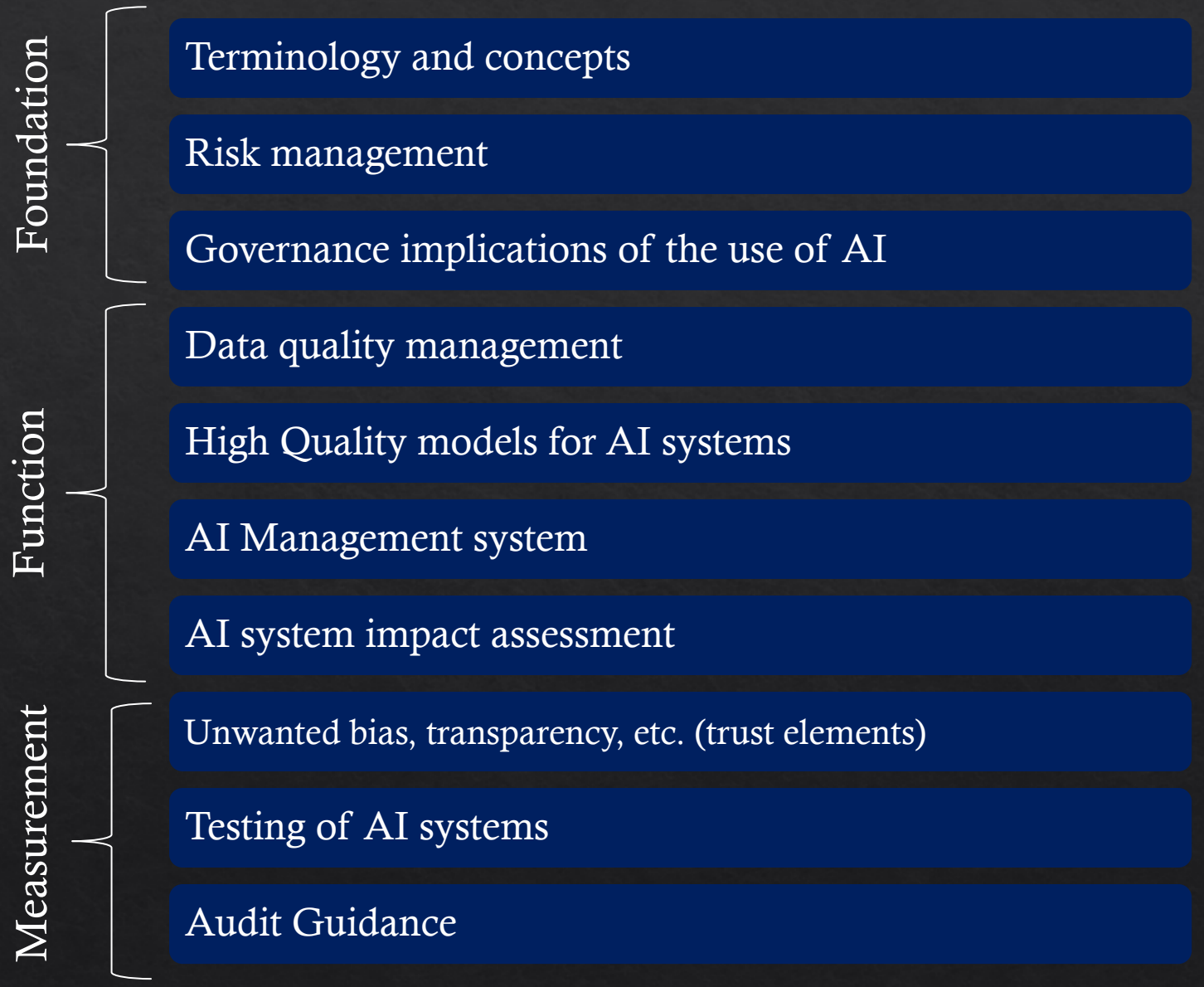
Weapons

Engineering & Ethics

Act 5:
Timing is Everything

JTC 1 Standards for Responsible AI

- Differentiated components
- A system of related standards
- Not standardized regulation
- Dependence on strong accreditation and certification practices



Act 6:
What's Next?

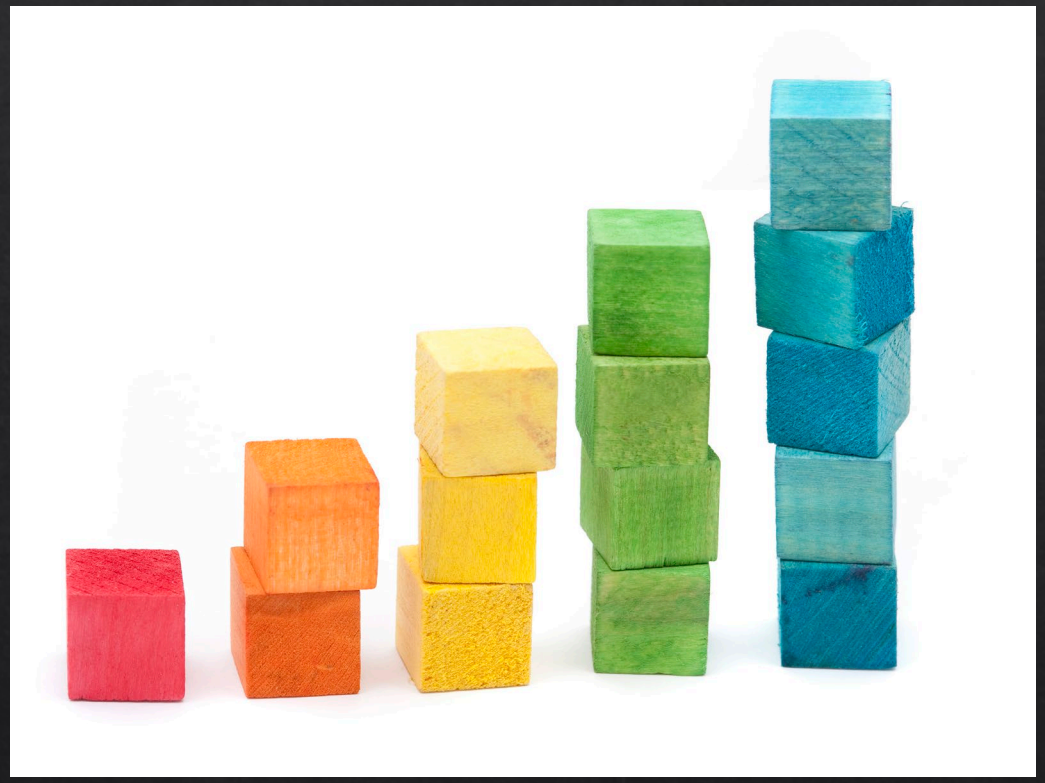
Solutions Integration

Regulatory Roadmap

Frontier Models

Responsible AI Standards: Meet the Scale of an Economy

- Define Behaviors for Good Actors
- Enable Efficient Contracting
- Promote Supply Chain Trust
- Preserve Competent Authority Resources
- Facilitate Cross-Border Commerce



Get AIMS Right

Address Digital Services Conformity

Establish Technology & Vertical Controls