SHARED ASSESSMENTS

Planning, Due Diligence, and Contracting for Third Party AI

Chris Johnson, Senior Advisor, Shared Assessments

Introduction

- Founder of Third Party Risk Advisors, L.L.C., is a Senior Advisor to Shared Assessments where he focuses on healthcare, insurance, and artificial intelligence and emerging technology.
- 25+ years of experience helping clients effectively manage risk while exhibiting a passionate and dynamic leadership style.
- Prior to joining Shared Assessments, Chris led third party risk management and information technology initiatives at Bristol Myers Squibb, Bank of America, Merrill Lynch, KPMG, and Marriott International.

Connect with Chris via email or LinkedIn
E-mail: chrisjohnson@sharedassessments.org
LinkedIn: https://www.linkedin.com/in/johnsonchrisw/

Chris Johnson
Senior Advisor, Shared Assessments

SHARED ASSESSMENTS

Session Overview

Landing The Right Agent: Planning, Due Diligence, and Contracting for Third Party AI is a practical session designed for leaders navigating the risks and opportunities of AI adoption.

The presentation explores how to align AI use cases with business strategy, conduct effective due diligence on suppliers' transparency, data practices, and model performance, and negotiate contracts that safeguard accountability and resilience.

Attendees will walk away with actionable insights and proven governance practices to strengthen their approach to third-party AI engagements.

SHARED ASSESSMENTS

Why This is Important

We rely heavily upon third-parties for AI technology and thought leadership (AI is third-party)

- 78% of companies are highly reliant on third-party AI (58% exclusively)
- 90% of companies have considered buying an AI solution
- BUY solutions are twice as likely to reach full deployment than BUILD solutions

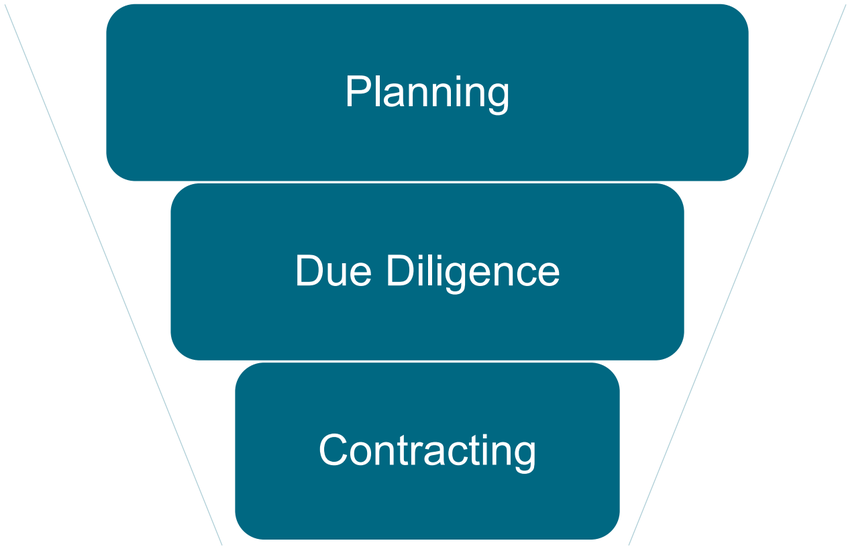
Not all AI implementations are a success – poor planning may be the problem

- 95% of GenAI pilots fail to deliver measurable business impact or ROI
- Reasons for failure include: poor data quality, lack of clear business problem definition, weak change management and culture, insufficient governance, and unrealistic expectations

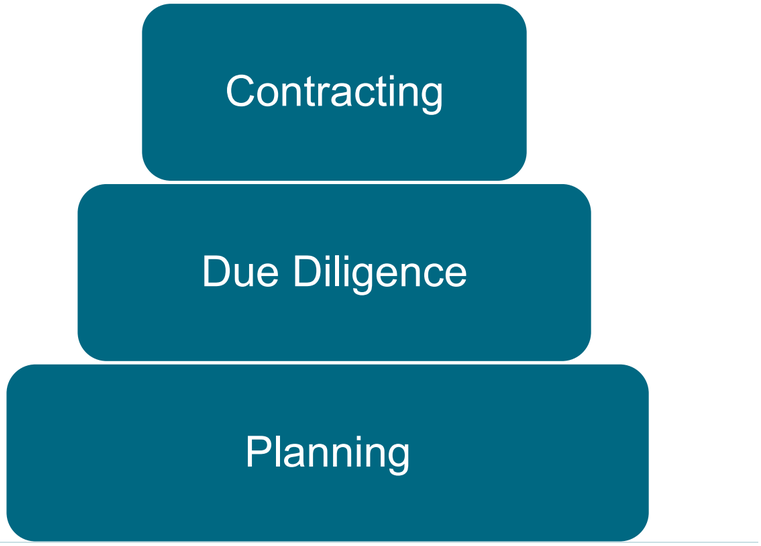
SHARED ASSESSMENTS

Today’s Focus: Planning, Due Diligence, Contracting

Think of the first three phases of the TPRM lifecycle as a funnel – Planning filters use cases, Due Diligence validates readiness, and Contracting embeds protections.



You can also think of the first three phases as building blocks – Planning forms the foundation, Due Diligence strengthens the structure, and Contracting locks it in place.



SHARED ASSESSMENTS

Planning Considerations

Consideration	Description
Understand the Type of AI Solution	Clarify if AI is the core product/service or an internal tool
Strategic Alignment and Risk Tolerance	Ensure AI use aligns with business goals and acceptable risk levels
Identify Oversight and Resource Needs	Assess internal expertise and resources for AI risk governance
Recognize AI-Specific Risks	Identify risks unique to AI, such as bias, opacity, and security threats
The Importance of Enterprise-Wide Collaboration	Foster cross-functional coordination for AI planning and oversight
Plan for Lifecycle Governance	Anticipate model evolution, review cadence, and exit strategies

"Failing to plan is planning to fail" – Benjamin Franklin

SHARED ASSESSMENTS

Planning Considerations

1. Determine if AI is central to the product or used internally to enhance service delivery.

	AI is the primary product or service	*AI enhances service delivery*
Definition	Suppliers offering native solutions where AI is central to the product's function and value	Suppliers using AI internally to enhance efficiency, lower costs, or support decision-making without offering AI directly to clients
Example	A supplier offering AI-enabled tools, such as a ring-fenced enterprise copilot or a fraud-detection engine	A supplier performing supplier assessments may use AI to assist with the report-writing process
Challenges	Predictability, accountability, responsible use, and data governance	Limited transparency, opaque decision logic, and reduced auditability

Why this is important: This helps determine what governance is needed.

SHARED ASSESSMENTS

Planning Considerations

2. Ensure AI use aligns with business goals and acceptable risk levels.

   - How will the AI service address a known business need or an operational gap?
   - What are the benefits and are they clear and measurable?
   - Could regulatory uncertainty, ethical concerns, or other risks exceed our risk appetite?

Why this is important: Companies can block or redirect high-risk use cases that misalign with current strategic or sector-specific regulatory obligations.

SHARED ASSESSMENTS

Planning Considerations

3. Assess internal expertise and resources for AI risk governance

   - Attorneys to assess emerging AI regulations and intellectual property (IP) implications
   - Engineers to evaluate the design, explainability, and performance
   - Security Analysts to assess risks such as prompt injection and model poisoning
   - Privacy Officers to evaluate how data is used for training or inference
   - Compliance Specialists to evaluate alignment with policies and regulatory expectations

Why this is important: Where gaps exist, companies may need to engage external experts or consider delaying the engagement until sufficient oversight can be established.

SHARED ASSESSMENTS

Planning Considerations

4. Foster cross-functional coordination for AI planning and oversight

   - Some companies are formalizing this collaboration by creating AI governance bodies, such as an Office of AI or an AI Review Board, that review use cases, ensure compliance with internal standards, and support decision-making across the lifecycle.
   - Some companies embed AI risk questions into their Inherent Risk Questionnaires, with clearly defined escalation paths for high-risk use cases.

Why this is important: AI impacts every part of the enterprise – legal, operational, reputational, and ethical – requiring cross-functional collaboration for effective planning.

SHARED ASSESSMENTS

Planning Considerations

5. Identify risks unique to AI, such as bias, opacity, and security threats

- **Bias and discrimination:** AI may reinforce unfair or unethical patterns.
- **Opacity:** Some models lack transparency and are hard to explain.
- **Data misuse:** Sensitive data may be exposed or reused without consent.
- **Security vulnerabilities:** Models can be attacked or manipulated.
- **Regulatory uncertainty:** Compliance expectations evolve quickly.

Why this is important: Traditional processes may not adequately capture risks unique to AI.

SHARED ASSESSMENTS

Planning Considerations

6. Anticipate model evolution, review cadence, and exit strategies

- How frequently will the AI be reviewed for fairness, accuracy, or compliance?
- What is the exit strategy if there is unacceptable risk or the supplier is no longer viable?
- How will ownership, portability, or continuity issues be addressed at termination?
- Will the effort to switch to another vendor prevent us from switching (e.g., vendor lock-in)?
- What is the model life expectancy? Will support extend once a new model is released?

Why this is important: AI systems evolve, sometimes in dramatic fashion and without notice.

SHARED ASSESSMENTS

Due Diligence Considerations

Consideration	Description
Assess AI Governance Maturity *	Evaluate supplier readiness and governance structure
Evaluate Transparency and Use Case Clarity	Understand how and where AI is used
Review Data Use and Protection Practices *	Examine data sources, privacy, and safeguards
Confirm Legal and Regulatory Readiness	Verify compliance with evolving AI laws and standards
Evaluate Model Risk Management and Performance Monitoring *	Assess model oversight, testing, and resilience

“You have to do your homework; you have to do your due diligence" - Chad Mendes

SHARED ASSESSMENTS

Due Diligence Considerations

1. Assess AI Governance Maturity

   - Common elements of a mature program may include: documented AI policies and principles, defined roles and responsibilities, opt-out options that enable human-only review, and procedures for testing, validating, and monitoring AI models
   - Understand the origin and structure of the AI system: Is it a proprietary model developed in-house, an open-source solution, or a foundational model built by another entity? Is it run locally, in the cloud, or in a hybrid deployment? Each structure carries different implications for transparency, control, and downstream dependencies.

   Why this is important: A structured AI governance function strongly indicates a company's readiness and reduces the likelihood of unmanaged risks later in the engagement.

SHARED ASSESSMENTS

Due Diligence Considerations

3. Review Data Use and Protection Practices

- What data were used to train the model, and how were they obtained?
- Does the dataset reflect the source diversity needed to avoid discriminatory outcomes?
- Is sensitive data involved, and if so, are privacy-preserving techniques applied?
- Will customer or company data be used to train or fine-tune the model?
- Are safeguards, such as data minimization, encryption, or access controls in place?
- What data remains within the company, and what data resides with the supplier?

Why this is important: If data is not carefully managed, AI can amplify existing risks.

SHARED ASSESSMENTS

Due Diligence Considerations

5. Evaluate Model Risk Management and Performance Monitoring

- Confirm the supplier tracks model accuracy, drift, and retraining needs.
- Ensure the supplier provides insight into decision logic or uses HITL controls.
- Request an AI-BOM or SBOM to support supply chain transparency.
- Require evidence of red teaming or adversarial testing to evaluate resilience.
- Expect proactive client notification for zero-day or other material vulnerabilities.

Why this is important: Model risk management helps AI systems remain accurate, resilient, and transparent – reducing the likelihood of errors, ethical breaches, or regulatory violations.

SHARED ASSESSMENTS

Contracting Best Practices

- Run a “litmus test” to verify that a supplier's offering is genuine AI and not just marketing
- Determine whether AI is the core product or an internal tool supporting service delivery
- Use SBOMs and AI-BOMs to enhance—not replace—contractual risk controls
- Maintain an inventory of AI contracts for visibility and governance
- Align contract terms with internal AI and cybersecurity frameworks
- Include flexible terms to adapt to evolving technology and regulations
- Ensure contracts reflect obligations under new AI laws like the EU AI Act

“Education is when you read the fine print. Experience is what you get if you don’t” – Pete Seeger

SHARED ASSESSMENTS

Contracting Considerations

Section	Considerations
Data Rights and Ownership	Define data categories, ownership, and permitted use to protect privacy and control.
System Transparency and Disclosure Obligations	Require disclosure of model details, updates, and third-party components.
Explainability and Interpretability	Ensure AI outputs are understandable, and decisions can be explained or interpreted.
Human Oversight and Decision-Making Safeguards	Require human-in-the-loop controls for high-impact or sensitive AI decisions.
Performance and Accountability	Establish AI-specific SLAs and hold suppliers accountable for biased or harmful outputs.
Indemnification and Liability	Define liability for AI-related harms, IP issues, and regulatory violations.
Security and Confidentiality	Mandate strong controls to protect data, model integrity, and prevent unauthorized access.
Ethical and Regulatory Compliance	Ensure supplier adherence to fairness, transparency, and evolving AI regulations.
Audit and Monitoring Rights	Secure audit rights across the AI lifecycle to verify compliance and assess risk management.
Termination Provisions	Define exit procedures, data return or deletion, and continuity.

SHARED ASSESSMENTS

Conclusion

- Third-party delivery and use of AI solutions has expanded significantly.
- Planning and Due Diligence are essential for safely and responsibly adopting AI.
- Traditional contracting practices must evolve to address these new risks.
- TPRM leaders play a critical role in enabling the safe and effective use of AI.

SHARED ASSESSMENTS

Third-Party AI Governance: A Leaders Guide

This reference distills best practices into a clear, actionable guide for leaders navigating AI-enabled relationships.

Planning	Due Diligence	Contracting
• **Define AI's Role:** Clarify if AI is the core product/service or an internal tool. • **Decide Fit:** Confirm alignment with objectives and risk appetite; disengage early if needed. • **Align Resources:** Ensure expertise in legal, compliance, privacy, and technical oversight. • **Plan Oversight:** Define review cadence, reassessment triggers, and exit strategies.	• **Test Governance:** Look for AI policies, roles, validation, and ethical review mechanisms. • **Demand Transparency:** Require model cards, training documentation, and AI/S BOMs. • **Scrutinize Data:** Verify data diversity, privacy safeguards, and limits on secondary use. • **Validate Regulations:** Check compliance with EU AI Act, NIST AI RMF, ISO/IEC 42001, etc. • **Probe Security:** Confirm adversarial testing, monitoring, and third-party dependency visibility.	• **Tailor Clauses:** Differentiate terms for core AI products vs. internal-use AI. • **Lock Data Rights:** Define ownership of input/output/derived data, require change notices, and updated AI/S BOMs. • **Human Oversight:** Mandate HITL controls and AI-specific SLAs for performance. • **Liability & Security:** Add indemnification for IP, bias, and privacy risks. Require audits. • **Plan Exit:** Avoid lock-in. Ensure termination rights, portability, and continuity.

SHARED ASSESSMENTS

Takeaway for Leaders: Think of the lifecycle as a funnel – Planning filters use cases, Due Diligence validates readiness, and Contracting embeds protections. Skipping steps invites unmanaged risks into your ecosystem.

Shared Assessments' AI & Emerging Technology Papers

Leading Practices and Key Considerations When Contracting for AI

Getting AI Right from the Start: Leading Practices in Planning and Due Diligence

SHARED ASSESSMENTS

How is AI reshaping Third-Party Risk Management?

These briefing papers offer practical guidance to strengthen due diligence, governance, and contracting practices in an evolving regulatory and risk landscape.

Download & Learn More

www.sharedassessments.org/papers-and-studies