Attachment C:

AI Buyer Governance Control Taxonomy

Based on procurement type and system usage context

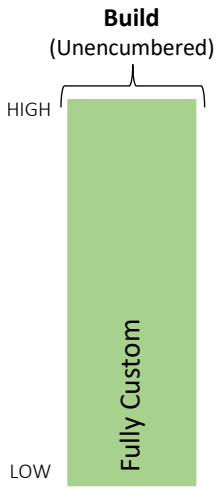
The
Center *for*
Inclusive Change

IT'S COMPLICATED

When a developer creates a product to take to market (e.g., an fitness tracking device), the developer maintains full control over all risk mitigation and governance decisions throughout the entire lifecycle of the product—from ideation to decommissioning. This leaves the buyer of that product with an asymmetrical risk profile for the product. The residual risks that the developer deemed ethically allowable are passed to the buyer—leaving the buyer with no choice but to accept the pre-determined acceptable risks.

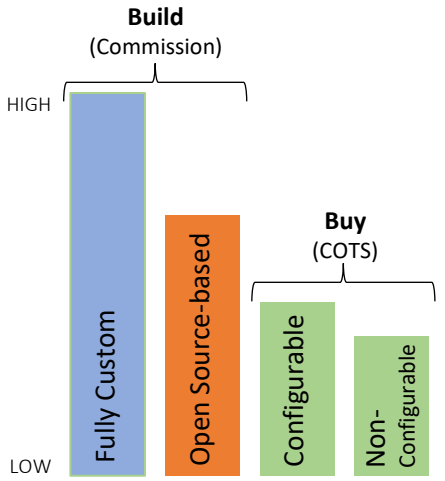
In the two charts below, the risk control profile of the developer of the fully-controlled product is depicted in the chart on the left. Clearly, this type of developer has a high degree of control over risk mitigation efforts. In contrast, the buyer's level of risk control, depicted in the chart on the right, is much lower for that same product. If the product is configurable (e.g., the user can opt-out of allowing the product to track age and weight), the buyer may gain some level of additional risk control. If the product is non-configurable, the buyer will experience a more limited ability to control risk.

Developer's Level of Risk Control



Buyer's Level of Risk Control

(by procurement type)



Unlike the commercial off-the-shelf (COTS) example from above, there are two additional scenarios that allow the buyer more risk control. In these scenarios, the buyer may commission a customized AI/ADS unique to the buyer's needs. In the first scenario, the commissioned build may be fully-customizable from scratch. As an alternative, which is growing in popularity, the commissioned build may include one or more open-source models (e.g., BERT, GPT-3, DALLE, etc), in which case, some of the buyer's risk is controlled by the open-source developer with all residual risks transferred to the buyer. ***The intersection of context adds to this complexity***.

The following pages provide additional descriptions.

AI/ADS Buyer Governance Controls Taxonomy

based on procurement and system usage context

	Level of Control ↑ High ↔ Moderate ↓ Limited			
	BUILD (COMMISSION)		**BUY (COTS)**	
	FULLY CUSTOM	OPEN-SOURCE BASED	CONFIGURABLE	NON-CONFIGURABLE
Buyer's Governance Control	↑ developer diversity ↑ training data ↑ algorithms ↑ UX/UI/configuration ↑ testing/validation ↑ deployment ↑ monitoring ↑ input data ↑ usage ↑ redress ↑ system updates	↓ developer diversity ↔ training data ↔ algorithms ↔ UX/UI/config. ↑ testing/validation ↑ deployment ↔ monitoring ↑ input data ↑ usage ↑ redress ↔ system updates	↓ developer diversity ↓ training data ↓ algorithms ↔ UX/UI/config. ↔ testing/validation ↑ deployment ↔ monitoring ↑ input data ↑ usage ↔ redress ↓ system updates	↓ developer diversity ↓ training data ↓ algorithms ↓ UX/UI/config. ↓ testing/validation ↑ deployment ↔ monitoring ↑ input data ↑ usage ↔ redress ↓ system updates

SYSTEM USAGE CONTEXT (by Impacted Stakeholder)	
Employees	Hiring systems, video interviewing, onboarding, security access, biometric analysis, chat bots, benefits recommender systems, productivity monitoring, surveillance, coaching, assessments, succession planning, learning and development, work assignments, workload balancing, scheduling, employee sentiment, inclusive-writing assistance tools, flight risk assessment, confidentiality breeches, termination, etc.
Customers & Consumers	Government/Social services: housing applications, background checks, child welfare technologies, educational technologies, sentencing recommendations, recidivism recommendations, disability claims processing, unemployment approval / processing, voter registration, insurance marketplace product offering decisions, community policing / surveillance, electronic vehicle inspections, geological/urban planning, etc.
	Healthcare: patient scheduling, benefits approval, medical imaging assistance, medication management, bedside management, diagnosis assistance, equipment QC monitoring, drug development, medical equipment development, facility security, etc.
	Banking / Finance: credit services, background checks, fraud detection, loan approvals, etc.
	Transportation: GPS, autonomous driving, safety & security, predictive maintenance, etc.
	CPG: Internet of things, connected devices, advertising tactics, service chatbots, etc.
Processes	Credit card reconciliation, NLP contract assistance, mechanical performance monitors, cyber threat detection monitoring, economic order quantity management, etc.

The Center for Inclusive Change

WHAT'S A BUYER TO DO?

There are three primary risk mitigation measures available to buyers that can help balance the asymmetry of risks that exist in the seller/buyer relationship: **1)** procurement vetting, **2)** contract terms and conditions, and **3)** internal controls (e.g., policies, procedures, user training, etc.). Each of these three elements will need to be adapted given the context of each AI/ADS that is procured. In other words, the level of risk and potential impact of each system varies. As such, the intensity of procurement, contracting, and internal controls will adapt.

AI/ADS Lifecycle Risk Decision Points	Buyer's Risk Mitigation Measure
Employee diversity	Procurement, EEO-1 report verification
Nature, scope, context, & purpose	Procurement, impact assessment, explainability, transparency Contract Terms & Scope of work, legal jurisdiction & compliance
Training data	Procurement, 3rd party auditor, ethical choice disclosures, privacy Contract Terms & Scope of work
Algorithms	Procurement, 3rd party auditor, explainability, transparency Contract Terms, annual audit review
Configuration/Features	Procurement, 3rd party auditor, system documentation Contract Terms & Scope of work
User Interface/Experience	Procurement, VPAT Contract Terms, annual VPAT submission
Test, Evaluation, Verification, & Validation	Procurement, 3rd party auditor, system documentation Contract Terms & Scope of work
Deployment	Contract Terms, system integration support, administrator & user training (start-up, new users, annual training)
Monitoring	Contract Terms KPI reporting frequency, key risk indicators Buyer-side KPI's, system usage, users, and cyber threats, adverse incidents
Input Data	Buyer's policies, user training (start-up, new users, annual training), system configuration (if available)
Usage	Written policies and procedures for appropriate use, avoiding misuse/disuse/over-use/under-use/abuse/over-trust, trained users, clear roles and responsibilities for system ownership
Redress	Written policies and procedures to report and expeditiously resolve adverse incidents Procurement, Contract Terms, & Scope of work
System updates	Procurement, Contract Terms, Advanced notices, advanced beta versions, transparency, explainability, & disclosures

One essential tool every buyer must maintain is a comprehensive inventory of all AI/ADS within their walls.

The Center for Inclusive Change