This document was translated from English by machine and may contain mistakes. The English original is at https://www.novaracg.com/2026/02/26/when-small-system-flaws-become-global-liabilities/.

Informationsarchitektur ist die neue Grenze der Governance: Warum organisatorische Transparenz von verteidigungsfähigen Informationssystemen abhängt

Heather Grizzle · February 26, 2026

Most organizations do not have a scandal problem. They have an information architecture problem, and AI has made it visible.

Inhalt

1. Governance-Versagen beginnt lange, bevor es öffentlich wird
2. Informationsarchitektur ist zur Governance-Infrastruktur geworden
3. Künstliche Intelligenz hat ein bestehendes Governance-Problem offengelegt
4. Governance-Resilienz ist eine architektonische Fähigkeit
5. Institutionen aufbauen, die einer Offenlegung standhalten können

Die zentrale Governance-Herausforderung des Jahres 2026 ist nicht die Transparenz selbst. Transparenz ist schlicht die Bedingung, unter der Organisationen heute agieren. Die folgenreichere Frage ist, ob Institutionen über Informationssysteme verfügen, die einer anhaltenden Prüfung standhalten können. Governance wird zunehmend nicht daran gemessen, was eine Organisation über sich selbst aussagt, sondern daran, ob ihre Informationen diese Darstellungen bei regulatorischer Prüfung, Rechtsstreitigkeiten, Vergabeprüfungen, investigativem Journalismus oder öffentlichen Untersuchungen belegen können.

Über einen Großteil der vergangenen Jahrzehnte konzentrierten sich Governance-Programme darauf, Richtlinien zu entwickeln, Verfahren zu dokumentieren, Compliance-Rahmenwerke umzusetzen und Aufzeichnungen zu führen, die die Sorgfalt der Organisation belegen sollten. Diese Bemühungen spiegelten ein Governance-Umfeld wider, in dem Dokumentation oft als ausreichender Nachweis dafür galt, dass eine Organisation eine angemessene Aufsicht ausgeübt hatte. Es wurde erwartet, dass Richtlinien existieren. Es wurde erwartet, dass Verfahren schriftlich festgehalten werden. Es wurde erwartet, dass Kontrollen dokumentiert sind. Ob diese Dokumente die betriebliche Realität tatsächlich widerspiegelten, wurde oft erst untersucht, nachdem etwas schiefgelaufen war.

Dieses Umfeld hat sich verändert. Regulierungsbehörden, Gerichte, Prüfer, Versicherer, Aufsichtsgremien, Investoren und zunehmend auch die Öffentlichkeit erwarten von Organisationen heute nicht nur den Nachweis, dass Richtlinien existieren, sondern dass diese Richtlinien im alltäglichen Betrieb tatsächlich so funktionieren, wie dargestellt. Dokumentation ist zum Ausgangspunkt der Governance geworden, nicht mehr zu deren Abschluss. Institutionelle Glaubwürdigkeit hängt heute von der Qualität, Integrität und Nachvollziehbarkeit der Informationen ab, die organisatorische Entscheidungen stützen.

Die praktische Konsequenz ist erheblich. Die zentrale Governance-Frage lautet nicht mehr: „Haben Sie eine Richtlinie?“ Sie lautet nun: „Kann Ihre Organisation anhand belastbarer Informationen nachweisen, dass die Richtlinie wie beabsichtigt funktioniert?“ Das sind grundlegend unterschiedliche Fragen. Die erste bewertet Dokumentation. Die zweite bewertet die Architektur, die institutionelles Wissen erzeugt, verwaltet und bewahrt.

Governance-Versagen beginnt lange, bevor es öffentlich wird

Governance-Versagen wird oft als isolierter Skandal beschrieben. Die öffentliche Diskussion konzentriert sich häufig auf eine bestimmte Offenlegung, einen Cybersicherheitsvorfall, ein unsachgemäß veröffentlichtes Dokument oder einen behördlichen Befund, wodurch der Eindruck entsteht, ein einzelnes Ereignis habe das institutionelle Versagen ausgelöst. Nachfolgende Untersuchungen stützen diese Interpretation nur selten.

Häufiger stellen hochgradig sichtbare Versagensfälle den Punkt dar, an dem sich über Jahre angesammelte Governance-Schwächen schließlich nicht mehr ignorieren lassen. Die Öffentlichkeit sieht das offengelegte Dokument. Regulierungsbehörden prüfen die Aufzeichnungen, die es hervorgebracht haben. Interne Ermittler entdecken widersprüchliche Klassifizierungen, fragmentierte Dateneigentümerschaft, undokumentierte Änderungen an Arbeitsabläufen, widersprüchliche Aufbewahrungspraktiken und Entscheidungshistorien, die sich nicht mehr mit Sicherheit rekonstruieren lassen. Was wie ein isolierter Vorfall erscheint, ist häufig das erste sichtbare Symptom eines weitaus tieferen strukturellen Zustands.

Die Beispiele variieren je nach Branche, doch das zugrunde liegende Muster bleibt bemerkenswert konstant. Ein Dokument wird veröffentlicht, ohne dass sensible Informationen geschwärzt wurden. Eine Programmierschnittstelle gibt Informationen über den vorgesehenen Adressatenkreis hinaus preis. Interne Berichte widersprechen Aussagen in öffentlichen Offenlegungen. Lieferantenangaben lassen sich nicht mit operativen Nachweisen in Einklang bringen. Systeme künstlicher Intelligenz erzeugen Empfehlungen, die sich nicht auf validierte Quellinformationen zurückführen lassen. Obwohl diese Ereignisse unzusammenhängend erscheinen, spiegelt jedes von ihnen dieselbe institutionelle Schwäche wider. Die Organisation hat das Vertrauen in ihre eigenen Informationen verloren.

Die Organisation hat das Vertrauen in ihre eigenen Informationen verloren.

Dieser Vertrauensverlust entsteht selten dadurch, dass ein einzelner Mitarbeiter ein Verfahren nicht befolgt hat. Vielmehr entwickelt er sich allmählich, während Organisationen expandieren, neue Technologien einführen, Abteilungen zusammenlegen, Betriebsabläufe auslagern und neue Governance-Anforderungen auf Informationssysteme aufsetzen, die ursprünglich für völlig andere Zwecke konzipiert wurden. Klassifizierungsstandards entwickeln sich ungleichmäßig. Verantwortung verteilt sich auf mehrere Geschäftsbereiche. Altanwendungen laufen weiter neben modernen Plattformen. Manuelle Behelfslösungen ersetzen nach und nach formale Prozesse. Mit der Zeit bewegen sich Informationen zwar weiterhin durch die gesamte Organisation, doch immer weniger Menschen können mit Sicherheit erklären, wie sie sich bewegen, warum sie sich verändern oder wer letztlich die Befugnis über sie ausübt.

Organisationen entdecken diese Zustände häufig erst, wenn Informationen einer externen Prüfung standhalten müssen. Zu diesem Zeitpunkt bietet die Korrektur eines einzelnen Dokuments nur wenig Beruhigung, da sich die Frage verschoben hat: von der Frage, ob ein einzelner Fehler vorlag, hin zur Frage, ob ähnliche Schwächen in der gesamten Institution bestehen.

Informationsarchitektur ist zur Governance-Infrastruktur geworden

Informationsarchitektur wurde traditionell als technische Disziplin verstanden, die für die Organisation von Informationen, die Strukturierung von Repositorien und die Verbesserung der Zugänglichkeit zuständig ist. Diese Funktionen bleiben zwar wichtig, erfassen jedoch nicht mehr ihre institutionelle Bedeutung. Informationsarchitektur ist zur Governance-Infrastruktur geworden, weil jede folgenreiche organisatorische Entscheidung letztlich davon abhängt, dass Informationen korrekt durch komplexe Systeme der Erfassung, Klassifizierung, Speicherung, Autorisierung, Abfrage und Kommunikation fließen.

Führungsentscheidungen stützen sich auf Informationen, die bereits zahlreiche technische und menschliche Prozesse durchlaufen haben, bevor sie die Leitungsebene erreichen. Behördliche Einreichungen beruhen auf operativen Aufzeichnungen, die über mehrere Abteilungen hinweg erfasst wurden. Personalentscheidungen beziehen Personalakten, Richtlinienvorgaben, rechtliche Anforderungen, Dokumentation von Anpassungen und zunehmend algorithmische Empfehlungen ein. Beschaffungsentscheidungen stützen sich auf Lieferantenangaben, Vertragsdokumentation, Finanzanalysen und technische Bewertungen, die von getrennten organisatorischen Funktionen erstellt werden. Keine dieser Entscheidungen entsteht unabhängig von der Informationsarchitektur. Sie sind deren Produkte.

Folglich kann Governance nicht mehr von den Systemen getrennt werden, die für die Erzeugung institutionellen Wissens verantwortlich sind. Organisationen, die nicht erklären können, wie Informationen entstehen, wie sie sich im Laufe der Zeit verändern, wie konkurrierende Versionen abgeglichen werden, wer Änderungen autorisiert oder wie Aufzeichnungen bewahrt werden, können Governance nicht überzeugend nachweisen – unabhängig davon, wie umfassend ihre schriftlichen Richtlinien erscheinen mögen.

Institutionelles Vertrauen hängt zunehmend von dieser Fähigkeit ab. Stakeholder bewerten nicht nur die Schlussfolgerungen einer Organisation. Sie bewerten die beweismäßigen Grundlagen, auf denen diese Schlussfolgerungen beruhen. Vertrauen entsteht, wenn Institutionen nachweisen können, dass Informationen während ihres gesamten Lebenszyklus vollständig, nachvollziehbar, intern konsistent und unabhängig überprüfbar bleiben. Vertrauen schwindet, wenn Organisationen ihre eigenen Informationen nicht erklären können.

Künstliche Intelligenz hat ein bestehendes Governance-Problem offengelegt

Künstliche Intelligenz hat vergleichsweise wenig an den grundlegenden Verpflichtungen der Governance verändert. Organisationen waren schon immer für die Qualität der Informationen verantwortlich, die folgenreiche Entscheidungen stützen. Was künstliche Intelligenz verändert hat, ist die Geschwindigkeit, der Umfang und die Sichtbarkeit, mit denen sich Schwächen in dieser Informationsarchitektur im gesamten Unternehmen verbreiten.

Informationen, die zuvor eine sequenzielle menschliche Prüfung durchliefen, fließen nun kontinuierlich durch automatisierte Arbeitsabläufe, die innerhalb von Sekunden Zusammenfassungen, Klassifizierungen, Empfehlungen, Prognosen und operative Entscheidungen erzeugen können. Diese Fähigkeiten bieten einen messbaren organisatorischen Nutzen. Sie verstärken jedoch auch Mängel, die zuvor lokal begrenzt blieben.

> **WIE SICH MÄNGEL VERBREITEN**
>
> Mangelhafte Klassifizierungspraktiken werden zu Trainingsdaten. Unvollständige Aufzeichnungen werden zu algorithmischen Eingaben. Widersprüchliche Dokumentation wird zu automatisierter Entscheidungsunterstützung. Schwache Governance-Strukturen werden zu automatisiertem Governance-Versagen.

Künstliche Intelligenz erfindet diese Schwächen nicht. Sie legt sie offen, indem sie die organisatorische Abhängigkeit von Informationen erhöht, deren Integrität möglicherweise nie vollständig geprüft wurde. Systeme, die zur Beschleunigung der Entschei-

dungsfindung konzipiert wurden, verstärken zwangsläufig sowohl die Stärken als auch die Schwächen der Informationen, die diesen Entscheidungen zugrunde liegen.

Diese Unterscheidung ist wichtig, weil viele Organisationen KI-Governance so angehen, als handle es sich um eine völlig neue Compliance-Verpflichtung. Tatsächlich beginnt verantwortungsvolle KI-Governance mit verantwortungsvoller Informations-Governance. Fragen zu Erklärbarkeit, Rechenschaftspflicht, Transparenz, Verzerrung, Validierung und menschlicher Aufsicht lassen sich nicht unabhängig von der Informationsarchitektur beantworten, aus der KI-Systeme lernen und auf deren Grundlage sie arbeiten. Bevor Organisationen die Qualität algorithmischer Ergebnisse bewerten, müssen sie bewerten, ob die zugrunde liegenden Informationen institutionelles Vertrauen verdienen. Die Qualität künstlicher Intelligenz kann niemals die Qualität der Governance übertreffen, die den von ihr verarbeiteten Informationen zugrunde liegt.

Governance-Resilienz ist eine architektonische Fähigkeit

Organisationen reagieren auf Informationsversagen häufig mit Sanierungsmaßnahmen. Zusätzliche Richtlinien werden verfasst. Neue Prüfungsausschüsse werden eingerichtet. Technologien werden angeschafft. Pflichtschulungen werden ausgeweitet. Kommunikationsstrategien werden überarbeitet. Diese Maßnahmen adressieren häufig unmittelbare operative Bedenken, lassen jedoch oft die strukturellen Bedingungen, die diesen Bedenken zugrunde liegen, grundlegend unverändert.

Langfristige Resilienz erfordert eine andere Perspektive. Governance sollte nicht als eine Sammlung isolierter Compliance-Aktivitäten verstanden werden, sondern als eine konstruierte institutionelle Fähigkeit, die von einer kohärenten Informationsarchitektur gestützt wird.

Diese Arbeit beginnt mit scheinbar einfachen Fragen:

- Woher stammen die Informationen der Organisation?
- Wer bestimmt, wie sie klassifiziert werden?
- Wie tauschen getrennte Informationssysteme Aufzeichnungen aus?
- Welche Arbeitsabläufe verändern institutionelles Wissen?
- Welche Entscheidungen stützen sich auf diese Aufzeichnungen?
- Kann die Organisation diese Entscheidungen Monate oder Jahre später anhand vollständiger, maßgeblicher Nachweise rekonstruieren, statt sich auf institutionelle Erinnerung zu verlassen?

Diese Fragen bewerten nicht nur das Informationsmanagement. Sie bewerten, ob Governance selbst einer Prüfung standhalten kann.

Organisationen, die diese Fragen beantworten können, besitzen etwas zunehmend Wertvolles. Sie besitzen Governance-Resilienz – die institutionelle Fähigkeit, unter behördlicher, rechtlicher, operativer oder öffentlicher Prüfung nachzuweisen, dass folgenreiche Entscheidungen weiterhin durch vollständige, nachvollziehbare und belastbare Informationen gestützt werden. Governance-Resilienz ist daher kein Ergebnis, das nach einer Krise erreicht wird. Sie ist ein architektonisches Merkmal, das lange vor einer Krise entwickelt wird.

Institutionen aufbauen, die einer Offenlegung standhalten können

Bei Novara Consulting Group verstehen wir Governance als eine Übung in institutionellem Systemdesign und nicht als Dokumentenproduktion. Richtlinien bleiben wichtig, doch Richtlinien allein begründen keine Rechenschaftspflicht. Rechenschaftspflicht entsteht aus Informationsarchitekturen, die nachweisen können, wie institutionelle Entscheidungen getroffen, gestützt, bewertet und über die Zeit bewahrt werden.

Unsere Arbeit konzentriert sich darauf, diese zugrunde liegenden Systeme zu stärken – durch Kartierung der Informationsarchitektur, Datenherkunftsanalyse, Abstimmung von Governance-Kontrollen, Integration von KI-Governance (künstliche Intelligenz), Nachverfolgbarkeitsprotokolle, operative Risikobewertung sowie funktionsübergreifende Koordination zwischen Rechtsabteilung, Compliance, Personalwesen, Informationstechnologie, Betrieb, Unternehmensführung und Risikomanagement. Das Ziel ist nicht nur regulatorische Compliance. Es geht darum, Organisationen dabei zu helfen, Governance-Systeme zu entwickeln, die institutionelles Vertrauen unter Bedingungen fortwährender Prüfung aufrechterhalten können.

Keine Organisation kann jede Untersuchung, jede Prüfung, jede Offenlegungsanfrage oder jede rechtliche Auseinandersetzung verhindern. Ebenso wenig kann eine Institution jeden technologischen Wandel vorhersehen, der ihr Informationsumfeld umgestalten wird. Organisationen können jedoch bestimmen, ob die Systeme, die ihre Entscheidungen stützen, bewusst so konstruiert wurden, dass sie bei Prüfung durch Dritte kohärent, transparent und belastbar bleiben.

Diese Unterscheidung trennt zunehmend resiliente Institutionen von anfälligen. Die Organisationen, die im kommenden Jahrzehnt führend sein werden, sind nicht zwangsläufig jene mit den wenigsten Governance-Herausforderungen. Es werden jene sein, deren Informationsarchitekturen es ermöglichen, diese Herausforderungen mit Zuversicht zu untersuchen, zu verstehen und zu lösen, weil die zugrunde liegenden Nachweise vollständig, vertrauenswürdig und intakt bleiben.

Governance wird nicht mehr daran gemessen, welche Richtlinien eine Organisation veröffentlicht. Sie wird daran gemessen, ob die Institution durch die Architektur ihrer eigenen Informationen belegen kann, dass diese Richtlinien die in der Praxis getroffenen Entscheidungen tatsächlich bestimmen.

> **TIPS**
>
> Know something about a sign language AI system that the public should know? Send it to tips@novaracg.com. Every tip is read by me and kept confidential. If you work in the UK, writing to us is not by itself a protected disclosure under the Public Interest Disclosure Act 1998, so before you share employer information, check your options with Protect (protect-advice.org.uk), the free whistleblowing advice line.

Zitierweise

Grizzle, H. M. (2026, February 26). Informationsarchitektur ist die neue Grenze der Governance: Warum organisatorische Transparenz von verteidigungsfähigen Informationssystemen abhängt. Novara Consulting Group. https://www.novaracg.com/de/2026/02/26/when-small-system-flaws-become-global-liabilities/