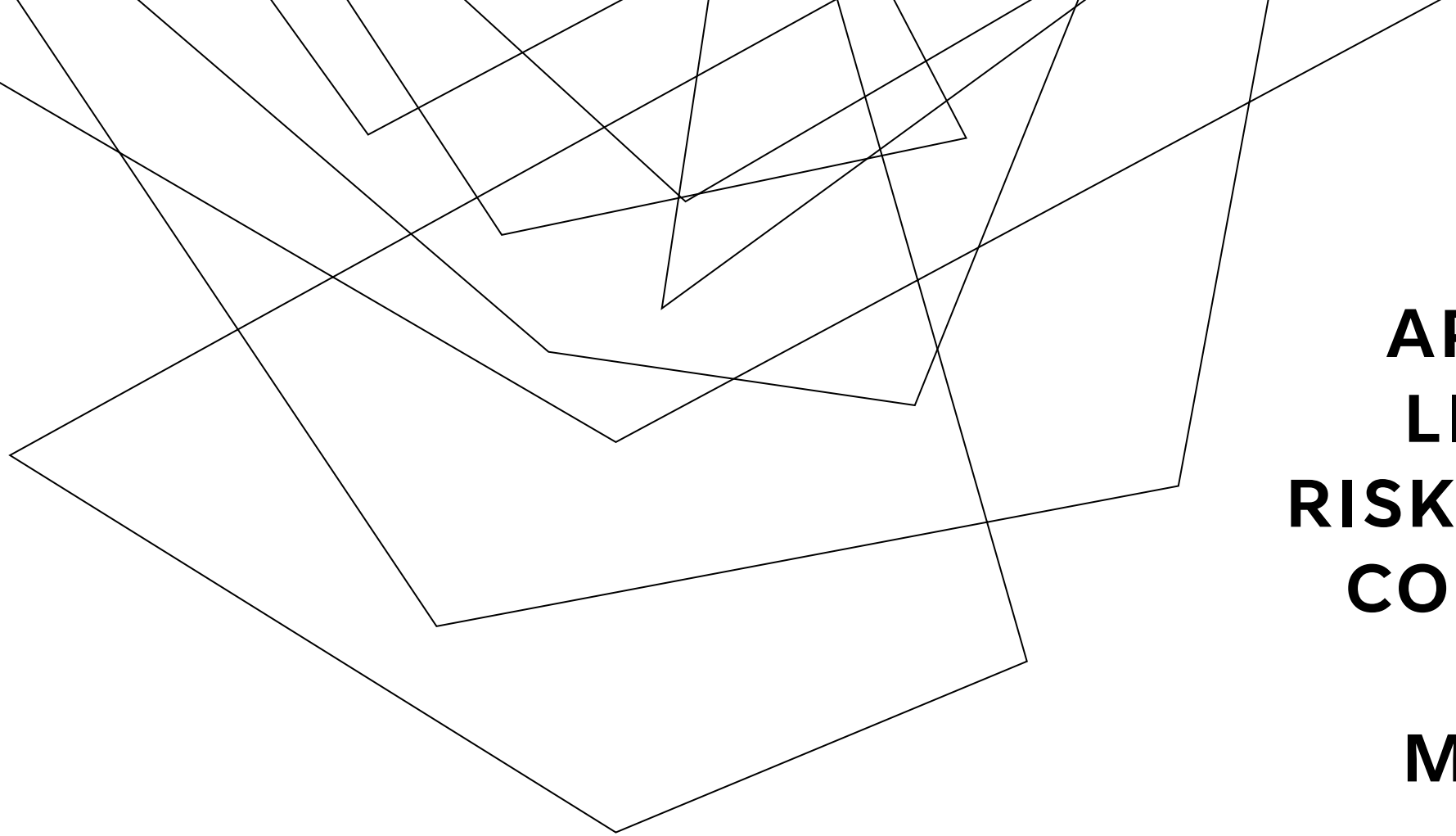


APPLIED AI LITERACY: RISK AND TEXAS COMPLIANCE

MODULE 2

TEXAS DEPARTMENT OF INFORMATION RESOURCE CERTIFIED AI TRAINING
AIQ GATE – CHARLOTTE WILBORN

LEARNING OBJECTIVES

-APPLY 10 PRINCIPLES OF THE TEXAS AI CODE OF ETHICS

- CLASSIFY AI SYSTEMS BY RISK LEVEL

-UNDERSTAND AGENCY REQUIREMENTS

-IMPLEMENT RISK MANAGEMENT STRATEGIES

-BUILD A COMPLIANT AI PROGRAM FOR YOUR AGENCY

THE TEXAS AI CODE OF ETHICS

The Texas Department of Information Resources has established a comprehensive Code of Ethics for AI use by state and local government.

All government entities must:

1. Adopt this Code of Ethics
2. Follow ethical principles when procuring, developing, deploying, or using AI systems
3. Document compliance

Authority: Texas Government Code *§ 2054.702*

THE 10 ETHICAL PRINCIPALS

1-5 states foundational commitments.
6-10 translate how to operationalize those commitments.

Module 1 covered Pillars 1-5:

1. Human Oversight
2. Fairness
3. Accuracy
4. Transparency
5. Accountability

Module 2 covers Principles 6-10:

6. Redress
7. Data Privacy
8. Security
9. Regular Evaluation
10. Documentation

PRINCIPLE 6 – REDRESS

- Definition: Providing an explicit mechanism for individuals to seek remedy when systems make consequential decisions that may cause unlawful harm.
- Requirements:
  1. Provide method for individuals to challenge AI decisions.
  2. Designate a point of contact for redress requests.
  3. Develop internal procedures for employees to identify and remedy negative impacts.
- Example: An AI system denies a constituent's application for benefits. The constituent must have:
  - Clear information on how to appeal
  - Designated person/team to contact
  - Documented process for human review of decisions for both constituent and government entity

PRINCIPLE 7 – DATA PRIVACY

- Definition: The obligation to collect, store, use, share, and dispose of personal data in a manner that protects individual's rights, limits unnecessary intrusion, and ensures that information is only used for authorized, transparent, and lawful purposes.
- Requirements:
  1. Collect only minimal PII needed for operation
  2. Understand what PII the system uses and how
  3. Track how PII is collected, stored, and shared
  4. Train employees on risks of inputting sensitive data into public AI
  5. Practice data minimization
  6. Delete PII consistent with retention schedules

Example: Entering constituent names and addresses into ChatGPT to generate data analysis for zoning purposes.

- Many AI systems use inputs/outputs to train models and may incidentally share inputs with other users. NEVER put PII into public models.

PRINCIPLE 8 – SECURITY

- Definition: The protection of systems, data, and outputs against unauthorized access, manipulation, disruption, or misuse, ensuring that AI operates reliably, safely, and as intended throughout its lifecycle.
- Requirements:
  1. Implement risk-based security measures.
  2. Control authorization/authentication of users
  3. Control access of external parties to internal systems
  4. Protect confidentiality and integrity of data
  5. Monitor for and track security incidents
  6. Train employees on AI security risks

Example: A chatbot interface must have security guardrails that prevent users from injecting malicious prompts that expose internal data or bypass control mechanisms.

PRINCIPLE 9 – REGULAR EVALUATION

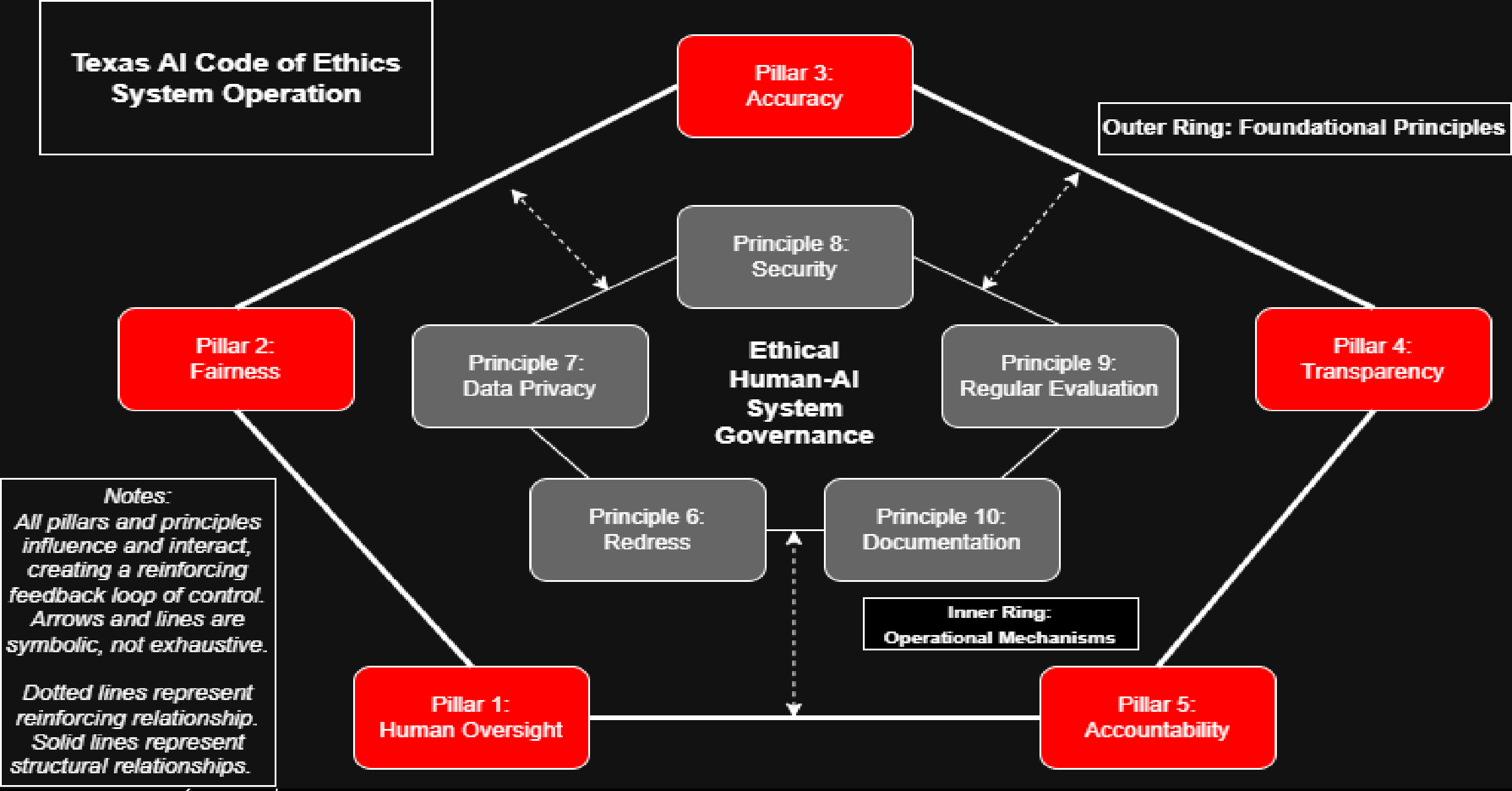
- Definition: The ongoing, systemic assessment of an AI system to ensure it continues to operate as intended, remains accurate and reliable, and complies with applicable standards, policies, and ethical requirements through its lifecycle from deployment to retirement.
- Requirements:
  1. Establish methods for performance assessment
  2. Review whether the system continues to serve its original intended purpose
  3. Monitor for performance degradation and drift patterns
  4. Document all evaluations

Example: Internal risk assessment chooses to perform a full evaluation of a constituent facing chatbot on a monthly basis to check internal alignment with external principles and goals.

PRINCIPLE 10 – DOCUMENTATION

- Definition: The comprehensive, accurate, and accessible record of an AI system's design, purpose, data, operation, decisions, and oversight processes, ensuring transparency, accountability, and auditability throughout its lifecycle.
- Requirements:
  1. Sources of allowed to be used in/with the AI systems
  2. How the system is modified throughout its lifecycle, from initial deployment to retirement
  3. Pre-deployment assessments
  4. Ongoing monitoring and testing results
  5. Complaints and incidents
  6. Evaluations and metrics
  7. Any documentation compliance requirements by specific field
  8. Any specific process and procedure relating to the use of AI systems

Texas AI Code of Ethics System Operation



Notes:
All pillars and principles influence and interact, creating a reinforcing feedback loop of control. Arrows and lines are symbolic, not exhaustive.

Dotted lines represent reinforcing relationship. Solid lines represent structural relationships.

RISK MANAGEMENT AND CLASSIFICATION

RISK

Risk = The potential for an AI system to produce outcomes that cause harm, violate rights, fail to meet legal, ethical, or operational requirements, considering both the likelihood of the occurrence and the severity of the impact.

Risk is based on:

- What the system does
- How it is used
- Who it affects
- What data is processed
- What decisions it makes

Texas Law distinguishes:

1. Lower Risk Systems – general use with limited impact
2. Heightened Scrutiny AI Systems – Systems that require enhanced oversight due to higher risk

HEIGHTENED SCRUTINY AI SYSTEMS

Heightened Scrutiny AI System: A system that has the potential for being a factor in consequential decisions concerning individual's:

- Civil rights or civil liberties
- Access to government services/benefits
- Education
- Employment
- Financial services
- Healthcare
- Housing
- Legal Status
- Essential government resources

EXAMPLES OF HEIGHTENED SCRUTINY SYSTEMS

Likely Heightened Scrutiny – Systems that:

1. Evaluate benefit eligibility
2. Score job applications for government positions
3. Assess child welfare cases
4. Predict risk assessments
5. Process healthcare coverage decisions
6. Determine housing assistance qualification

NOT Heightened Scrutiny:

1. Asking ChatGPT about general public available information
2. Asking AI to summarize meeting notes (general and not confidential information)
3. Automated systems categorizing emails
4. Tools generating general draft internal communications

RISK ASSESSMENT REQUIREMENTS

Written Risk Assessments must be conducted before deploying Heightened Scrutiny Systems. The assessment must include:

1. Security Risks
    - Known vulnerabilities
    - Mitigation measure available
    - Unavoidable, unmitigated risks
2. Performance Metrics
    - Accuracy rates of outputs
    - Operational efficiency
    - Known error patterns
3. Transparency
    - How the system makes decisions
    - Data sources and training procedures
    - Availability of inputs/outputs for monitoring

RISK MITIGATION STRATEGIES

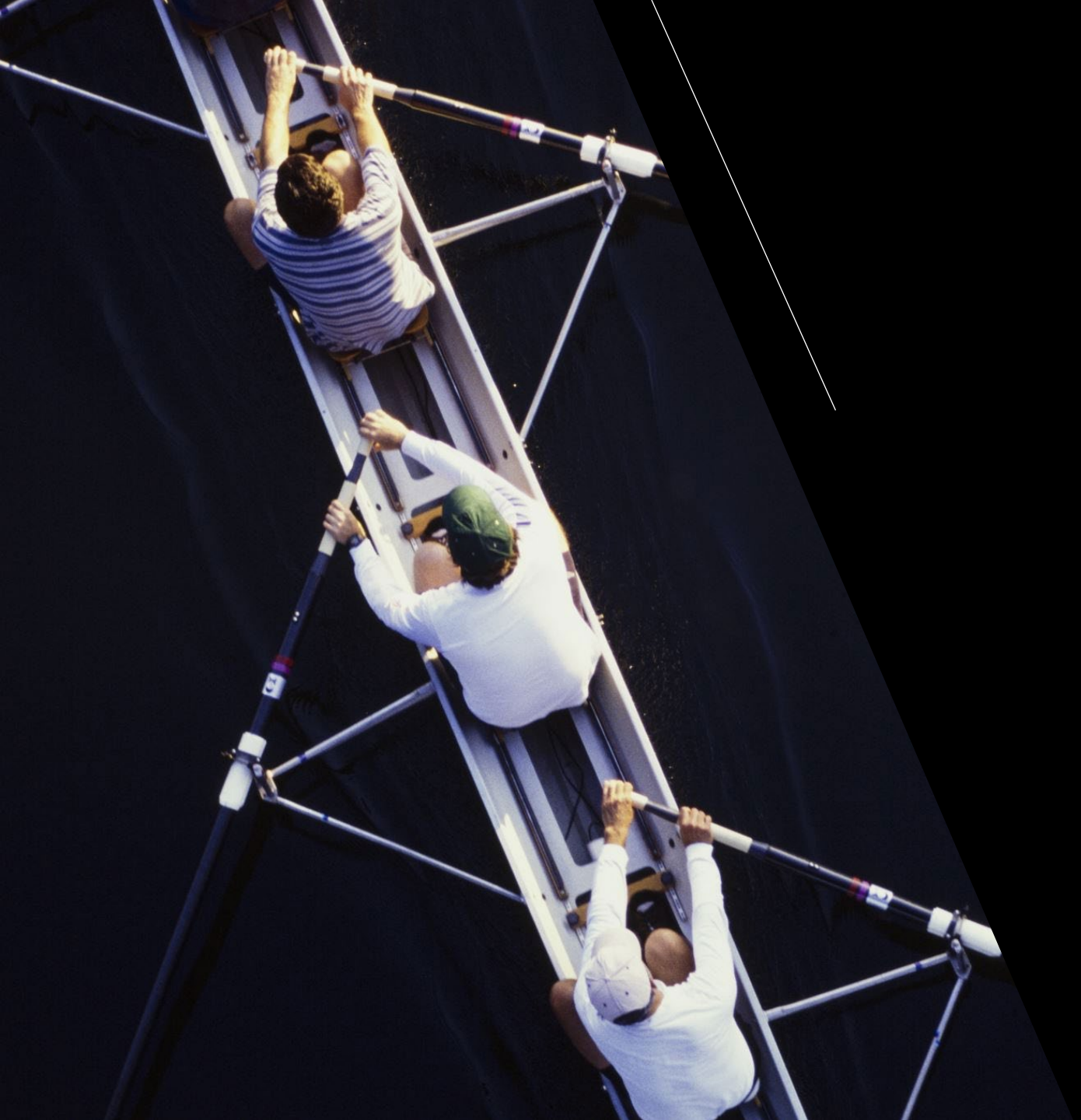
Mitigation techniques and measures should match risk level of system use.

For all systems:

1. Clear acceptable use policies
2. Employee training of procedures and system use
3. Regular monitoring
4. Documentation

For Heightened Scrutiny Systems:

1. Enhanced human oversight
2. Formal review processes
3. Dedicated monitoring protocols
4. Regular accuracy testing
5. Incident response procedures
6. Redress mechanisms



ORGANIZATIONAL REQUIREMENTS

THE AI RISK OFFICER

Every state and local government must designate an AI Risk Officer.

- Responsibilities:
  - Promote ethical AI procurement, development, deployment, and use
  - Ensure compliance with the Texas AI Code of Ethics
  - Align with NIST AI Risk Management Framework
- Responsibilities for Heightened Scrutiny Systems:
  - Ensure risk assessments are completed
  - Evaluate risk assessments
  - Approve or deny deployment
  - Notify executive leadership of deployment decisions
- This role may be:
  1. A dedicated position, OR
  2. Added to an existing employee’s duties

THE AI SYSTEM INVENTORY

Agencies must establish a process to identify and inventory all heightened scrutiny AI systems.

Inventories should include:

1. System name and purpose
2. Date of deployment
3. Department/employees approved for use
4. Risk classification
5. Review schedule
6. Risk Assessment status
7. Escalation procedures

Inventories should be living documents – systems and information should be updated as systems and procedures change.

ACCEPTIBLE USE POLICIES

For Heightened Scrutiny Systems, agencies must:

- Identify acceptable use cases
- Identify system limitations
- Adopt an acceptable use policy
- Train all employees on the policy

Policies must define:

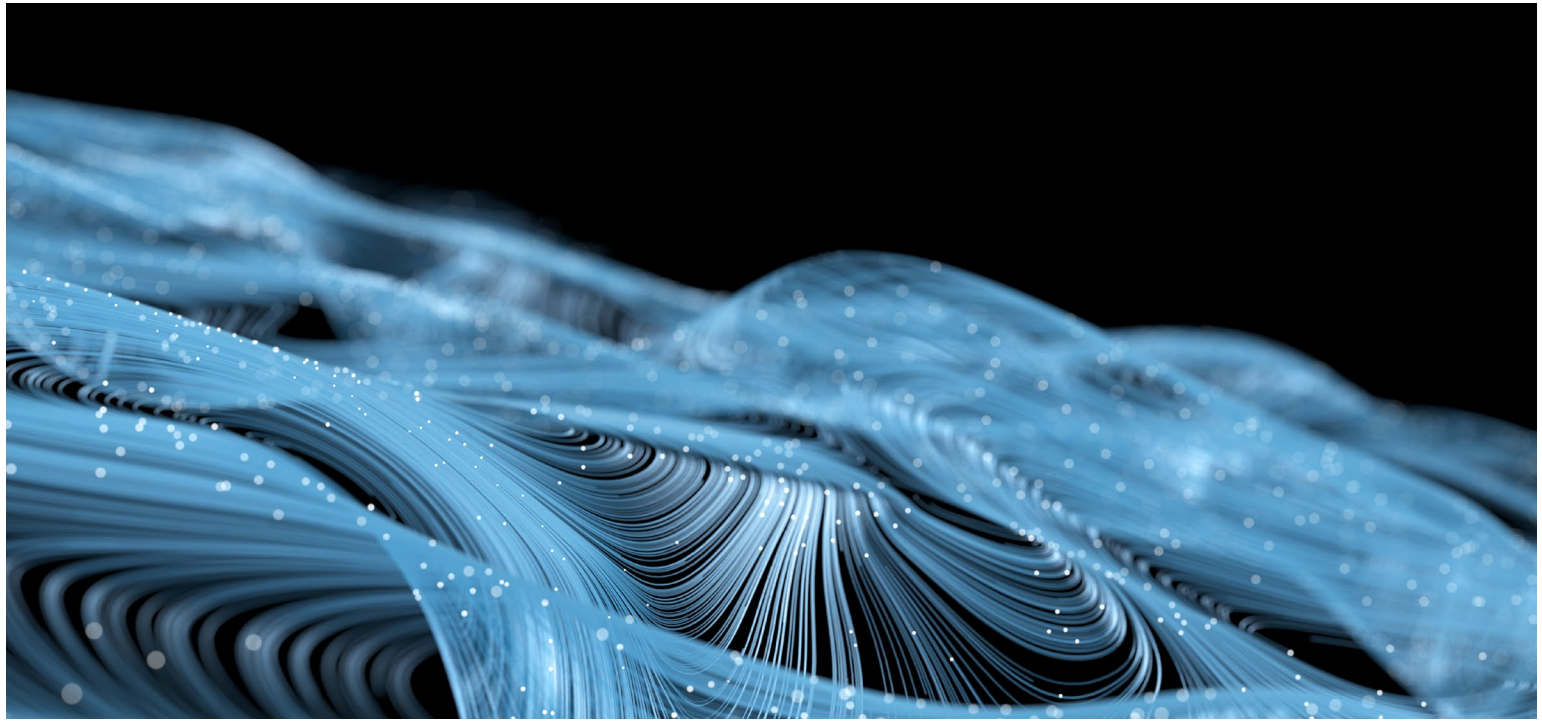
- Approved uses
- Prohibited uses
- Who can access the system
- What data can be processed
- Review and approval requirements
- Incident reporting procedures
- Escalation procedures

TRAINING REQUIREMENTS

Employees who access, use, or manage Heightened Scrutiny Systems must receive training.

- **The training must include:**
  1. Identified risks
  2. Appropriate risk mitigation techniques
  3. System limitations
  4. Acceptable use policies
  5. Incident reporting
  6. When to escalate to human review
- **Training must be:**
  1. Provided prior to system access
  2. Documented
  3. Updated as procedures/accesses change
  4. System and risk specific

THE AI LIFECYCLE



STATIC VS NON-STATIC TOOLS

Deterministic (Static) Tools

Operate with fixed algorithms, providing predictable results based on predefined rules.

Probabilistic (Non-Static) Tools

Use models that incorporate randomness, yielding different outcomes across runs to handle uncertainty.

Comparison & Use Cases

Static tools are ideal when consistency is needed, while probabilistic tools excel in complex, uncertain environments.

AI SYSTEMS VERSUS TRADITIONAL SOFTWARE

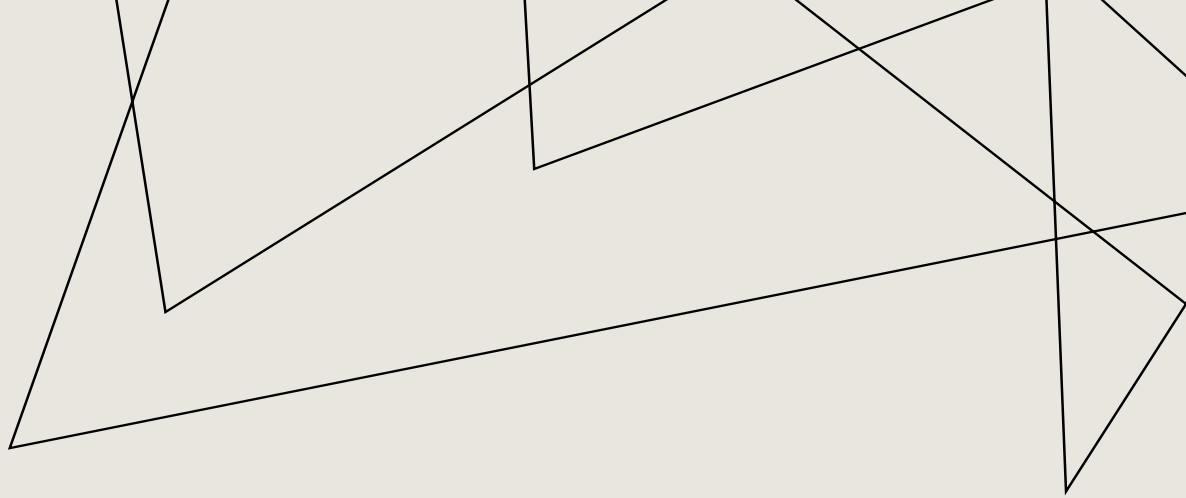
Traditional Software: Programmed and behaves predictably.
AI Systems: Continuous lifecycle with evolving behaviors.

The AI Lifecycle:

1. Data – Input and Training Data
2. Model Development – System design and training
3. Output Generation – Results produced
4. Feedback – Evaluation and monitoring
5. Improvement – Retraining and Adjustment

This cycle continues through the system's operational life.

STAGE 1 AND STAGE 2



STAGE 1: DATA

- Data is the foundation of AI performance
- Key activities
  - Acquiring and curating data
  - Cleaning and removing known errors
  - Labeling and structuring
  - Confirming accuracy and relevance

Garbage in = Garbage Out

STAGE 2: MODEL DEVELOPEMENT

- Where the model learns patterns
- What happens
  - Engineers define goal
  - Model architecture is designed
  - Model is systematically trained on specific datasets
  - Patterns and relationships are identified by the model
  - Stress testing pre-deployment

STAGE 3: OUTPUT GENERATION

The system produces results:	• Text, analyses, predictions, recommendations
Safety measures decided during Stage 2 are applied:	• Guardrails constrain outputs • Filters prevent harmful content • Access controls limit use
User interaction	• Can see and interpret the output • Apply domain knowledge and context • Make final decisions based on output + human judgment

STAGE 4: FEEDBACK AND MONITORING

Outputs must be evaluated by:

- Users (operational review)
- AI Risk Officer (systematic oversight)
- Auditors (compliance verification)
- Automated monitoring systems

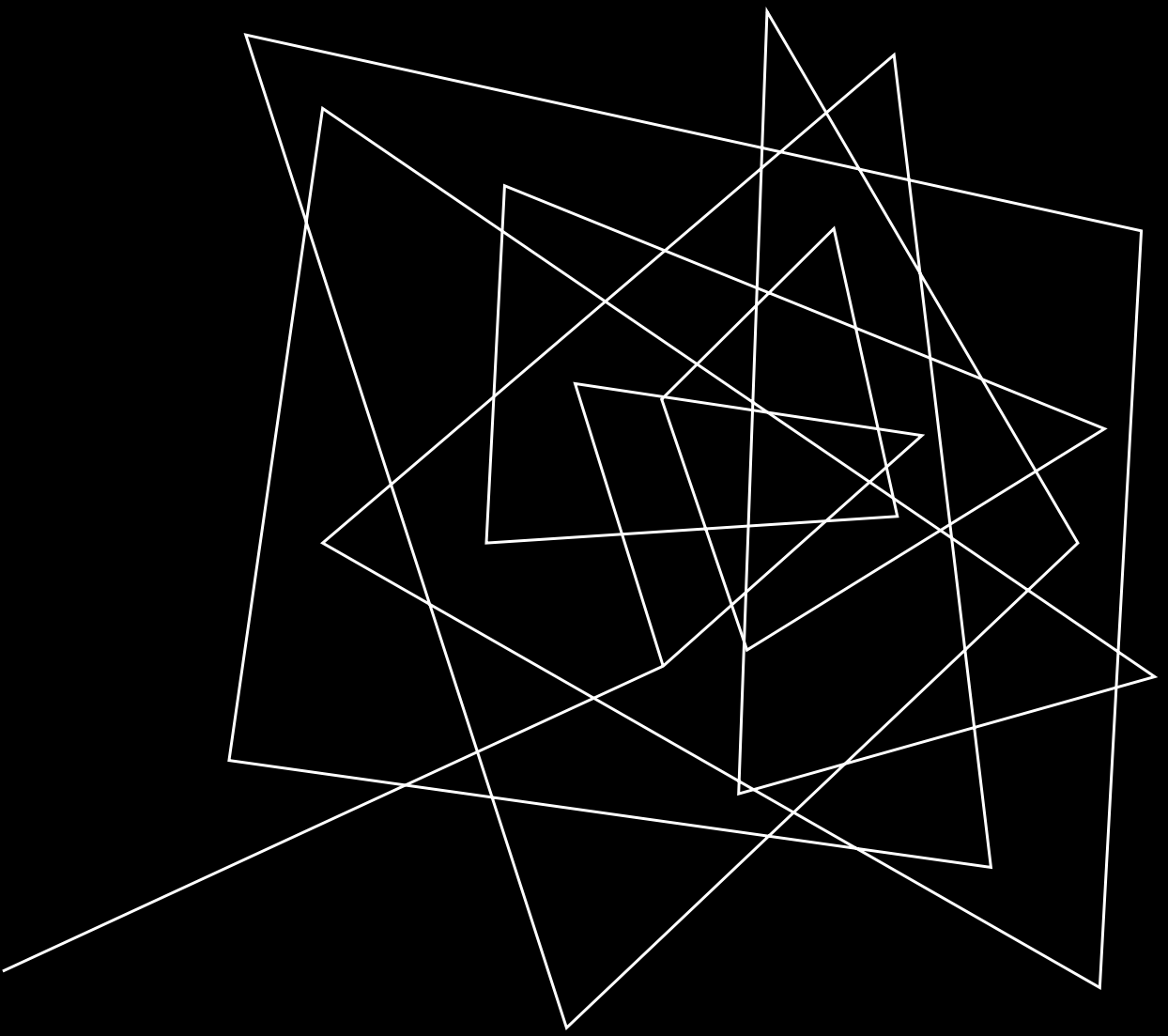
What to monitor:

- Accuracy rates
- Bias indicators
- Hallucinations or errors
- Drift from expected behavior
- User satisfaction
- Negative impacts

STAGE 5: IMPROVEMENT AND ADJUSTMENT

Feedback only matters if it drives improvement.

- Actions may include:
  - Incorporating feedback into training data
  - Adjusting system parameters
  - Retraining or fine-tuning
  - Updating acceptable use policies
  - Enhancing guardrails
  - Retiring the system if it no longer meets needs



REGULATORY ALIGNMENT

TEXAS REQUIREMENTS AND ALIGNMENT WITH FEDERAL FRAMEWORKS

The Texas AI Code of Ethics is grounded in

- NIST AI Risk Management Framework (NIST AI RMF)
- Federal AI governance principles
- National AI initiative standards

This means:

- Texas agencies following state laws are also aligned with federal best practices
- There exists shared vocabulary across jurisdictions
- Interoperability with federal systems and requirements

Learning Texas requirements prepares you for the broader AI governance landscape.

NIST AI RMF

NIST AI RMF provides a structured approach to managing AI risk.

Four Core Functions:

1. Govern – Establish culture and responsibilities
2. Map – Understand context and categorize risks
3. Measure – Analyze and track risks
4. Manage – Prioritize and respond to risks

NIST AI RMF CONTINUED

NIST AI RMF maps directly to the Texas AI Code of Ethics.

- Human Oversight and Accountability > Govern
- Risk Assessment and Regular Evaluation > Map
- Documentation and Monitoring > Measure
- Security, Fairness, Redress > Manage

ai.gov/ai-risk-management-framework

KEY FEDERAL CONSIDERATIONS

While Texas law governs state/local use, federal frameworks should be taken into consideration.

- **For agencies receiving federal funds:**
  - Federal contract requirements may impose additional standards
  - Grant compliance may include AI use restrictions
  - Data sharing with federal agencies requires security alignments
- **For constituent services interfacing with federal programs:**
  - Medicaid/Medicare
  - Social Security Coordination
  - Federal Benefits administration
  - Law enforcement data sharing

Always remember to check all compliance requirements for cross-departmental work.

Q & A

THANK YOU

Charlotte Wilborn
Charlotte@AIQGate.com
Document Title: APPLIED AI LITERACY: RISK AND TEXAS COMPLIANCE - MODULE 2
Version 1.0

Revision Date	Revision Summary
03.21.2026	Created original PPT/PDF.

AI Disclosure Statement:
This document was generated through human-AI collaboration with the use of ChatGPT/Claude/Grok. All content has been reviewed for alignment with NIST RMF and ISO 42001 standards in compliance with current AI data governance as of 03/18/2026.