

This document was translated from English by machine and may contain mistakes. The English original is at <https://www.novaracg.com/2026/08/30/the-procurement-file-is-the-governance-system/>.

采购档案就是治理体系

Heather Grizzle · August 30, 2026

This article argues that AI governance becomes real only in the procurement file, where institutions must document evidence justifying deployment decisions affecting disabled people.

1. 目录

1. 执行摘要
2. 治理最终必须触及交易本身
3. 作为问责工具的采购档案
4. 1. 预期用途与禁止用途
5. 2. 受影响人群分析
6. 3. 供应商声明记录
7. 4. 独立保障
8. 5. Failure and Fallback Architecture
9. 6. Performance Boundaries and Known Unknowns
10. 7. Logging, Traceability, and Reconstruction
11. 8. Complaint, Contestability, and Redress
12. 9. Model Change and Revalidation
13. 10. Suspension and Exit Authority
14. From AI Policy to Institutional Evidence
15. NCG政策立场
16. Closing Position

作者：Heather Grizzle, Novara Consulting Group



2. 执行摘要

人工智能治理越来越多地通过政策、委员会、原则、清单和风险分类来体现。这些结构固然重要。但当一家公共机构真正采购并部署一套人工智能系统时，治理最终必须变成远没那么抽象的东西。它必须变成一份记录。

Someone has to describe what the system is allowed to do. Someone has to decide what evidence is sufficient to support the vendor's claims. Someone has to identify the people who may be harmed when the system fails. Someone has to determine which failures require human intervention, which changes require reevaluation, and which conditions require the system to be suspended. If those decisions are not documented before deployment, an AI governance policy does not cure the omission. The procurement file is where institutional principles become operational commitments.

摘要

对于影响残障人士的人工智能系统而言，采购档案应当包含足够的证据，以便在出现问题之后能够回答一个基本问题：机构有何合理依据相信该系统适用于这一用途、这一人群和这些条件？如果无法从记录中还原出这一答案，那么在系统上线之前，治理体系就已经是不完整的。

3. 治理最终必须触及交易本身

备用机制只有在需要的人真正能够使用它时，才称得上是一种保障。

Heather Grizzle

Organizations are building increasingly sophisticated AI governance structures. They establish responsible AI principles, create review committees, maintain inventories, and classify systems according to risk. They adopt policies requiring fairness, transparency, accountability, privacy, accessibility, and human oversight. Then procurement begins. A vendor responds to a solicitation. Product demonstrations are scheduled. Accessibility



documentation is collected. Security questionnaires are completed. Legal terms are negotiated. Business owners describe the efficiencies they expect. The technology clears the institution's established gates and enters service.

这些关卡的存在可以带来相当程度的机构信心，但信心并不等同于一项站得住脚的决定。关键的治理问题不仅仅在于该系统是否通过了必要的流程，而在于由此形成的记录中是否包含足以证明所批准的具体部署合理性的证据。

That distinction becomes especially important when AI mediates access for disabled people. A system may summarize information, communicate with patients, evaluate applicants, translate language, generate instructional material, prioritize cases, assist employees, authenticate users, answer questions, or, increasingly, act on behalf of an institution. In each case, accessibility is not simply a characteristic of the interface. It is part of the decision architecture. A disabled person may encounter a system differently from the population on which it was primarily designed, tested, or validated, and an accessibility failure may alter the information that person receives, the choices available to them, their ability to respond, or the institution's interpretation of their behavior. The procurement record therefore needs to establish more than whether accessibility was considered. It needs to establish what was considered, what was tested, what remains unknown, and what the institution decided to do about the uncertainty.

作为问责工具的采购档案

4. 作为问责工具的采购档案

Procurement files are often understood primarily as administrative records. For AI, they should increasingly be understood as governance instruments. A mature AI procurement record should allow an independent reviewer to reconstruct the institution's reasoning without relying on the institutional memory of the people who participated in the purchase. That means the record should answer several questions:

1. 该系统被购买的确切目的是什么？
2. 它被明确禁止做什么？
3. 预期哪些人群会接触到它？



4. 在批准过程中所依赖的各项声明，有什么证据支持？这些证据由谁产生？
5. 已知哪些局限性？还有哪些局限性仍属未知？
6. 当系统出现不确定或错误时会发生什么？
7. 谁保留着推翻其结果的权力？
8. 受影响的人如何能够对其输出结果提出质疑？
9. 什么情况会促使机构重新考虑该部署？
10. 谁拥有叫停它的权力？

这些不是故障发生后事故调查时才需要提出的问题，而是采购环节就应回答的问题。

1. 预期用途与禁止用途

5. 1. 预期用途与禁止用途

第一项要求看似简单：明确机构究竟购买了什么。人工智能系统常常是通过宽泛的功能描述来采购的。系统可能被描述为助手、翻译工具、无障碍工具、决策支持系统、聊天机器人、代理、筛查工具或生产力平台。这些标签作为治理规范是不充分的。采购记录应当明确该系统的实际机构职能。

用于帮助某人浏览网站的通讯工具，其风险与用于医疗接诊环节的同一技术不同。用于生成会议记录的自动转录系统，其风险与用于形成纪律处分程序正式记录的同一系统不同。个人出于试验性目的使用的手语识别系统，与机构将其作为另一种沟通可及方式之替代品来呈现的同一系统，二者并不等同。因此，同一项技术在底层模型未发生任何变化的情况下，也可能在不同风险类别之间转移，原因在于部署场景发生了变化。

在便利抹去边界之前先划定边界

采购档案应当同时说明预期用途和禁止用途。若缺少后者，机构就会产生可预见的范围扩张：一款为有限用途而获批的工具变得可用，员工发现了额外的应用方式，机构的使用范围便逐渐超出了最初获批所依据的证据。

2. 受影响人群分析



6.2. 受影响人群分析

传统技术采购问的是谁将使用该系统。人工智能治理还必须追问谁将受其影响，而这两类人群未必相同。员工可能操作某一人工智能系统，而承受其后果的却是患者、学生、申请人、居民、客户或福利领取者。残障人士往往特别难以通过常规的用户分析被识别出来，因为残障状况改变的往往是通过系统的路径，而非名义上的用户类别。

The procurement record should therefore identify foreseeable accessibility interactions. Does the system process speech? Does it generate or interpret language? Does it depend on vision, hearing, dexterity, cognition, timing, biometric characteristics, or a particular mode of communication? Does it infer intent or competence from behavior that disability may affect? Does an inaccessible output alter a person's ability to participate in a subsequent decision? These questions convert accessibility from a compliance artifact into a system-risk inquiry.

3. 供应商声明记录

7.3. 供应商声明记录

Every consequential vendor claim relied upon during procurement should have an evidentiary status. Not every claim requires independent testing, but institutions should distinguish among at least three categories. A capability is claimed when the vendor states that it exists. It is demonstrated when evidence shows that it has been observed under specified conditions. It is established for deployment when evidence reasonably supports reliance on it in the institution's intended context. Those categories are not interchangeable.

一次演示可以证明系统能够产生某种输出结果，但未必能够证明该系统在不同人群、不同环境或不同重大用例下产生该结果的可靠程度。同样，文档可以证明供应商就其系统做出了何种陈述，却不能独立证明该陈述的正确性。采购档案应当保留这一区分，否则，断言仅仅因为在足够多的文件中被反复重申，就会逐渐被当作既定事实。

已确立可供部署

A vendor claim status meaning evidence reasonably supports reliance on the capability in the institution's actual, intended context, not merely that the capability has been observed under demonstration conditions.



4. 独立保障

8. 4. 独立保障

Vendor evidence has a legitimate role in procurement. Vendors know their systems better than purchasers do and should be expected to disclose testing, architecture, limitations, known failure conditions, and relevant performance evidence. But the commercial relationship matters. The party seeking the contract should not be the only party determining whether the evidence is sufficient to award it.

Independent assurance does not mean recreating the vendor's engineering program. It means testing the claims that matter to the purchasing decision under conditions capable of disproving them. For accessibility-related AI, this may require evaluation involving people with the relevant disability and, where linguistic access is involved, qualified members of the language community. The objective is not ceremonial participation. It is evidentiary authority. The people capable of identifying a consequential failure must have a mechanism for causing that failure to affect the procurement decision. Otherwise, participation exists without governance.

5. FAILURE AND FALLBACK ARCHITECTURE

9. 5. Failure and Fallback Architecture

Every AI procurement should contain a written answer to a single question: what happens when the system does not work? "Human in the loop" is not an adequate answer. The record should identify the human, the trigger, the authority, the response time, and the alternative pathway available to the affected person.

For disabled users, the fallback itself must also be accessible. An AI communication system that fails and directs a Deaf person to make a telephone call has not produced a fallback. An automated digital process that becomes inaccessible and requires a blind user to complete the same inaccessible interface has not transferred the person to human oversight in any meaningful sense.

备用机制只有在需要的



人真正能够使用它时，
才称得上是一种保障。

6. PERFORMANCE BOUNDARIES AND KNOWN UNKNOWN

Heather Grizzle

10. 6. Performance Boundaries and Known Unknowns

Procurement documents tend to record what products can do. Governance records also need to state where confidence ends. AI performance is conditional. It may vary according to language, dialect, accent, signing style, lighting, camera position, disability, device, environment, domain terminology, interaction length, demographic characteristics, or countless other variables. Institutions should require vendors to disclose known performance boundaries and should separately document areas that have not been evaluated.

That distinction matters. Not evaluated is not the same finding as failed, but it is also not the same finding as safe. Uncertainty is not a procurement defect if it is recognized and governed. Undocumented uncertainty is.

7. LOGGING, TRACEABILITY, AND RECONSTRUCTION

11. 7. Logging, Traceability, and Reconstruction

When an AI-mediated interaction produces harm, the institution should be able to reconstruct what happened, and that requires decisions about logging before deployment. What system version was operating? What inputs were received? What output was generated? Was the output modified? Did a human review it? What information did that reviewer see? What action followed? Can the institution reproduce the event without retaining data that should never have been retained in the first place?

Traceability and privacy can create legitimate competing requirements. That conflict should be resolved through system design and governance rather than discovered during litigation, an accessibility complaint, or an internal investigation. The procurement file should document the resolution.

8. COMPLAINT, CONTESTABILITY, AND REDRESS



12. 8. Complaint, Contestability, and Redress

A person affected by AI needs more than a mechanism for reporting a technical problem. They may need to contest what the institution did because of the system, and that is a different function. If an AI system mistranslates communication, incorrectly characterizes behavior, produces inaccessible information, generates a false inference, or contributes to an adverse institutional action, the affected person needs a pathway to challenge the resulting decision.

The institution should know before deployment who receives the challenge, who investigates it, what evidence is preserved, whether the contested AI output remains operative during review, what remedies are available, and how quickly the institution must respond.

A FEEDBACK FORM IS NOT A REDRESS MECHANISM

Redress requires an identified recipient, an investigation process, preserved evidence, a decision on whether the contested output stays live during review, defined remedies, and a response deadline.

9. MODEL CHANGE AND REVALIDATION

13. 9. Model Change and Revalidation

AI procurement creates a problem that traditional software contracts were not designed to handle particularly well: the product that was evaluated may not remain the product that is deployed. Models are updated. Guardrails change. Training data changes. Interfaces change. Third-party dependencies change. Vendors replace underlying models. Performance can improve in one domain and degrade in another without the purchasing institution initiating any change itself.

The procurement file therefore needs a change-control rule. The relevant question is not whether the vendor is permitted to update its product. It is which changes invalidate the evidence on which the institution relied. Contracts should identify material changes requiring notice, reevaluation, renewed acceptance testing, or approval before continued use in specified contexts. Otherwise, an institution can perform rigorous assurance at acquisition



and still find itself governing a materially different system six months later using evidence produced for the previous one.

10. SUSPENSION AND EXIT AUTHORITY

14. 10. Suspension and Exit Authority

Governance without stop authority is advisory. Someone within the institution must have the authority to restrict, suspend, or terminate an AI deployment when evidence no longer supports its use, and the triggering conditions should not have to be invented during a crisis.

- ☐ Repeated accessibility failures
- ☐ Undisclosed material model changes
- ☐ Loss of required human oversight
- ☐ Significant divergence from validated performance
- ☐ Unresolved complaints
- ☐ New evidence of population-specific harm
- ☐ Failure to provide contractually required information
- ☐ Expansion beyond the approved use case

The procurement record should identify both the triggers and the decision authority.

It should also address exit. Who owns or receives institutional data when the relationship ends? What records must be retained? What must be deleted? How does the institution restore the previous service pathway? What happens to people who have become dependent on the AI-mediated process? Exit planning is not merely vendor management. It is continuity-of-access planning.

FROM AI POLICY TO INSTITUTIONAL EVIDENCE



15. From AI Policy to Institutional Evidence

The emerging challenge for AI governance is not a shortage of principles. It is translation. Fairness has to become an evaluation criterion. Transparency has to become a disclosure requirement. Human oversight has to become an assigned authority. Accessibility has to become a deployment condition. Accountability has to become a named office and a documented remedy. Monitoring has to become a trigger for action. And responsible AI eventually has to become something a procurement officer can place in a file.

This is particularly important in public institutions because procurement is where abstract institutional commitments encounter money, contracts, vendors, statutory duties, and people who cannot simply choose another government, school, hospital, court, or public service when the technology does not work for them. The procurement file therefore performs a function much larger than recordkeeping. It establishes the institution's theory of acceptable risk.

NCG政策立场

16. NCG政策立场

Novara Consulting Group holds that AI systems affecting disabled people should not be approved solely because they have satisfied an organization's general AI governance process. The procurement record should contain sufficient evidence to reconstruct and defend the specific deployment decision.



AT MINIMUM, THE RECORD SHOULD ESTABLISH

- The intended and prohibited uses of the system
- The populations foreseeably affected
- The evidentiary status of consequential vendor claims
- The basis for independent assurance where warranted
- Known failure conditions and untested conditions
- Accessible fallback and human-review pathways
- Logging and traceability requirements
- Complaint, contestability, and redress procedures
- Material-change and revalidation triggers
- Institutional authority to restrict, suspend, or terminate deployment

The standard is not perfect knowledge. No procurement process can eliminate uncertainty. The standard is governed uncertainty: knowing what has been established, what has not, what evidence justified proceeding anyway, and who bears responsibility for the decision.

CLOSING POSITION

17. Closing Position

After an AI failure, institutions often ask whether the vendor should have warned them. Sometimes the answer will be yes. But public accountability requires another question: what evidence did the institution require before it agreed to proceed? That question cannot be outsourced. The vendor can supply evidence. An assessor can evaluate it. A committee can advise. Disabled stakeholders can identify failures that others cannot see. Lawyers can negotiate the allocation of contractual risk. The institution still makes the decision, and its procurement record should prove that it knew what decision it was making.

An AI system is not
governed because an

The procurement file is where that accountability
begins.



organization has an AI policy. It is governed when the institution can show why this system, for this purpose, affecting these people, under these conditions, was permitted to operate.

Heather Grizzle

18. 引用方式

Grizzle, H. M. (2026, August 30). 采购档案就是治理体系. Novara Consulting Group. <https://www.novaracg.com/zh/2026/08/30/the-procurement-file-is-the-governance-system/>

