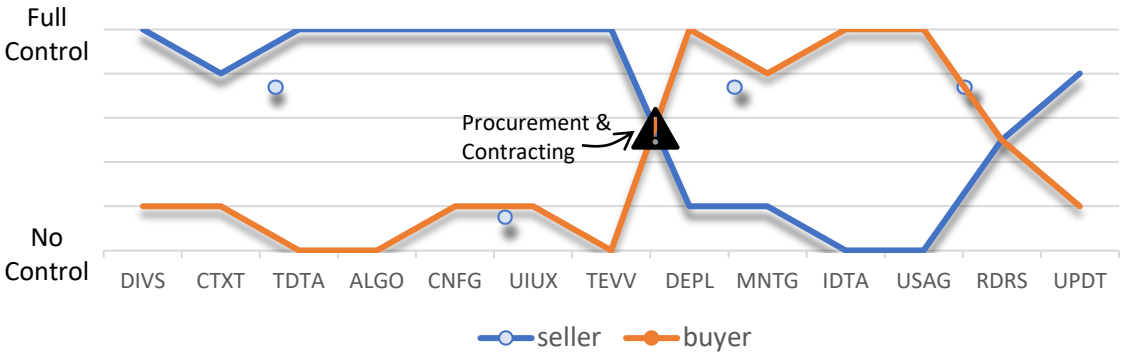
Attachment A:

AI Lifecycle
Transfer of Governance & Risk Control
from Seller to Buyer

The
Center *for*
Inclusive Change

AI Lifecycle
Transfer of Governance & Risk Control
from Seller to Buyer



Early in the AI/ADS lifecycle, the developer maintains most, if not all, of the decision-making authority over the system. Hence, there is an asymmetry of power in governance favoring the sellers' decision morality until the system is released into the wild. At which point, asymmetry of power in governance of the AI/ADS becomes the responsibility of the buyer and the seller loses control over system governance until such time as the seller provides an update, new version, or decommissions the system.

AI LIFECYCLE DECISION POINTS
DIVS – Employee diversity
CTXT – Context & Impact assessment
TDTA – Training data
ALGO – Algorithms
CNFG – Configuration/Features
UIUS – User Interface/Experience
TEVV – Test, Evaluation, Verification, & Validation
DEPL – Deployment
MNTG – Monitoring
IDTA – Input Data
USAG – Usage
RDRS – Redress
UPDT – System update / decommission

As the ability to control risk mitigation efforts shifts from one party to the next, accountability for establishing and upholding appropriate governance practices follows.

The keystone between the two parties is the *procurement and contracting process*.

This process is *NOT* defined on the typical AI/ADS lifecycle and in fact, the word "procurement" is only mentioned one time in the NIST AI RMF preamble. However, it is one of the most critical risk mitigation elements for any buyer of an AI/ADS—especial a buyer of a socio-technical AI/ADS.

Another important risk management element for a buyer of multiple AI/ADS is a comprehensive inventory of AI/ADS systems. This inventory should not simple be a listing of system names, vendors, and business owners, but should be a living risk management tool that includes a risk assessment score for each system, links to version release notes, contract terms, system inspection logs, incident logs and resolutions, etc.

My point is that there are a number of differences in risk management needs between the developer/seller and the buyer/user. Bringing clarity and distinction to these differences may serve our business community well.

Further details can be found in the tables on the following pages.

Provider vs Buyer Governance Control & Accountability
High-level Distinctions

System Element	Developer / Vendor	Buyer / User
PRINCIPLES: AI and data ethics principles, risk appetite, impact assessments, & governing policies during development	Unique to each seller, transferred to buyer	Unique to each buyer, assumed from seller
DIVERSITY: Diversity of seller's direct employees: product designers, engineers, coders, testers, evaluators, validators, etc.	Assumes full control and accountability	May apply social expectations, but lacks control and accountability
CONTEXT: Defining the use case and determining the ethical impact of the system on humans.	Assumes full control and accountability	May provide voice-of-the customer input, but lacks control and accountability
TRAINING DATA: Ethical choices related to training data (in socio-technical systems) provenance, fit for purpose, relevance, robustness, accuracy, completeness, representativeness, appropriateness, privacy protection, sensitive categories, proxy categories, etc.	Assumes full control and accountability May or may not provide full transparency to all ethical choices	No or limited control over ethical decisions May request disclosure during procurement, but limited ability to validate responses. May use 3rd party auditor to attempt validation
ALGORITHMS: Ethical choices related to algorithm selection, training, and testing (in socio-technical systems) to ensure fairness, equity, legal and regulatory compliance without over-fitting or underfitting, over-weighting or over-weighting.	Assumes full control and accountability May or may not provide full transparency to all ethical choices	No or limited control over ethical decisions May request disclosure during procurement, but limited ability to validate responses. May use 3rd party auditor to attempt validation
FEATURES: Configurability considerations and features that incorporate foreseeable user misuse, disuse, and abuse.	With multi-stakeholder feedback, may be able to address to the best of their ability. Should provide full transparency and disclose via a "user handbook" or user training guide.	May provide voice-of-the customer input, but lacks control and accountability Should request discloser and training during procurement and prior to deployment.

System Element	Developer / Vendor	Buyer / User
UI/UX: UI/UX compliance with ADA and conformance with WCAG2+ guidelines.	Assumes full control and accountability	May provide-voice-of-the customer input, but lacks control and accountability Should request 3rd party VPAT during procurement.
TESTING/VALIDATION: Ethical choices related to testing, evaluation, verification, and validation (TEVV) of data, data collection, system design, models, outcomes, measurements, UI/UX, process flows, feature functions, pipeline data, security risks, etc.	Assumes full control and accountability May or may not provide full transparency to all ethical choices	No or limited control over ethical decisions May request disclosure during procurement, but limited ability to validate responses. May use 3rd party auditor to attempt validation
DEPLOYMENT: System integrations, determining user roles & security, admin and end-user training, TEVV, piloting, and launch.	No or limited control May provide implementation support resources and instructions	Assumes full control and accountability May require contractual obligation to assist in implementation accuracy
MONITORING: Output, system usage, users, and cyber threats, adverse incidents, etc.	No or limited control May request access through contractual terms	Assumes full control and accountability May require contractual obligation to assist i
INPUT DATA: Accurate, consistent, appropriate, complete data entered into the system	No or limited control May request controls and limits through contractual terms	Assumes full control and accountability
USAGE: Appropriate, trained users, avoiding misuse/disuse/over-use/under-use/abuse/over-trust	No or limited control May request controls and limits through contractual terms	Assumes full control and accountability
REDRESS: Managing and resolving adverse incidents	Should establish mutual agreement in contract	Should establish mutual agreement in contract
SYSTEM UPDATES: Version documentation, testing, communication, piloting, release management, decommission decision	Assumes full control and accountability May or may not provide full transparency to all ethical choices	No or limited control over ethical decisions May request controls and limits through contractual terms