From Data Governance to AI Governance
The New Role of the CIO (CDO, CTO, CAIO, etc.)

@jfgagne
jfgagne.ai
We deliver **cutting-edge AI software** products at scale that make businesses safer, stronger and more **agile**.

A modular approach to product development enables us to deliver **industry-specific software at scale**.

Unlike traditional rule-based software, AI software is **pattern-based and self-learning** to continuously deliver strategic insights.

Our team of **in-house researchers and university fellows** brings the latest AI techniques to our products.

Our products are catered to **key industries** and deliver value to the **Global 2000**.
What do the Chief Officers all have in Common?
Driving the Digital Side of the Cyber-Physical Revolution
Does your organization have a data governance framework in place?

- Yes: 39%
- No: 22%
- Just starting to design & implement one: 24%
- In the middle of implementing one: 15%

How long has your organization been implementing data governance?

- 0 – 6 months: 38%
- 6 months – 1 year: 15%
- 1 – 2 years: 27%
- 3 – 4 years: 6%
- Over 5 years: 13%

Source: [https://ciowatercooler.co.uk/the-data-governance-report-2017-your-copy/](https://ciowatercooler.co.uk/the-data-governance-report-2017-your-copy/)
#1 Concern for Data Governance Boards

- **Efficiencies in processes**: 54%
- **Regulatory requirements**: 39%
- **Customer service**: 7%

Source: [https://ciowatercooler.co.uk/the-data-governance-report-2017-your-copy/](https://ciowatercooler.co.uk/the-data-governance-report-2017-your-copy/)
The Myth of the Big Data Era

A Clean Path towards AI
3 trillion images of cats will not inform me about the shape of a dog.
3 Myths about data

- There’s value in big data because it’s more than we can comprehend
- All data is created equal
- We will be able to boil the ocean of data to get AI
The opportunity
A whole new world of opportunities

Reasoning
Understanding concepts & relations

Communication
Processing and generating media that convey meaning

Decision making
Optimizing to specific outcomes

Perception
Sensing the world

Interaction
Taking actions to achieve goals
Real World

Objectives

AI Perception

Representation of Perceptions

SEARCH

AI Decisions

Representation of Decisions

LEARN

FEEDBACK

LEARN

PLAN

Action
Developing Enterprise-grade AI Solutions is a multi-step, iterative process...

- **DESIGN**: Design the model and interface with human users and end business goal in mind
- **AUDIT DATA**: Ensure it can meet the design requirements, and adapt the design if not
- **MODEL**: Search for right model architecture and features, adapting to problem at hand
- **PROTOTYPE**: Train and test different models, create, test and refine the user interface
- **DEPLOY**: Go live, connecting model inputs and outputs to other systems in the business
- **OPERATIONALIZE**: Incorporate solution into everyday processes and workflows with user feedback
- **MAINTAIN & SUPPORT**: Monitor analytical and engineering performance of solution and retrain periodically
A new role in driving value

Less about managing data and more about ensuring that

- Learning feedbacks are well orchestrated
- AI is extracting the right IP (within a gradient of ownership)
- Overall the model is driving the right business objectives / performance
An AI Governance Framework
AI Governance Framework

**PERFORMANCE**
- Accuracy
- Bias
- Completeness

**SECURITY**
- Adaptability
- Adversarial Robustness

**PRIVACY**
- IP Capture
- Impacted Users

**TRANSPARENCY**
- Explainability
- Intent
AI Governance Framework

**Nature of Task / Level of Autonomy**

### Human-Driven

0. **Disconnected**
   - Passive recording without analytics.
   - In-store security camera

1. **Watching**
   - Go Store at Amazon
   - Analytics
   - Categorizing

2. **Coaching**
   - Active tips / suggestions
   - Direction guides

### AI-Driven

3. **Collaborating**
   - Semi-Autonomous
   - Calls in human for certain circumstances
   - Still control via governance

4. **Autonomous**
   - Monitored

---

---
AI Governance Framework

**ACCURACY**
Assess model confidence and ability to classify and make decisions, tracking through entire feedback loop

**BIAS**
Watch for diversity of data sets and inputs; don’t overcompensate given the circumstance of your model

**COMPLETENESS**
A human, qualitative assessment of how representative the model is
## AI Governance Framework

### Nature of Task / Level of Autonomy

<table>
<thead>
<tr>
<th>Nature of Task / Level of Autonomy</th>
<th>Human-Driven</th>
<th>AI-Driven</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Human-Driven</strong></td>
<td>1. Watching</td>
<td>3. Collaborating</td>
</tr>
<tr>
<td>Humans to monitor and sample to see if model is making mistakes.</td>
<td>Measure the accuracy based on the action taken by human.</td>
<td>More diligent monitoring of degrees of confidence based on the action taken by AI.</td>
</tr>
<tr>
<td>Getting unstructured or semi-structured data to be structured.</td>
<td>Monitoring the human’s scoring or outcomes.</td>
<td>If machine is not convinced, it can bring the human in.</td>
</tr>
<tr>
<td><strong>AI-Driven</strong></td>
<td>2. Coaching</td>
<td>4. Autonomous</td>
</tr>
<tr>
<td>Self-assessing and self-adapting for confidence levels.</td>
<td>Have filters and alerts for human monitoring agent.</td>
<td></td>
</tr>
</tbody>
</table>
AI Governance Framework

Volume and diversity of situations the model has seen, whether tested synthetically with adversarial agent or in the data.

Same as above but focused on attacks using an agent not necessarily aligned with the goals of the business.
AI Governance Framework

Have an architecture for IP segmentation, determining user, system, and shareability that you can train your models around.

Traceability of where the information is going and how it’s used, even outside of the organization. Mechanisms for erasing user data and related learnings.
AI Governance Framework

Determine the most *probable* decision path, reducing margin of error with greater autonomy.

Based on Agent definition, ensure it complies with the ethics of the company and society, and make easily available to user.
Some Takeaways
An overview

AI Governance Framework

- Corp Gov’t
- Ethics

CDO

Problem & Solution Definition

Agent Definition

AI Governance
- Value Management
- Risk Management

Prod
Food for Thought

Ethics and Corporate Governance
AI-Augmented Governance
The Learning Organization
Digital Literacy
Show this to the outside world
AI to watch the AI

The problem of scalable governance

Adversarial Governance Agents can:
- Help force explanations of decisions
- Measure biases
- Estimate completeness
Questions?

For news forthcoming book subscribe to:

🌐 jfgagne.ai  🐦 @jfgagne