ASPEN POLICY ACADEMY
aspen institute

The Coordinated AI Requirements (CAIR) Playbook

A Coordinated Evaluation Process for Accessibility, Cybersecurity, and AI Governance

By Tiffani Martin

November 2026

This playbook was developed by an Aspen Policy Academy Fellow while participating in the 2026 Science and Technology Policy Fellowship. This playbook helps public agencies, private companies, colleges and universities, and nonprofit organizations set up a coordinated, enforceable process for evaluating artificial intelligence (AI) systems. The playbook is a step by step guide to help organizations implement the CAIR process. The full project, including a policy brief explaining the Fellow's core recommendations, is available here. Please note that the author's opinions published here are their own. This project was created with the help of AI. Generative AI is experimental and information quality may vary. The content has been reviewed, edited, and finalized by the author. This publication does not reflect the views of the Aspen Policy Academy or the Aspen Institute. This project was developed between June 26 and August 31, 2026, with initial submission on August 31, 2026. The content reflects information available during this period.

Contents

Section 1: Overview of the CAIR Process **2**
Why Coordinated AI Evaluation Is Needed, and Why It Fails Without Authority 2
What the CAIR Playbook Includes 2
Who Participates, Who Decides, and How Conflicts Are Resolved 3
When and Where CAIR Applies: Checkpoints, Triggers, Inventory, and Triage 5

Section 2: The CAIR Process Step by Step **6**
Step 1: Complete the Implementation Charter 6
Step 2: Complete the Readiness Assessment and Launch the 90-Day Road Map 7
Step 3: Measure the Success of the CAIR Pilot and Complete the 6-Month Review) 9
Appendices **10**
Appendix A: Vendor Evidence Checklist 10
Appendix B: Sample CAIR Operating Procedures 11
Appendix C: Sample Conflict Resolution Procedure 13

Section 1: Overview of the CAIR Process

Why Coordinated AI Evaluation Is Needed, and Why It Fails Without Authority

The decision to use and incorporate AI technology into services touches many responsibilities at once: accessibility, cybersecurity, governance, legal duties, operations, privacy, purchasing, and public trust. When departments review these areas separately, gaps appear. A system can pass 1 office's check while creating serious problems for another office or the people who use it. Separate reviews also cause duplicated work, delays, and conflicts that go unresolved. Public agencies, private companies, colleges, and nonprofits all face this problem.

The Coordinated AI Requirements (CAIR) process brings together accessibility findings (can people with disabilities use it?), cybersecurity findings (can it be protected?), and AI governance findings (should this system be used and how?) into one review before an AI system is purchased, deployed, renewed, expanded, or significantly changed.

A coordination process treated as a paperwork project rather than a governance change will not hold: A process with no named leader, no deadlines, no enforcement, and no decision authority becomes voluntary guidance that departments ignore. Therefore, this playbook requires, alongside the process itself, the authority, staffing, and accountability to make it operational.

What the CAIR Playbook Includes

The CAIR Playbook is a step by step guide to help organizations implement the CAIR process. It introduces no new regulation or certification and leaves each department's expertise in place. The CAIR Playbook provides ready to use materials, including filled in examples and sample language, so that teams can begin evaluating systems.

The CAIR Playbook includes the following:

- **CAIR Implementation Charter:** The charter outlines who is involved, defines roles and responsibilities, and establishes key deadlines and success measures to ensure a successful CAIR process.

- **Readiness Assessment:** This assessment checks whether the organization can run coordinated evaluations. Every yes answer must include evidence (a document, a named person, or a recent example) and must state whether the practice is in active daily use or exists only in written policy. Self ratings without proof produce inaccurate profiles. The results distinguish gaps that can be fixed during implementation from gaps (no accessibility expertise, no decision authority, no capacity) that must be fixed before evaluations can begin.
- **Vendor Evidence Checklist (Appendix A):** This checklist provides a short list of proof that vendors must provide before review, covering security, accessibility, how they handle data, and any outside AI tools their product relies on. When evidence is missing or refused, treat the missing item as an unmitigated risk in the findings report.
- **Sample CAIR Operating Procedures (Appendix B):** These procedures are built from this playbook and the Implementation Charter. Keep them short. Define a small mandatory core (scope, triggers, roles, intake, decision categories, escalation, records) and optional components. Long, complicated procedures push teams toward workarounds. Include a fast, simplified path for low risk systems.
- **Sample conflict resolution procedure (Appendix C):** A sample conflict resolution procedure is provided that organizations may use as written, adapt to fit their own structure and timelines, or use as a reference while writing their own. The roles, deadlines, and recordkeeping steps should match what the organization sets in its CAIR Implementation Charter and operating procedures.
- **A minimum viable version:** Small organizations without mature governance functions use the starter model: 1 owner, 1 intake form, 1 joint review meeting covering all 3 domains, and 1 signed decision. Start there and grow.
- **Sector notes:** Notes marking what is universal and what public agencies (records, procurement rules, public accountability) and private companies (commercial risk, contracts, speed to market) must customize.

Who Participates, Who Decides, and How Conflicts Are Resolved

The business owner explains the proposed use, users, and goals. The AI governance reviewer checks the purpose, accountability, oversight, and data practices. The cybersecurity reviewer checks the technical risk, data protection, access, and vendor security. The accessibility reviewer checks whether people with disabilities can complete essential tasks, get equivalent information, and obtain support. Procurement holds the contract gate. Legal and compliance flag obligations. The process owner

consolidates findings and routes decisions. Participants should be drawn from leadership, IT, governance, security, accessibility, legal, procurement, operations, human resources, communications, and audit as relevant.

- **Accessibility joins at intake** (required): The accessibility reviewer participates from the first intake conversation, before design and purchasing decisions are made, with the same authority, time, and resources as security.
- **Conflict resolution follows a defined procedure:** When domains conflict (e.g., a security control blocks assistive technology), the reviewers meet jointly to propose secure, accessible alternatives. Reviewers have 10 business days of joint problem solving. If the conflict remains unresolved at that point, the process owner escalates both positions and their impacts to the person named in the approval chart, who must decide. Every conflict receives a resolution. This mirrors the decision model in 1 Texas Administrative Code (TAC) §219.22(c), under which a designated AI risk officer approves or denies deployment based on the completed risk assessment and notifies the executive head, who may hold final approval.[1]
- **Role specific training** (required): Each participant is trained on exactly what they review, document, approve, and escalate.
- **Affected users participate** (required for public- and employee-facing systems): The people who will experience the system (employees, customers, students, residents, patients, and people with disabilities) take part in testing and feedback before approval.
- **Change is managed through a named change liaison:** CAIR leaves each department's authority intact; say so clearly and often. Appoint 1 change liaison with 3 specific duties: brief each participating department on why the process exists and how it affects their work; collect concerns (loss of control, added liability, workload) and questions from departments on an ongoing basis; and feed those concerns back to the process owner with recommended responses. The liaison also involves departments in designing the procedures so engagement produces visible changes to the process, and the position is named in the charter's resources and capacity field.

When and Where CAIR Applies: Checkpoints, Triggers, Inventory, and Triage

- **Mandatory triggers:** CAIR review should be required, at a minimum, in the following scenarios for an AI technology:
  - before purchase or contract;
  - before build or pilot;
  - before public or employee use;
  - before renewal;
  - after major updates;
  - when purpose, users, data, or environment change;
  - when incidents or barriers appear; and
  - at monitoring intervals.
- **Checkpoints:** CAIR controls the specific checkpoints named in the charter. Contracts are not signed and systems are not deployed without a recorded CAIR decision. Bypassing the checkpoint triggers the enforcement rules.
- **AI inventory:** The process depends on knowing which AI systems exist. Maintain a basic organization wide inventory of AI systems, including AI features embedded in existing platforms, AI bought inside broader technology contracts, and tools tested outside formal procurement. Update it as part of intake, procurement, and IT review. Texas law imposes a comparable requirement on state government entities to identify and inventory all implementations of heightened scrutiny AI systems.[2]
- **Risk-based triage** (required): Before any review begins, every request to buy, build, or use an AI system should be sorted by the amount of risk it poses. This sorting step is called “triage,” and it decides how in-depth the review needs to be:
  - Low risk tools, such as a basic productivity aid, take a fast track with a short combined review, completed within 5–10 business days.
  - High risk systems, meaning anything affecting employment, education, health, benefits, or access to services, get the full evaluation, completed within 20–30 business days. This category parallels the “heightened scrutiny” systems defined in Texas Senate Bill 1964: systems intended to autonomously make, or be a controlling factor in making, a consequential decision.[3]

Section 2: The CAIR Process Step by Step

Step 1: Complete the CAIR Implementation Charter

Before the Readiness Assessment can begin, leadership must complete and sign the CAIR Implementation Charter, which is issued as a separate companion document. The charter puts every foundational decision in writing at the start of the process:

- **A named executive sponsor with ongoing duties.** The sponsor assigns staff and funding, sets deadlines, requires departments to participate, resolves disputes between departments, and receives a short written status report every month until launch.
- **A named process owner.** A single, specific position is accountable for moving the organization from discussion to operation. Everyone must be able to answer "who is leading this?" with one name.
- **A signed approval chart.** This document names exactly who can accept risk, require fixes, delay a system, or reject it and who breaks ties when departments disagree. No evaluation may begin until this is signed.
- **The checkpoints that the CAIR process controls.** Outline the specific existing checkpoints that this CAIR process affects – for example, a contract signature or deployment approval that cannot be passed without a completed CAIR decision. CAIR must operate inside an existing process.
- **Enforcement rules.** State what happens when a team bypasses the process, submits incomplete information, or deploys before evaluation: Purchases are not signed, systems are not deployed, and the process owner has stop-work authority backed by the sponsor.
- **Resources and capacity.** Name who will do the review work and how their existing workload will be adjusted, including the change liaison role described in Section 4. If reviewers keep their full current workload, the process will stall. Set turnaround expectations for each review type: Fast track reviews are completed within 5–10 business days and full evaluations within 20–30 business days, adjusted to organizational capacity and recorded in the charter. This 2-tier structure is consistent with the tiered approach outlined in 1 TAC Chapter 219, which reserves full written risk and impact assessments for "heightened scrutiny" AI systems while applying baseline ethical standards to all others.[4]
- **Deadlines and measures.** Adopt the 90-day road map and the success measures with target dates and named owners.

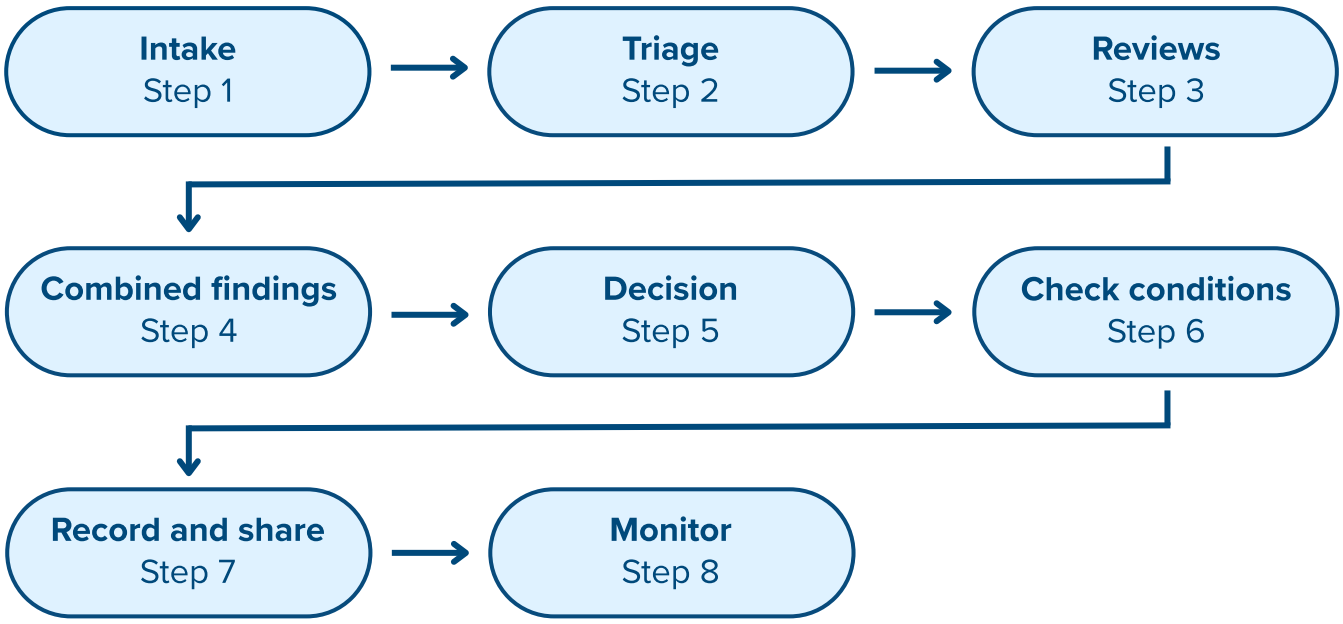
The charter exists because shared participation without individual accountability leads every department to assume another office is leading. The charter makes ownership, authority, and consequences explicit before the first meeting.

Step 2: Complete the Readiness Assessment and Launch the 90-Day Road Map

For each milestone below, set a target date and name 1 person who will be responsible. Adjust the timeline to fit the size of your organization.

- **Days 1–15: Get ready.** Complete the Readiness Assessment, which checks whether you have the evidence you need before you start. If the assessment identifies problems that would stop the process from working, fix them or formally decide to accept the risk before moving on.
- **Days 16–45: Prepare to run the process.** Customize the 4 required tools in your operating procedures: the intake form, the rules for sorting requests by risk (triage), the categories you will use for decisions, and the process for resolving disagreements. Sign the decision matrix, which shows who can make which decisions. Start your inventory of AI systems. Make sure every form meets Web Content Accessibility Guideline 2.2 Level AA, the same accessibility standard you will use to evaluate the AI systems as well as the W3C Accessibility Maturity Model. Use the Vendor Evidence Checklist in Appendix A to request more information from an AI vendor about a specific product.
- **Days 46–60: Review roles and responsibilities.** Make sure each person understands their role and responsibilities. Set up 1 shared place to store forms, evidence, findings, and decisions. Confirm how much work people can realistically take on and how quickly reviews should be finished.
- **Days 61–90: Run a CAIR test.** Pick 1 small, low risk system to test the process, with an owner who is willing to work with you. Don't choose a complicated or sensitive system for this first test. If the test runs into every possible problem at once, the whole process can look broken, even when it isn't. Run the full process on this 1 system from start to finish: intake, triage, the 3 required reviews, combining the findings, making a decision, and recordkeeping. Fix anything that was confusing or duplicated. The Sample CAIR Operating Procedures in Appendix B show how the 8-step CAIR test can work in practice. Appendix C provides a Sample Conflict Resolution Procedure. Organizations may modify the sample to fit their structure, staffing, and existing procedures.

Every CAIR test follows these 8 steps:



↻ Sent back for more work at Step 5: return to step 3

↻ Major change, or yearly check for high risk systems: return to step 1

Figure 1. The 8 steps of a CAIR test.

1. **Intake.** Someone submits a request to buy, build, or use an AI system.
2. **Triage.** The request is sorted by risk to decide how in depth the review should be.
3. **Reviews.** Three reviewers look at the system: 1 for accessibility (can people with disabilities use it?), 1 for cybersecurity (can we protect it?), and 1 for AI governance (should we use it and how?).
4. **Combined findings.** The reviewers bring their results together in 1 report. It lists where the reviews disagree, what depends on something else being fixed first, any risks that remain, and what must be done.
5. **Decision.** The person named in the approval chart chooses 1 of 4 outcomes: approve, approve with conditions, send back for more work, or stop.
6. **Check conditions.** If the system was approved with conditions, confirm they have been met before it goes live.
7. **Record and share.** Save the decision and the reasons for it in the system's decision record (the file that holds its forms, findings, and decision), and tell the people affected.

8. **Monitor.** Name an owner and set a schedule to check for problems, including product or AI updates, vendor changes, security incidents, complaints, and accessibility issues. Write the schedule into the decision record. This follows 1 TAC §219.23, which requires Texas state agencies to write down, before using a high risk AI system, how they will check it for accuracy and harm, and how often.[5]

Two minimum rules always apply. High risk systems should be re-reviewed at least once a year. Any system is re-reviewed when there is a major change to the system, to the data it uses, or the purposes it is used for. The owner named in step 8 decides whether a change is major, and should ask the process owner when unsure. Oversight does not stop once a system is approved.

This completes the initial CAIR pilot process. After the initial pilot, keep reviewing low-risk systems until your team can complete reviews on time without major problems. Then move on to more complex systems, and take on high risk systems last.

Step 3: Measure the Success of the CAIR Pilot and Complete the 6-Month Review

Record baseline data at launch, then track a small set of indicators: how many AI systems were found and evaluated, evaluation turnaround times, risks and accessibility barriers caught before deployment, conflicts resolved, duplicated reviews eliminated, bypasses detected, and user-reported problems after deployment. For deployed systems, track the performance measures listed in 1 TAC §219.22(b)(2): how accurate the system is and how efficiently it operates.[6]

Report the indicators quarterly, an interval consistent with the reporting cadence in the Texas Responsible AI Governance Act sandbox program, which covers performance metrics, risk mitigation updates, and stakeholder feedback.[7] Because a new process has no history, the first 6 months establish the baseline; numeric targets for each indicator are set at the 6-month review.

At 6 months, the sponsor leads a review of both the AI systems and the CAIR process, using those indicators plus feedback from reviewers, system owners, and affected users. Update the procedures, triage rules, forms, and training based on what the numbers and the people say. The goal is a repeatable practice in which accessibility, cybersecurity, and AI governance findings reach the same decision, with real authority behind it, before any AI system is approved for use.

Appendix A: Vendor Evidence Checklist

Before reviewing an AI product, ask the vendor for the following items. Ask for more proof when a system is higher risk. Evidence should be recent, generally no more than 12 months old. Organizations should use this checklist as part of the 90-day road map.

- ☐ **Security.** An independent audit report, such as a System and Organization Controls 2 (SOC 2) report or an International Organization for Standardization (ISO) 27001 certificate. These show that an outside auditor checked how the vendor protects data.
- ☐ **Accessibility.** A report showing how well the product works for people with disabilities. Vendors usually provide this using the Voluntary Product Accessibility Template; the completed version is called an Accessibility Conformance Report.
- ☐ **Data use.** A plain description of what data the product collects, where it is stored, who can see it, and whether your data are used to train the vendor's AI.
- ☐ **Outside AI tools.** A list of any other companies or AI models the product depends on.
- ☐ **Incident notice.** How quickly the vendor will tell you about a security problem.
- ☐ **Texas public agencies.** Confirm that the product is certified under the Texas Risk and Authorization Management Program, the state's security program for cloud services.

Appendix B: Sample CAIR Operating Procedures

How to use this sample

This document shows what the 8-step test might look like when an organization uses it for a real AI request. This example shows organizations how to evaluate a specific tool. Organizations may modify the sample to fit their size, staffing, existing procedures, legal requirements, and operating environment.

Sample organization: North Valley Public Agency
Sample request: The Human Resources Department wants to purchase an AI system that will help screen employment applications.

1. **Intake.** Human Resources submits the proposed AI system through the agency's CAIR intake process. The process owner receives the request, confirms that the required information has been provided, and creates a record for the review.
2. **Triage.** The request is reviewed to determine how much evaluation it needs. Because the proposed system would be used in employment decisions, it is placed on the full evaluation path under the CAIR risk rules.
3. **Reviews.** The same information about the proposed system is provided to the appropriate reviewers. The AI governance reviewer examines how the system will be used and overseen. The cybersecurity reviewer examines security, data protection, access, and vendor risk. The accessibility reviewer examines whether people with disabilities can use the system and complete the tasks required of applicants. Other departments participate when required by the organization's CAIR Implementation Charter.
4. **Combined findings.** The reviewers complete their reviews and send their findings to the process owner. The process owner brings the findings together into 1 summary. The summary identifies concerns, required changes, remaining risks, and any areas where the reviewers disagree.

Sample conflict resolution

During the review, the cybersecurity reviewer recommends a security setting that prevents some assistive technology from working correctly. The accessibility reviewer identifies the setting as a barrier for applicants who use that technology.

The 2 reviewers work together to identify another option that protects the system while keeping it accessible. If they find an acceptable solution, the solution is recorded in the combined findings and the review continues.

If they cannot resolve the disagreement within the time established by CAIR, the process owner documents both positions and their impacts, then sends the issue to the decision maker identified in the organization's approval chart. The decision and the reason for it are recorded. *This example uses the conflict resolution procedure already established in the CAIR Playbook.*

5. **Decision.** The decisionmaker reviews the combined findings. In this sample, the system is approved with conditions. Human Resources may move forward only after the identified accessibility issue is corrected and the required condition is verified.
6. **Check conditions.** Before the system is used, the appropriate reviewer confirms that the required correction has been made. The system does not move forward until the condition attached to the approval has been satisfied.
7. **Record and share.** The process owner saves the request, supporting evidence, review findings, conflict resolution record, final decision, and confirmation that the required condition was completed. Human Resources and the other appropriate parties are notified of the final decision.
8. **Monitor.** An owner is assigned to monitor the system after it is put into use. The monitoring schedule is recorded with the decision. The system is reviewed again when required by the CAIR Playbook, including when a major change occurs or when a new issue is identified. High risk systems are reviewed at least once each year.

Appendix C: Sample Conflict Resolution Procedure

About this sample: This is a sample conflict resolution procedure. Organizations may use it as written, adapt it to fit their own structure and timelines, or use it as a reference while writing their own. The roles, deadlines, and recordkeeping steps should match your organization's CAIR Implementation Charter and operating procedures, and the people named below should be identified.

When to Use This Procedure

A conflict exists when 2 or more reviewers reach findings that cannot all be met as written. The most common example is a security setting that blocks assistive technology. When more than 2 reviewers are involved, every reviewer whose requirement is affected takes part in all the steps below. A reviewer disagreeing with a decision after it is made is not a conflict; that goes through the normal decision process instead.

Most conflicts end at step 7, when the reviewers agree on a solution. Steps 5, 6, 8, 9, and 11 apply only when something does not go as expected.

Who Does What

- **Reviewers** (AI governance, cybersecurity, accessibility, and any other reviewer named in your charter, such as legal, procurement, IT, or operations) raise conflicts and work to solve them.
- **Process owner** logs conflicts, tracks the deadline, and escalates when needed.
- **Change liaison**, the person named in your charter to coordinate changes with system owners and vendors, helps find workable alternatives.
- **Decisionmaker** named in the approval chart (the signed chart showing who can approve a system, require fixes, delay it, or reject it) settles anything the reviewers cannot. In some organizations the charter assigns dispute resolution to the executive sponsor; if so, that is the same role.

Steps

1. **Name the conflict.** Any reviewer who finds that their requirement cannot coexist with another's tells the process owner in writing. State the requirement, the competing requirement, and who is affected. Save it in the system's decision record, the file holding that system's forms, findings, and decision.

2. **Log it and start the clock.** The process owner logs every reported conflict on the day it is reported and records that date. Reviewers have 10 business days from that date to agree. Do not wait to confirm the conflict is real; if the reviewers settle it the next day, close it as resolved on day 1.
3. **Meet jointly.** All reviewers whose requirements are affected meet together, not by passing messages through the process owner. Each explains what their requirement protects and what happens if it is not met.
4. **Look for an option that meets every requirement.** The goal is a solution that is secure and accessible, not a trade of 1 requirement for another. Bring in the system owner, the vendor, or the change liaison if they can offer alternatives.
5. **Ask the vendor early if a vendor change is needed.** Send the request as soon as a vendor fix looks possible and tell the process owner. If the vendor has not answered 2 business days before the deadline, move to escalation with the request still open and note it as pending.
6. **Extend only once, in writing.** If the reviewers are close to agreement when the deadline arrives, the process owner may grant 1 extension of up to 5 business days. Record the reason and the new date. There is no second extension.
7. **If the reviewers agree, write it down.** Record the agreed solution, who is responsible for carrying it out, and the deadline. It becomes a condition attached to the decision.
8. **If they do not agree by the deadline, escalate.** The process owner sends the decisionmaker every position in full, what each requirement protects, the effect of overruling each requirement, what was already tried, any partial agreement, and anything still pending from a vendor. Other reviews continue while this happens; a conflict pauses the decision, not the whole evaluation.
9. **The decisionmaker decides within 5 business days.** They choose 1 position, or another option, and state the reasons in writing. If a requirement is set aside, record the risk that remains and the name of the person accepting it. Accessibility requirements are not set aside informally; as with any other requirement, this is a recorded decision with a named person accepting the risk.
10. **Record and share.** The conflict, what was tried, the outcome, and the reasons go in the system's decision record. Tell everyone involved, including anyone affected by the outcome.
11. **Reopen if the agreed solution fails.** If the solution cannot be carried out as written, the reviewer or system owner who finds this tells the process owner, and the conflict is reopened at step 2 with a new date. A solution that fails does not become a quiet exception.

12. **Carry the outcome forward.** No system passes its checkpoint with an open conflict. If the resolution sets a requirement aside, add the remaining risk to the system's monitoring schedule so it is reviewed again rather than forgotten. Conditions created by the resolution are confirmed before the system goes live.

Deadlines and Turnaround Time

The 10 business days above is the default for full evaluations. Fast track reviews are expected to finish in 5–10 business days, so a 10-day conflict clock can outlast the entire review. Set a shorter deadline for fast track conflicts, along with a shorter extension and escalation window, and write them into your operating procedures.

A conflict can also push an evaluation past its expected turnaround time. When that happens, the process owner records the new expected date and tells the system owner. The evaluation is not late without explanation; it is a conflict being worked through.

Track These 5 Numbers

Section 7 already asks you to track conflicts resolved. These five numbers break that down. A conflict counts as resolved when it is closed by any route, whether the reviewers agreed or the decision maker decided. Report these with your other indicators and review them at the 6-month review.

1. Conflicts logged.
2. Conflicts resolved by the reviewers, and how many needed an extension.
3. Conflicts escalated to the decisionmaker.
4. Conflicts still open at the 6-month review, and how long each has been open.
5. Conflicts that ended with a requirement set aside, and whether it came from AI governance, cybersecurity, or accessibility.

If no conflicts were logged in 6 months, look into why. It may mean reviews are running smoothly, or that reviewers are settling disagreements informally without a record.

Every conflict should receive a resolution. Nothing should be dropped because reviewers cannot agree.

Endnotes

1. 1 Texas Administrative Code, Chapter 219, Artificial Intelligence, adopted March 2026 pursuant to Senate Bill 1964, §219.22(c), Texas Register, accessed August 13, 2026, https://www.sos.state.tx.us/texreg/archive/March132026/Adopted%20Rules/1.ADMINISTRATION.html.
2. See 1 Texas Administrative Code Chapter 219, supra note 1, at §219.21(b).
3. Texas Legislature, Senate Bill 1964, 89th Legislature, Regular Session (2025), accessed August 13, 2026, https://capitol.texas.gov/tlodocs/89R/billtext/html/SB01964F.htm.
4. *See* 1 Texas Administrative Code Chapter 219, supra note 1.
5. See 1 Texas Administrative Code Chapter 219, supra note 1, at §219.23. Section 219.23 was adopted without changes to the proposed text published in the Texas Register on November 7, 2025 (50 TexReg 7167), https://www.sos.state.tx.us/texreg/archive/November72025/Proposed%20Rules/1.ADMINISTRATION.html.
6. See 1 Texas Administrative Code Chapter 219, supra note 1, at §219.22(b)(2).
7. Chambers and Partners, "Artificial Intelligence 2026 — USA: Texas, Trends and Developments," Chambers Practice Guides, May 2026, accessed August 13, 2026, https://practiceguides.chambers.com/practice-guides/artificial-intelligence-2026/usa-texas/trends-and-developments.

If you'd like to learn more, see the full project, including a policy brief explaining the Fellow's core recommendations, at aspenpolicyacademy.org/project/texas-ai-evaluation-2026.

ASPEN POLICY ACADEMY
aspen institute

aspen institute

About the Aspen Policy Academy

The Aspen Institute's Policy Academy helps community leaders and experts across the political spectrum elevate their voices, influence key decisions, and strengthen democracy from the ground up. Our innovative training programs and resources equip people across sectors – from tech to the environment, science to civic engagement – with the skills to shape critical policy efforts. Learn more at aspenpolicyacademy.org.

Header photo by Luke Jones via Unsplash