The Incomplete Ledger

Security sieht die Schuld. Privacy und AI zahlen sie.

Bettina Sterner, BA
kaffeekipferl.at
30. April 2026

Die in diesem Whitepaper enthaltenen Ausführungen, Analysen und Schlussfolgerungen spiegeln ausschließlich die persönliche fachliche Einschätzung der Autorin zum Zeitpunkt der Veröffentlichung wider. Sie sind unabhängig entstanden und stehen in keinem Zusammenhang mit aktuellen oder früheren Arbeitgebern, Auftraggebern, Mandanten oder sonstigen Organisationen, denen die Autorin angehört oder angehört hat. Das Whitepaper ersetzt keine rechtliche oder regulatorische Beratung im Einzelfall.

Abstract

Deutsch — Organisationen akkumulieren Governance-Schulden in drei Domänen gleichzeitig: Security, Privacy und AI. Sie behandeln diese Schulden als drei separate Probleme mit drei separaten Zuständigkeiten — und erzeugen damit systematisch blinde Flecken, die kein Einzelframework schließen kann. Dieses Paper nimmt den Security Debt Index von ISACA als Ausgangspunkt, benennt seine methodischen Schwächen und seinen zu engen Scope, und entwickelt daraus ein erweitertes Konzept: den Blind Spot Debt. Es beschreibt, wie Security Debt, Privacy Debt und AI Debt entstehen, wie sie sich gegenseitig verstärken und warum integrierte Governance keine Option, sondern eine Notwendigkeit ist. Mit dem Blind Spot Debt Index (BSDI) wird ein operationalisierbares Messinstrument vorgestellt — mit definierten Indikatoren, klaren Messmethoden und einer Eskalationsskala, die dort beginnt, wo Handeln noch möglich ist, und dort endet, wo Governance als zahnloser Papiertiger entlarvt wird. Das Paper schließt mit einem Ausblick auf AI Agents, regulatorische Verdichtung und die Frage, wie das Three Lines of Defence-Modell nach DORA konsequent auf alle drei Domänen angewendet werden kann — auch dort, wo kein Regulator explizit hinschaut.

English — Organizations accumulate governance debt across three domains simultaneously — security, privacy, and AI — while treating them as three separate problems with three separate owners. The result is a systematic architecture of blind spots that no single-domain framework can address. This paper takes ISACA's Security Debt Index as its starting point, identifies its methodological weaknesses and narrow scope, and develops an expanded concept: Blind Spot Debt. It describes how security debt, privacy debt, and AI debt emerge, how they amplify each other, and why integrated governance is not an option but a necessity. The Blind Spot Debt Index (BSDI) introduced here is a fully operationalized measurement instrument — with defined indicators, concrete measurement methods, and an escalation scale that begins where action is still possible and ends where governance is exposed as a paper tiger with no teeth. The paper concludes with a forward-looking perspective on AI agents, regulatory convergence, and the question of how the Three Lines of Defence model under DORA can be applied consistently across all three domains — including where no regulator is explicitly watching.

Security Debt — ein unvollendetes Konzept

ISACA hat im Frühjahr 2026 etwas sehr Richtiges getan: Das Konzept des **Technical Debt** aus der Softwareentwicklung in die Governance-Welt übertragen. Die Grundidee ist überzeugend — aufgeschobene Sicherheitsentscheidungen akkumulieren Risiko, das sich mit der Zeit verzinst, bis es irgendwann sichtbar wird. Meist dann, wenn es zu spät ist.

Der Ansatz ist richtig — und er öffnet eine Tür, die das Paper selbst nicht weit genug aufstößt. Wer hindurchgeht und fragt, wie dieses Konzept in der Praxis funktionieren soll, findet: Methodische Unschärfen, eine Formel ohne Kalibrierung und einen Scope, der die komplexesten Governance-Domänen außen vor lässt.

Eine Formel ohne Fundament

Das Paper schlägt einen Security Debt Index vor — kurz SDI. Die Berechnungslogik klingt zunächst solide: Severity (Schweregrad) multipliziert mit Duration (Bestandsdauer) und Velocity (Wachstumsgeschwindigkeit), dividiert durch einen – nicht näher definierten – Anpassungsfaktor. Das Ergebnis liefert einen Score zwischen 0 und 100, aufgeteilt in vier Zonen: „Controlled", „Rising", „Escalating" und „Critical".

Klingt präzise. Ist es nicht.

Denn das Paper lässt konsequent offen, wie Severity konkret gemessen wird, wie Duration berechnet wird, was Velocity in der Praxis bedeutet und was unter dem Begriff „Anpassungs- oder Normalisierungsfaktor" zu verstehen ist. Der einzige Hinweis auf Methodik: Die Organisation solle das intern klären — etwa durch Workshops. Älteren Verfahren wie OCTAVE, die für deutlich engere Anwendungsfälle konzipiert wurden, gelingt es trotzdem, mehr Struktur für die Eigenarbeit mitzuliefern. Das ist kein Vorwurf — aber es ist ein Maßstab.

Ein Messinstrument, das seine eigene Kalibrierung nicht mitliefert, ist kein Messinstrument. Es ist eine Metapher mit Gleichheitszeichen. Für Kommunikationszwecke in Richtung Management mag das ausreichen. Als Steuerungsinstrument für Organisationen, die tatsächlich verstehen wollen, wo sie stehen, reicht es nicht.

Eine Skala, die genau dort endet, wo sie anfangen sollte

Noch gravierender als die methodischen Lücken in der Formel ist, was die Skala mit ihrem höchsten Eskalationsgrad macht — oder eben nicht macht. Für „Controlled", „Rising" und „Escalating" liefert das Paper zumindest eine Lagebeschreibung. Bei „Critical" — dem Punkt, an dem Debt laut SDI sein maximales Schadenspotenzial erreicht — lautet die Handlungsempfehlung sinngemäß: Ein vollständiger Systemneustart sei notwendig.

Was das operativ bedeutet, bleibt vollständig offen. Welche Schritte eine Organisation konkret einleiten soll, wenn sie diesen Score erreicht, wird nicht ausgeführt. Wer die Verantwortung trägt, welche Ressourcen mobilisiert werden müssen, in welcher Reihenfolge gehandelt werden soll — nichts davon findet sich im Text. Ausgerechnet in dem Moment, in dem Orientierung am dringendsten gebraucht wird, endet die Guidance. Das ist nicht nur eine Lücke — es ist eine Kapitulation des Frameworks vor seiner eigenen Relevanz.

Der Abgrund beginnt vor dem Abgrund

Es gibt ein konzeptuelles Problem, das schwerer wiegt als alle methodischen Unschärfen: Die implizite Annahme, dass „Escalating" eine Vorstufe zu „Critical" ist — eine gelbe Ampel vor der roten, eine Warnstufe mit noch vorhandenem Handlungsspielraum.

Das Gegenteil ist richtig.

Wer sich in der Zone „Escalating" befindet, steht bereits am Rand. Debt hat die Agilität der Organisation bereits eingeschränkt, die Organisation hat Handlungsspielraum verloren und Schwachstellen sind exponiert. Die Kosten der Schadensbehebung steigen. Neue Risiken überlagern ungelöste alte. In dieser Situation ist nicht erhöhte Aufmerksamkeit erforderlich die angemessene Reaktion — es ist unmittelbare Intervention. Wer wartet, bis der Score „Critical" erreicht, wartet zu lang. Der freie Fall hat zu diesem Zeitpunkt bereits begonnen.

Wer buchstäblich vor einem Abgrund steht und kurz davor ist, hinunterzufliegen, muss in diesem Moment die Kurve kriegen — nicht beim nächsten Schritt. Ein Framework, das seinen eigenen Eskalationsmechanismus falsch kalibriert, produziert falsche Sicherheit. Und falsche Sicherheit ist teurer als gar keine.

Zu eng gedacht: Der Scope

Neben den methodischen Schwächen liegt ein weiteres, strukturelles Problem vor: Security Debt wird behandelt, als wäre Security die einzige Domäne, in der Organisationen Governance-Schulden anhäufen. Das ist keine böswillige Auslassung — es ist die typische Folge von Fachexpertise ohne integrierten Blick.

Security ist jedoch nicht die komplexeste der betroffenen Domänen. Sie ist die einfachste. Unpatched Systems lassen sich inventarisieren. Vulnerability Scores existieren. Patch-Zyklen sind messbar. Die Domänen, die außen vor bleiben — Privacy und AI — sind strukturell schwerer zu greifen, regulatorisch komplexer verflochten und in ihren Wechselwirkungen mit Security noch kaum systematisch beschrieben.

Das ist die Lücke, die dieses Paper schließt.

Privacy Debt — wenn Compliance aufhört, wo das Dokument endet

Security Debt entsteht, wenn Patches ausbleiben und Systeme veralten. Privacy Debt entsteht leiser — und wird deshalb seltener bemerkt. Kein Alarm schlägt an, wenn ein Auftragsverarbeitungsvertrag (AVV) seit drei Jahren nicht mehr aktualisiert wurde. Kein Monitoring registriert, dass die technischen und organisatorischen Maßnahmen im internen Dokument und die tatsächlich implementierte Systemarchitektur längst auseinanderdriften. Kein Vulnerability Scanner meldet, dass eine DPIA für einen neuen Verarbeitungsvorgang schlicht nie durchgeführt wurde.

Aber es geht noch stiller. In vielen Organisationen existiert kein Datenschutzmanagementsystem — nicht, weil niemand die DSGVO kennt, sondern weil Datenschutz als reaktive Aufgabe verstanden wird: Man beantwortet Betroffenenanfragen, wenn sie kommen. Man dokumentiert, wenn eine Prüfung droht. Risikoeinschätzungen für kritische Verarbeitungen finden nicht statt, weil das Verarbeitungsverzeichnis als bürokratisches Pflichtübel geführt wird — nicht als Steuerungsinstrument. Eine strukturierte Risikoanalyse setzt jedoch voraus, dass man überhaupt weiß, was verarbeitet wird, wo, von wem und auf welcher Rechtsgrundlage. Wer das nicht weiß, muss nichts entscheiden. Unwissenheit ist kein Versagen — sie ist manchmal einfach nur bequem eingerichtet.

Besonders aufschlussreich ist in diesem Zusammenhang ein Befund aus der Bitkom-Studie Datenschutz in der deutschen Wirtschaft aus dem Jahr 2026[1]: 59 Prozent der befragten Unternehmen gaben an, in den vergangenen zwölf Monaten keinen einzigen meldepflichtigen

[1] Bitkom, Datenschutz in der deutschen Wirtschaft, Februar 2026, S. 16, https://www.bitkom.org/sites/main/files/2026-02/bitkom-studienbericht-datenschutz_1.pdf

Datenschutzverstoß erlitten zu haben. Das ist keine Erfolgsgeschichte — **es ist ein Warnsignal.** Denn Datenschutzverstöße passieren. Die plausiblere Erklärung ist nicht, dass sie ausgeblieben sind, sondern dass sie nicht erkannt, nicht als solche eingestuft oder nicht gemeldet wurden. Dass von den Unternehmen, die Verstöße einräumten, immerhin 29 Prozent diese nicht an die zuständige Aufsichtsbehörde meldeten, verstärkt diesen Eindruck. Eine Organisation, die Sicherheitsvorfälle mit datenschutzrechtlicher Relevanz nicht wahrnimmt oder nicht meldet, hat kein Datenschutzproblem weniger — sie hat eines mehr.

Und dann ist da noch der stille Tod: Der Datenschutzbeauftragte (DSB), der keine Fortbildungen macht. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit hält in seinem 53. Tätigkeitsbericht fest, dass die Teilnahme an Schulungen stellenweise unzureichend sei — und empfiehlt, neben einer Grundausbildung vor der Benennung fortwährend mindestens zwei Tage im Jahr für Fortbildungen aufzuwenden, um das erforderliche Fachwissen auf dem notwendigen Niveau zu halten.[2] Wer diese Empfehlung in Fachkreisen erwähnt, erntet kein nachdenkliches Schweigen, sondern Lachen. Dabei ist die Konsequenz ernst: Ein DSB, der mit den aktuellen rechtlichen Entwicklungen nicht à jour ist, kann weder angemessen beraten noch zuverlässig überwachen. Er erkennt nicht, wann eine neue Verarbeitung eine DPIA erfordert. Er bewertet nicht, ob ein Incident meldepflichtig ist. Er sieht nicht, was er nicht weiß. Ein DSB ohne aktuelles Wissen ist kein Schutzschild — **er ist selbst Privacy Debt.**

Was Privacy Debt ist — und was sie von Security Debt unterscheidet

Privacy Debt bezeichnet den akkumulierten Rückstand an datenschutzrechtlichen Pflichten, Dokumentationsanforderungen, Prozessen und Governance-Entscheidungen, der entsteht, wenn Organisationen schneller handeln als ihre Datenschutz-Infrastruktur mitwächst. Der Mechanismus ist derselbe wie bei Security Debt: Kurzfristige Entscheidungen, aufgeschobene Korrekturen, fehlende Verantwortlichkeiten. Das Ergebnis ist dasselbe: Akkumuliertes Risiko, das mit der Zeit teurer wird.

Der entscheidende Unterschied liegt in der Natur des Schadens. Security Debt gefährdet primär die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen. Privacy Debt gefährdet etwas, das sich schlechter reparieren lässt: Das Vertrauen von Menschen.

Und dieser Vertrauensverlust ist im Datenschutzrecht keine abstrakte Größe — er ist rechtlich kodiert. Art. 82 DSGVO räumt betroffenen Personen einen eigenständigen Schadensersatzanspruch ein, wenn ihnen durch eine datenschutzwidrige Verarbeitung ein Schaden entstanden ist. Dieser Schaden muss nicht finanzieller Natur sein — auch immaterieller Schaden ist anspruchsbegründend. Security Debt hat eine Rechnung. Privacy Debt hat viele — und ein paar davon sind adressiert an die Aufsichtsbehörde.

AI Debt — wenn das System lernt, aber niemand hinschaut

Von allen Formen des Governance Debt ist AI Debt die am schwierigsten zu greifende — und die am schnellsten wachsende. Das liegt nicht zwingend daran, dass KI-Systeme besonders komplex wären. Es liegt daran, dass sie auf eine Art veralten, die weder in Compliance-Kalendern noch in Governance-Strukturen auftaucht, die für eine andere Welt gebaut wurden.

Ein KI-Modell, das vor zwei Jahren in Betrieb ging und seither niemanden interessiert hat, gilt intern als erledigt. Es ist keines. Die Daten haben sich verändert. Der Kontext hat sich verändert.

[2]Hessischer Beauftragter für Datenschutz und Informationsfreiheit, 53. Tätigkeitsbericht zum Datenschutz, vorgelegt zum 31. Dezember 2024, S. 79f., https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2025-05/53-tb-online.pdf

Die regulatorischen Anforderungen haben sich verändert. Das Modell läuft trotzdem weiter — einsam, still, unbeobachtet.

Das ist AI Debt in seiner reinsten Form: nicht das, was falsch gebaut wurde — sondern das, was richtig gebaut wurde und trotzdem falsch geworden ist.

Was AI Debt ist — und was sie von den anderen unterscheidet

Security Debt entsteht durch Unterlassen: Ein System wird nicht abgelöst, ein Prozess nicht aktualisiert. Privacy Debt entsteht durch Drift: Dokumentation und Realität entwickeln sich auseinander, ohne dass jemand aktiv etwas falsch macht. AI Debt entsteht durch beides — und durch etwas Drittes, Neues: Durch die strukturelle Eigenschaft von KI-Systemen, dass ihre Qualität, ihre Fairness und ihre Rechtmäßigkeit nicht statisch sind.

Ein KI-Modell kann zum Zeitpunkt seiner Inbetriebnahme alle Anforderungen erfüllen und sechs Monate später keines mehr — ohne dass eine einzige Zeile Code geändert wurde. Die Welt hat sich verändert, das Modell nicht. Dieser Mechanismus ist in keinem der derzeit beschriebenen klassischen Governance-Framework adäquat abgebildet. Und er ist der Grund, warum AI Debt eine eigene Kategorie verdient.

Mit der KI-VO ist ein Rechtsrahmen in Kraft getreten, der KI-Systeme nicht nur zum Zeitpunkt ihrer Markteinführung bewertet, sondern — abhängig von der Risikokategorie — laufende Pflichten für Betreiber und Anbieter begründet. Beispielsweise begründet Art. 26 KI-VO für Betreiber von Hochrisiko-KI-Systemen laufende Pflichten — geeignete technische und organisatorische Maßnahmen, aktives Monitoring des Systemverhaltens und die Pflicht, den Anbieter bei Vorfällen oder Fehlfunktionen zu informieren — die mit dem ersten Tag des Betriebs beginnen. Wer diese Pflichten nicht erfüllt, akkumuliert nicht nur technisches Risiko. Er akkumuliert regulatorisches Haftungsrisiko — still, kontinuierlich — und fällig, sobald jemand unangenehme Fragen stellt.

Wie AI Debt entsteht

KI-Systeme im Einsatz ohne Risikobewertung. In der Praxis werden KI-Tools eingeführt, weil sie ein operatives Problem lösen — schnell, pragmatisch, oft auf Initiative einzelner Fachabteilungen. Die Frage, ob das System unter die KI-VO fällt, welche Risikokategorie es hat und welche Pflichten daraus für den Betreiber folgen, wird nicht gestellt. Nicht weil sie niemanden interessiert — sondern weil keine Stelle im Unternehmen klar zuständig ist, sie zu stellen. Das Ergebnis ist ein KI-System im Produktivbetrieb, dessen regulatorisches Risikoprofil niemand kennt.

Kein Monitoring nach Deployment. Selbst dort, wo eine initiale Risikobewertung stattgefunden hat, endet die Governance häufig mit der Inbetriebnahme. Modelle driften — ihre Ausgaben verändern sich, wenn sich die Eingabedaten verändern. Bias, der zum Zeitpunkt des Trainings nicht sichtbar war, kann durch veränderte Nutzungsmuster sichtbar werden. Ein Modell, das in einer stabilen Umgebung kalibriert wurde, kann in einer veränderten Umgebung systematisch falsche Ergebnisse produzieren — ohne Fehlermeldung, ohne Alarm, ohne dass jemand es bemerkt. KI ohne Post-Deployment-Monitoring ist kein fertiges Produkt. Es ist eine Hypothese im Produktivbetrieb.

Fehlende oder veraltete DPIA für KI-gestützte Verarbeitungen. Viele KI-Systeme verarbeiten personenbezogene Daten — und viele dieser Verarbeitungen sind hochriskant im Sinne des Art. 35 DSGVO: Automatisierte Entscheidungen, Profiling, Verarbeitung besonderer Kategorien personenbezogener Daten. Eine DPIA ist in diesen Fällen üblicherweise verpflichtend. In der Praxis wird sie häufig nicht durchgeführt — oder sie wurde einmalig erstellt und nicht aktualisiert, obwohl sich das Modell, die Datenbasis oder der Verwendungszweck geändert

haben.. Eine veraltete DPIA für ein KI-System ist nicht nur ein Datenschutzproblem — sie ist der dokumentierte Beweis, dass die Organisation das Risiko ihres eigenen Systems nicht kennt.

Keine Dokumentation von Trainingsdaten und Modellentscheidungen. Die KI-VO verlangt für Hochrisiko-Systeme eine umfassende technische Dokumentation — Trainingsdaten, Testverfahren, Leistungsmetriken, bekannte Limitierungen. Diese Anforderung wird für die meisten Hochrisiko-Systeme erst mit August 2026 verbindlich. Das ist jedoch keine Entschuldigung — sondern ein Versäumnis. Wer KI-Systeme betreibt, die personenbezogene Daten verarbeiten, Entscheidungen beeinflussen oder sicherheitsrelevante Funktionen übernehmen, hätte diese Fragen im eigenen Interesse längst stellen müssen. Was nicht dokumentiert ist, kann nicht geprüft werden. Was nicht geprüft werden kann, kann nicht verantwortet werden. AI Debt beginnt oft genau hier: Nicht beim falschen Modell, sondern beim fehlenden Gedächtnis des richtigen.

Governance-Vakuum bei GenAI-Tools. Generative KI-Anwendungen sind in Organisationen eingedrungen, lange bevor Governance-Strukturen existierten, die sie hätten einhegen können. Mitarbeiterinnen und Mitarbeiter nutzen diese Tools für Aufgaben, die personenbezogene Daten, vertrauliche Geschäftsinformationen oder regulierte Inhalte berühren — oft ohne Kenntnis der Datenverarbeitungspraktiken der Anbieter, ohne Freigabeprozess, ohne Protokollierung. Das ist **Shadow IT der nächsten Generation:** nicht mehr ein nicht genehmigtes SaaS-Tool, sondern ein nicht genehmigtes KI-System, das in Echtzeit mit sensiblen Daten interagiert. Die Governance hinkt nicht nur hinterher — sie hat in vielen Fällen noch nicht begonnen.

AI Debt ist strukturell anders

Was AI Debt von Security Debt und Privacy Debt fundamental unterscheidet, ist ihre Dynamik. Security Debt ist im Wesentlichen linear: Ein bekanntes Risiko bleibt unbehandelt und wächst mit der Zeit. Privacy Debt ist prozessual: Dokumentation und Realität driften auseinander. AI Debt wächst schneller als jede andere Form: Nicht nur mit der Zeit, sondern mit jeder Interaktion und jedem neuen Datenpunkt — und von zwei Seiten gleichzeitig, weil sich das Modell und die rechtlichen Anforderungen unabhängig voneinander weiterentwickeln.

Das bedeutet: AI Debt kann sich schneller akkumulieren als jede andere Form von Governance Debt. Und sie kann sich schneller materialisieren — in einem diskriminierenden Ergebnis, einem Datenleck, einer Aufsichtsmaßnahme oder einem Reputationsschaden, der entsteht, bevor irgendjemand im Unternehmen verstanden hat, was passiert ist.

AI Debt auf der Eskalationsskala

Der kritische Moment liegt nicht beim sichtbaren Schaden — er liegt beim ersten Zeichen, dass die Kontrolle schwindet. Ein KI-System, das ohne Risikobewertung betrieben wird, ist nicht „noch in Ordnung, solange nichts passiert". Es ist ein System, dessen Risikoprofil die Organisation nicht kennt — und das sie deshalb nicht steuern kann.

Der Unterschied zwischen einem verwalteten Risiko und einem unkontrollierten ist nicht die Schwere des Schadens. Es ist die Fähigkeit zur Reaktion. Diese Fähigkeit setzt Sichtbarkeit voraus. Sichtbarkeit setzt Governance voraus. Und Governance setzt voraus, dass jemand die Frage stellt — bevor das System die Antwort liefert.

Wer KI einsetzt, ohne Governance aufzubauen, kauft Geschwindigkeit auf Kredit. Der Zins ist fällig — spätestens dann, wenn die Aufsichtsbehörde fragt, das Modell diskriminiert oder die Daten weg sind.

The Blind Spot Factory

Die vorangegangenen drei Kapitel haben Security Debt, Privacy Debt und AI Debt einzeln beschrieben — ihre Entstehung, ihre Dynamik, ihre Eskalationslogik. Das war notwendig. Aber es war auch eine Vereinfachung. Denn in der Realität existieren diese drei Formen von **Blind Spot Debt** nicht nebeneinander. Sie entstehen zusammen, wachsen zusammen und verstärken sich gegenseitig — in einer Weise, die unsichtbar bleibt, solange man nur auf eine Domäne schaut.

Das ist die eigentliche These dieses Papers: Nicht Security Debt, nicht Privacy Debt, nicht AI Debt allein ist das Problem. Das Problem ist **die stille Triade — drei Schulden, ein Absturz.**

Wer nur eine davon sieht, sieht keine.

Warum Silos das Problem nicht lösen, sondern erzeugen

Organisationen denken in Zuständigkeiten. Der CISO verantwortet Security. Der DSB verantwortet Privacy. Wer KI verantwortet, ist in den meisten Organisationen noch nicht einmal klar geregelt — eine Beobachtung, die für sich schon ein Befund ist. Diese Aufteilung ist administrativ nachvollziehbar. Als Risikomodell ist sie gefährlich.

Denn Risiken respektieren keine Organigramme. Ein Sicherheitsvorfall ist fast immer auch ein Datenschutzereignis. Ein KI-System ohne Governance ist fast immer auch ein Security-Problem und ein Privacy-Problem. Eine Organisation, die ihre Blind Spot Debt in getrennten Registern führt, getrennt berichtet und getrennt bearbeitet, produziert systematisch blinde Flecken — nicht trotz ihrer Strukturen, sondern wegen ihnen.

The Blind Spot Factory ist kein Vorwurf. Es ist eine Beschreibung. Organisationen, die gut gemeinte Governance-Strukturen aufgebaut haben, die aber nicht miteinander sprechen, erzeugen genau das: Sichtbarkeit in Ausschnitten, Blindheit im Ganzen.

Wo die drei Schulden sich berühren

Die Überschneidungen zwischen Security Debt, Privacy Debt und AI Debt sind keine Randphänomene. Sie sind die Regel.

Security trifft Privacy. Jede Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 4 Z 12 DSGVO löst eine Kaskade von Pflichten aus: Meldepflicht gegenüber der Aufsichtsbehörde nach Art. 33 DSGVO, gegebenenfalls Benachrichtigungspflicht gegenüber den Betroffenen nach Art. 34 DSGVO — und Haftungsrisiko nach Art. 82 DSGVO. Security Debt, der zu einem Data Breach führt, materialisiert sich nicht nur als operativer Schaden, sondern als Privacy Debt, der schlagartig sichtbar wird. Umgekehrt gilt: Eine Organisation, deren Verarbeitungsverzeichnis nicht aktuell ist, weiß im Ernstfall nicht, welche Daten betroffen sind — und kann weder die Meldepflicht korrekt erfüllen noch den Schaden begrenzen. Privacy Debt macht Data Breaches teurer.

Privacy trifft AI. Ein KI-System, das personenbezogene Daten verarbeitet, ohne dass eine aktuelle DPIA vorliegt — wo dies nach Art. 35 DSGVO geboten wäre — ist gleichzeitig ein Privacy-Problem und ein AI-Governance-Problem. Die fehlende DPIA bedeutet nicht nur, dass eine gesetzliche Pflicht nicht erfüllt wurde — sie bedeutet, dass die Organisation die Risiken des Systems nicht systematisch bewertet hat. Was nicht bewertet wurde, kann nicht gesteuert werden. Was nicht gesteuert wird, eskaliert unkontrolliert. AI Debt und Privacy Debt verstärken sich hier direkt: jede Lücke in der einen Domäne vergrößert die Lücke in der anderen.

Für die, die es wirklich umsetzen wollen: Die DPIA fokussiert naturgemäß auf Datenschutzrisiken — sie ist kein vollständiges AI Risk Assessment. Wer jedoch mit

praxistauglichen Templates arbeitet, etwa jenen der CNIL oder des ICO, wird feststellen, dass diese strukturell so gut aufgebaut sind, dass sie als Ausgangspunkt für ein AI Risk Impact Assessment im Sinne der ISO 42001 durchaus genutzt werden können. Integrierte Governance muss nicht bei null anfangen — sie muss nur anfangen.

AI trifft Security. Ein KI-System ohne Post-Deployment-Monitoring (Überwachung nach der Inbetriebnahme) ist nicht nur ein Governance-Problem — es ist ein Angriffsziel. Modelle können manipuliert werden: Durch vergiftete Trainingsdaten, durch manipulierte Inputs, durch gezielte Ausnutzung von Bias. Eine Organisation, die ihr KI-System nicht beobachtet, bemerkt diese Angriffe nicht. Security Debt und AI Debt verschmelzen hier zu einem kombinierten Risiko, das weder der CISO allein noch der KI-Verantwortliche allein im Blick hat — weil keiner von beiden das vollständige Bild sieht.

Alle drei gemeinsam. Der häufigste Fall ist nicht die paarweise Überschneidung — es ist die vollständige Überlappung. Ein KI-System, das ohne Risikobewertung eingeführt wurde, personenbezogene Daten verarbeitet ohne aktuelle DPIA, nicht überwacht wird und dessen Schnittstellen security-seitig nie bewertet wurden, ist gleichzeitig Security Debt, Privacy Debt und AI Debt. Es ist der Normalfall in Organisationen, die KI pragmatisch eingeführt haben — und Governance als nachgelagerte Aufgabe betrachten, die irgendwann nachgeholt wird. Um es mit den Worten einer deutschen Popikone der 1980er zu sagen: Irgendwie, irgendwann, irgendwo — nur nicht heute, nicht hier, nicht von uns.

Warum Integrierte Governance keine Option ist, sondern eine Notwendigkeit

Die Konsequenz aus diesen Überschneidungen ist eindeutig: Wer Blind Spot Debt reduzieren will, muss alle drei Domänen gemeinsam denken. Nicht weil das eleganter wäre. Sondern weil getrennte Governance strukturell nicht in der Lage ist, kombinierte Risiken zu erkennen — geschweige denn zu steuern.

Integrierte Governance bedeutet nicht, dass der CISO plötzlich auch DSB ist oder der DSB plötzlich KI-Expertin. Es bedeutet, dass die drei Domänen gemeinsame Sichtbarkeit, gemeinsame Sprache und gemeinsame Eskalationswege haben. Dass ein Risk Register nicht drei separate Listen führt, sondern Querverbindungen sichtbar macht. Dass ein Incident nicht in einer Domäne geschlossen wird, ohne zu prüfen, ob er in einer anderen noch offen ist.

Das klingt nach Mehraufwand. Es ist das Gegenteil. Eine Organisation, die kombinierte Risiken früh erkennt, zahlt weniger — weniger Nachbesserungsaufwand, weniger Bußgelder, weniger Reputationsschaden, weniger Erklärungsbedarf gegenüber Behörden und Partnern. Und weniger administrativer Aufwand: wer Governance-Strukturen domänenübergreifend denkt, verteilt Arbeit auf mehrere Schultern und vermeidet Doppel- und Dreifachdokumentation. Dasselbe Asset, dasselbe System, dasselbe Risiko — einmal bewertet, mehrfach genutzt. Integrierte Governance ist kein Luxus für gut aufgestellte Organisationen. Sie ist die Grundvoraussetzung dafür, dass Governance überhaupt funktioniert.

Das gemeinsame Fundament

Was alle drei Formen von Blind Spot Debt verbindet, ist nicht ihre Herkunft — es ist ihre Ursache. Sie entstehen dort, wo Entscheidungen ohne vollständige Information getroffen werden. Wo Verantwortlichkeiten unklar sind. Wo Geschwindigkeit wichtiger ist als Sorgfalt. Wo Governance als Bremse gilt statt als Steuerungsinstrument.

Diese Ursachen lassen sich nicht domänenspezifisch beheben. Ein Security-Framework, das Privacy ignoriert, löst das Problem nicht. Ein Datenschutzmanagementsystem, das KI nicht

abdeckt, löst das Problem nicht. Ein KI-Governance-Framework, das Security und Privacy als fremde Zuständigkeiten behandelt, löst das Problem nicht.

Was das Problem löst, ist ein gemeinsames Verständnis davon, was Blind Spot Debt ist — domänenübergreifend, messbar und mit klarer Verantwortung versehen. Das ist der Anspruch der folgenden Kapitel.

Vom blinden Fleck zum Steuerungsinstrument — Indikatoren, Score und Praxis

Die vorangegangenen Kapitel haben beschrieben, was Blind Spot Debt ist, wie er entsteht und warum er in drei Domänen gleichzeitig gedacht werden muss. Dieses Kapitel liefert das, was bisher gefehlt hat — und was das ISACA-Whitepaper schuldig geblieben ist: Ein operationalisierbares Framework. Keine Metaphern mit Gleichheitszeichen. Keine Indikatoren ohne Messung. Keine Skala, die bei „Critical" aufhört zu funktionieren.

Der Anspruch ist einfach formuliert: Wer Blind Spot Debt managen will, muss ihn sehen können. Wer ihn sehen will, braucht Indikatoren, die Bewegung zeigen. Wer Bewegung zeigen will, braucht einen Score, der nicht nur beschreibt, wo eine Organisation steht — sondern auch, wohin sie sich bewegt und wie schnell.

Wie man sinnvolle Indikatoren entwickelt

Ein Indikator ist nur dann nützlich, wenn er drei Dinge gleichzeitig tut: Er zeigt Bewegung, er ist messbar ohne unverhältnismäßigen Aufwand, und er ist direkt mit einer Entscheidung oder Maßnahme verbunden. Ein Indikator, der keinen Handlungsimpuls auslöst, ist kein Steuerungsinstrument — er ist Dekoration. Für Blind Spot Debt gelten **zusätzlich zwei Anforderungen,** die über klassische Security-Metriken hinausgehen:

Erstens müssen Indikatoren in allen drei Bereichen gleichzeitig anschlussfähig sein. Ein Indikator, der nur in einer Domäne Sinn ergibt, reproduziert den Silo-Fehler, den integrierte Governance überwinden soll. Die stärksten Indikatoren sind jene, die auf mindestens zwei Domänen gleichzeitig einzahlen.

Zweitens müssen Indikatoren die Zeitdimension abbilden. Blind Spot Debt akkumuliert nicht durch einzelne Ereignisse, sondern durch kontinuierliche Unterlassung. Ein Indikator, der nur den aktuellen Zustand beschreibt, ohne zu zeigen, wie lange dieser Zustand bereits besteht, unterschätzt das Risiko systematisch.

Zwei Schritte, eine Sicht

Die Indikatoren in diesem Kapitel folgen einer bewussten Struktur. Im ersten Schritt werden Indikatoren je Domäne entwickelt — Security, Privacy und AI getrennt. Das ist notwendig, weil jede Domäne ihre eigene Messlogik, ihre eigenen Datenquellen und ihre eigenen Schwellenwerte hat. Wer versucht, alles auf einmal zu messen, misst am Ende nichts präzise.

Im zweiten Schritt werden diese domänenspezifischen Indikatoren zusammengeführt — nicht addiert, sondern verschnitten. Die stärksten Signale für Blind Spot Debt sind nicht jene, die in einer Domäne ausschlagen, sondern jene, die in zwei oder drei Domänen gleichzeitig Bewegung zeigen. Dieser Verschnitt ist der eigentliche Mehrwert des integrierten Ansatzes: Er macht sichtbar, was getrennte Governance systematisch übersieht.

Indikatoren für Security Debt

Patch Latency — durchschnittliche Zeit zwischen Bekanntwerden einer Schwachstelle und ihrer Behebung.

Messung: Abgleich zwischen CVE-Veröffentlichungsdatum und Datum der Remediation im Vulnerability Management System. Getrennt zu erheben für kritische, hohe und mittlere Schwachstellen.
Zeitdimension: Gleitender Durchschnitt über 90 Tage.

End-of-Life Asset Rate — Anteil der Systeme, die auf nicht mehr unterstützten Plattformen laufen.
Messung: Abgleich des Asset Inventars mit den offiziellen End-of-Life-Daten der Hersteller. Systeme ohne bekanntes EOL-Datum gelten als ungeklärt und werden separat ausgewiesen.
Zeitdimension: Datum des EOL-Eintritts als Gewichtungsfaktor.

Control Effectiveness Trend — Entwicklung der Testergebnisse für implementierte Sicherheitskontrollen über Zeit.
Messung: Ergebnisse aus internen und externen Audits, Penetrationstests und automatisierten Control-Tests, aggregiert pro Kontrollbereich.
Zeitdimension: Vergleich aktueller Ergebnisse mit den Ergebnissen der letzten zwei Messzyklen.

Exception Aging — Anteil offener Risikoausnahmen, die älter als 90 Tage sind.
Messung: Risk Register, gefiltert nach offenen Ausnahmen mit Datum der Genehmigung. Ausnahmen ohne definierten Review-Termin gelten automatisch als eskalationswürdig.
Zeitdimension: Alter der Ausnahme als primärer Gewichtungsfaktor.

Ein strukturelles Problem vorweg: In der Praxis existieren Risikoausnahmen häufig nur als Vorstandsbeschluss — und werden nie in ein operatives Security- oder Risikoregister übertragen. Was nicht im Register steht, wird nicht überwacht, nicht reviewed und nicht eskaliert. Die erste Maßnahme zur Operationalisierung dieses Indikators ist daher nicht die Messung selbst, sondern die Überführung bestehender Ausnahmen aus Beschlüssen in ein zentrales Register mit Owner, Genehmigungsdatum und definiertem Review-Termin. Erst dann ist Exception Aging messbar. Und erst dann ist die Ausnahme tatsächlich unter Kontrolle.

Indikatoren für Privacy Debt

AVV-Abdeckungsrate — Anteil der Auftragsverarbeiter, für die ein AVV vorliegt, gemessen an allen Dienstleistern, die nach Art. 28 DSGVO einen AVV erfordern.
Messung: Abgleich des Dienstleisterverzeichnisses mit dem AVV-Register. Zielwert: 100% — jede Abweichung ist Privacy Debt.
Zeitdimension: Datum der Ersterfassung relativ zum Datum des Beginns der Auftragsverarbeitung.

Sub-Auftragsverarbeiter-Transparenz — Anteil der Auftragsverarbeiter, für die eine aktuelle Liste der eingesetzten Sub-Auftragsverarbeiter vorliegt und geprüft wurde.
Messung: Abgleich der vertraglich gemeldeten Sub-Auftragsverarbeiter mit dem internen Register, ergänzt um eine Risikoeinschätzung je Sub-Auftragsverarbeiter.
Zeitdimension: Datum der letzten Überprüfung relativ zu Änderungsmeldungen des Auftragsverarbeiters.
Ein nicht geprüfter Sub-Auftragsverarbeiter ist ein unentdecktes Supply-Chain-Risiko — und damit gleichzeitig Privacy Debt und Security Debt. Dass die Lieferkettenthematik kein Randthema ist, unterstreichen NIS2 und DORA explizit: NIS2 verpflichtet betroffene Einrichtungen zur Berücksichtigung von Sicherheitsrisiken in der Lieferkette, DORA verlangt für Finanzunternehmen ein vollständiges IKT-Drittanbieter-Risikomanagement inklusive vertraglicher Mindestanforderungen und laufender Überwachung. Ein Sub-Auftragsverarbeiter, der datenschutzrechtlich nie geprüft wurde, ist in diesen Kontexten nicht nur ein Privacy-Problem — er ist ein regulatorischer Blind Spot in zumindest zwei Frameworks gleichzeitig.

TOM-Aktualität — Grad der Übereinstimmung zwischen den vertraglich vereinbarten technischen und organisatorischen Maßnahmen des Auftragsverarbeiters und dem aktuellen Stand der Technik — sowie zwischen den tatsächlich implementierten Maßnahmen und ihrer Dokumentation beim Verantwortlichen.
Messung: Regelmäßige Überprüfung der TOMs — idealerweise durch Fragebögen, Audits oder Zertifikatsnachweise.
Parallel dazu: Abgleich der intern dokumentierten TOMs mit der tatsächlich implementierten Systemarchitektur und den aktuellen Verarbeitungspraktiken. Eine TOM-Dokumentation, die die eigene Realität nicht mehr abbildet, ist nicht nur wertlos — sie ist im Ernstfall ein Haftungsrisiko, weil sie Schutzmaßnahmen verspricht, die nicht existieren.
Zeitdimension: Datum der letzten TOM-Überprüfung relativ zu wesentlichen Änderungen beim Dienstleister, in der eigenen Infrastruktur oder in der Bedrohungslage.

Verarbeitungsverzeichnis-Drift — Zeitabstand zwischen letzter Aktualisierung des Verarbeitungsverzeichnisses und letzter nachweisbarer Änderung von Systemen, Prozessen oder Dienstleistern.
Messung: Dieser Indikator ist nur erhebbar, wenn mindestens eine der folgenden Voraussetzungen erfüllt ist:

1. Erstens ein funktionierendes Change Management, dessen Protokolle mit dem Verarbeitungsverzeichnis abgeglichen werden können — neue Tools, neue Dienstleister, neue Prozesse müssen dort erfasst sein, bevor sie in Betrieb gehen.
2. Zweitens eine regelmäßige strukturierte Befragung der Fachabteilungen — mindestens jährlich, besser halbjährlich — mit der expliziten Frage, ob sich Verarbeitungstätigkeiten seit der letzten Überprüfung geändert haben.
3. Drittens ein Abgleich mit Einkaufs- und Lizenzdaten: Neue Software-Lizenzen oder Dienstleisterverträge sind ein zuverlässiger Proxy für neue Verarbeitungstätigkeiten — und in den meisten Organisationen leichter zugänglich als Change-Management-Protokolle.

Wo keine dieser Voraussetzungen erfüllt ist, ist der Drift selbst der Befund: Eine Organisation, die nicht sagen kann, ob ihr Verarbeitungsverzeichnis aktuell ist, hat bereits Privacy Debt — unabhängig davon, ob tatsächlich Änderungen stattgefunden haben.
Zeitdimension: Je größer der Abstand zwischen letzter Aktualisierung und letztem nachweisbarem Änderungsereignis, desto höher der Drift-Score.

DPIA-Abdeckungsgrad — Anteil der Verarbeitungstätigkeiten, für die eine DPIA nach Art. 35 DSGVO erforderlich ist und eine aktuelle DPIA vorliegt.
Messung in zwei Schritten: Erstens eine strukturierte Prüfung aller Verarbeitungstätigkeiten nach dem Kriterium „DPIA erforderlich ja oder nein“ — unter Berücksichtigung der EDSA-Guidance zu Hochrisikoverarbeitungen sowie der lokalen Black- und Whitelist-Verordnung der zuständigen Aufsichtsbehörde. Erst dieser Schritt schafft die Grundlage für eine sinnvolle Messung. Zweitens Abgleich der als DPIA-pflichtig eingestuften Verarbeitungen mit den tatsächlich vorliegenden DPIAs — dokumentiert im Verarbeitungsverzeichnis selbst oder in einem daran angehängten Nachweis. Als „wesentliche Änderung", die eine Aktualisierung der DPIA auslöst, gelten: Änderung des Verarbeitungszwecks, Änderung der Datenkategorien, Wechsel des Verarbeitungssystems oder -dienstleisters, sowie Änderungen in der Risikobewertung durch neue regulatorische Anforderungen oder Bedrohungslagen.
Zeitdimension: Datum der letzten DPIA relativ zum Datum der letzten dokumentierten Änderung in einer der genannten Kategorien.

Betroffenenrechte-Prozessreife — Fähigkeit der Organisation, Anfragen fristgerecht, vollständig und verständlich zu beantworten, unabhängig davon, über welchen Kanal sie eingehen.
Messung: Tracking von Bearbeitungszeiten und Vollständigkeit bei eingehenden Anfragen — ergänzt um die Erfassung des Eingangskanals, da Anfragen über verschiedene Wege eingehen können: Dediziertes Datenschutzpostfach, allgemeine Unternehmens-Email, Telefon, postalisch oder über Dritte. Anfragen, die nicht beim DSB landen, weil der Kanal nicht bekannt oder nicht weitergeleitet wird, sind selbst ein Indikator für Prozessschwäche.
Zusätzlich: Erfassung von Rückfragen seitens der Betroffenen nach Erhalt einer Antwort — als Proxy für Verständlichkeit und Vollständigkeit. Eine Auskunft, die Rückfragen auslöst, war keine ausreichende Auskunft. Ergänzt durch regelmäßige interne Testanfragen zur Überprüfung der operativen Funktionsfähigkeit.
Zeitdimension: Entwicklung der Bearbeitungszeiten und Rückfragenquote über die letzten vier Quartale.

Indikatoren für AI Debt

KI-Inventar-Abdeckung — Anteil der im Einsatz befindlichen KI-Systeme, die im Verarbeitungsverzeichnis erfasst sind, soweit sie personenbezogene Daten verarbeiten, sowie in der IT-Asset-Liste für alle übrigen Systeme. Eine gesonderte Pflicht zur Führung eines KI-Registers existiert weder in der KI-VO noch mittelbar aus anderen Rechtsquellen — wer ein solches einführt, schafft Mehraufwand ohne rechtliche Grundlage. Sinnvoller ist es, bestehende Strukturen zu nutzen: Das Verarbeitungsverzeichnis als primären Ankerpunkt für KI-Systeme mit Personenbezug, die IT-Asset-Liste für alle übrigen.
Messung: Abgleich zwischen Verarbeitungsverzeichnis und IT-Asset-Liste einerseits und den tatsächlich genutzten Systemen andererseits — ermittelt durch Befragung der Fachabteilungen, Analyse von Lizenz- und Beschaffungsdaten sowie technisches Scanning auf API-Verbindungen zu bekannten KI-Anbietern.
Zeitdimension: Datum der Ersterfassung relativ zum Inbetriebnahmedatum.

Risikokategorisierungs-Quote — Anteil der erfassten KI-Systeme, für die eine Risikobewertung nach KI-VO durchgeführt wurde.
Messung: Abgleich des KI-Inventars mit dem Dokumentationsstand der Risikobewertungen. Systeme ohne abgeschlossene oder veraltete Bewertung gelten als offen.
Zeitdimension: Datum der letzten Bewertung relativ zu Änderungen am System oder seinem Nutzungskontext.

Post-Deployment-Monitoring-Abdeckung — Anteil der produktiven KI-Systeme, für die ein nutzungsseitiges Monitoring dokumentiert ist. Der Betreiber ist nicht verpflichtet und in der Regel auch nicht in der Lage, das Modell selbst technisch zu überwachen — das ist Aufgabe des Anbieters. Was der Betreiber leisten muss und kann: Die Beobachtung des Systemverhaltens im eigenen Nutzungskontext, orientiert am Benutzerhandbuch des Anbieters.
Messung: Dokumentierter Nachweis, dass das Benutzerhandbuch vorliegt und bekannt ist, sowie eine strukturierte Erfassung von Auffälligkeiten, unerwarteten Ausgaben oder wahrnehmbaren Verhaltensänderungen des Systems — etwa in einem einfachen Logbuch oder im Ticketsystem.
Zeitdimension: Zeitraum seit letztem dokumentiertem Monitoring-Eintrag. Ein System ohne einen einzigen Eintrag seit Inbetriebnahme ist kein unauffälliges System — es ist ein unbeobachtetes.

GenAI-Governance-Reife — Vorhandensein einer organisationsweiten Richtlinie für generative KI-Tools sowie deren tatsächliche Wirksamkeit im Alltag.
Messung: Erstens Dokumentenprüfung der Richtlinie — existiert sie, ist sie aktuell, ist sie kommuniziert? Zweitens, und aussagekräftiger: Auswertung durch die IT — welche KI-

bezogenen Websites und Dienste sind gesperrt oder freigegeben, und entspricht das der Richtlinie? Drittens Scanning auf Shadow-KI: API-Verbindungen zu bekannten KI-Anbietern, Browser-Plugins mit KI-Funktionalität, nicht freigegebene SaaS-Tools mit eingebetteten KI-Features. Was die IT im Netz sieht, ist ehrlicher als jede Selbstauskunft einer Fachabteilung. Besondere Aufmerksamkeit verdienen AI Agents — autonome Systeme, die nicht nur auf Eingaben reagieren, sondern selbstständig handeln, Entscheidungen treffen und mit anderen Systemen interagieren. Eine Richtlinie, die GenAI-Tools adressiert, aber AI Agents nicht explizit einschließt, hat eine Lücke genau dort, wo das Risiko am größten ist. *Zeitdimension:* Datum der letzten Aktualisierung der Richtlinie relativ zu neu verfügbaren GenAI-Tools und Agent-Frameworks im Markt — eine Richtlinie, die ChatGPT kennt aber Gemini, Copilot, lokale LLM-Clients und AI Agents nicht, ist bereits veraltet.

Praxisbeispiele — Indikatoren, die auf zwei Domänen einzahlen

Die stärksten Indikatoren für Blind Spot Debt sind jene, die domänenübergreifend wirken. Die folgenden Beispiele illustrieren, wie ein einziger Befund gleichzeitig Security Debt, Privacy Debt oder AI Debt sichtbar macht.

Beispiel 1: Das KI-System im HR-Bereich ohne DPIA und ohne Security-Bewertung. Ein Unternehmen setzt ein KI-gestütztes Tool zur Vorauswahl von Bewerbungen ein. Das Tool wurde eingeführt, weil es den Prozess beschleunigt. Eine DPIA wurde nicht durchgeführt — obwohl automatisierte Entscheidungen über Personen eine DPIA-Pflicht nach Art. 35 DSGVO ausgelöst hätten, und zwar vor Inbetriebnahme des Systems. Eine Security-Bewertung der API-Schnittstelle zum Bewerbermanagementsystem wurde nie vorgenommen. Indikator-Befund: DPIA-Abdeckungsgrad = 0% für dieses System (Privacy Debt), Risikokategorisierungs-Quote = offen (AI Debt), keine dokumentierte Schnittstellenbewertung (Security Debt). Alle drei Domänen, ein System, null Sichtbarkeit.

Beispiel 2: Der veraltete AVV und die ungepatchte Schnittstelle. Ein Dienstleister verarbeitet personenbezogene Daten im Auftrag — der AVV wurde bei Vertragsschluss unterzeichnet und seither nicht aktualisiert. Die technische Schnittstelle zum Dienstleister läuft auf einer Komponente, die seit acht Monaten eine bekannte Schwachstelle aufweist. Indikator-Befund: AVV-Abdeckungsrate = nicht aktuell (Privacy Debt), Patch Latency = 240 Tage für diese Komponente (Security Debt). Im Ernstfall — einem Data Breach über diese Schnittstelle — treffen beide Schulden gleichzeitig ein: Die Organisation kann weder die Meldepflicht korrekt erfüllen noch den Schaden begrenzen, weil sie weder die aktuelle Verarbeitungssituation noch die technische Schwachstelle im Griff hat.

Beispiel 3: GenAI im Einsatz, Governance nicht gestartet. Mitarbeiterinnen und Mitarbeiter eines Unternehmens nutzen einen Large Language Model-Dienst für die Erstellung von Angeboten und internen Berichten — inklusive gelegentlicher Eingabe von Kundendaten. Eine Richtlinie existiert nicht. Eine Datenschutzbewertung des Dienstleisters wurde nicht durchgeführt. Eine Security-Freigabe fehlt. Indikator-Befund: GenAI-Governance-Reife = nicht vorhanden (AI Debt), keine Bewertung der Datenverarbeitungspraktiken des Anbieters (Privacy Debt), keine Security-Freigabe (Security Debt). Das Risiko ist real, die Sichtbarkeit ist null — und niemand im Unternehmen weiß es, weil niemand gefragt hat.

Der überarbeitete Score — Blind Spot Debt Index

Der von ISACA vorgeschlagene Security Debt Index — Severity multipliziert mit Duration und Velocity, dividiert durch einen nicht definierten Normalisierungsfaktor — war ein richtiger Impuls, wenn auch mit falscher Ausführung. Der **Blind Spot Debt Index (BSDI)** übernimmt die

Grundstruktur, operationalisiert sie konsequent und erweitert sie um die fehlende Domänendimension.

Der BSDI basiert auf denselben drei Dimensionen:

Severity beschreibt den potenziellen Geschäftsschaden des identifizierten Debt-Elements — regulatorisches Risiko, operativer Schaden, Reputationsverlust. Skala 1–5, definiert nach organisationsspezifischen Schwellenwerten, die im Vorfeld festzulegen sind. Konkret: Severity 1 = minimales Risiko ohne regulatorische Relevanz; Severity 3 = Risiko mit potenziellem Bußgeld oder operativer Einschränkung; Severity 5 = existenzielles Risiko mit behördlicher Intervention oder schwerem Reputationsschaden.

Duration beschreibt, wie lange das Debt-Element bereits ungelöst besteht. Skala 1–5: 1 = unter 30 Tage; 2 = 30–90 Tage; 3 = 90–180 Tage; 4 = 180–365 Tage; 5 = über 365 Tage. Damit ist Duration nicht nur benannt, sondern operationalisiert — jede Organisation kann jeden offenen Befund direkt einstufen.

Velocity beschreibt, wie schnell sich neue Debt-Elemente desselben Typs akkumulieren. Skala 1–5: 1 = isolierter Einzelbefund; 3 = wiederkehrendes Muster in einer Domäne; 5 = systemisches Muster über mehrere Domänen. Velocity ist der Frühwarnindikator: Ein hoher Velocity-Score zeigt, dass das Problem struktureller Natur ist — und dass punktuelle Nachbesserung nicht reicht.

Die Berechnung: BSDI = (Severity × Duration × Velocity) / Anzahl bewerteter Debt-Elemente im Messzeitraum. Der Divisor ist damit explizit definiert — nicht als abstrakter "Normalisierungsfaktor", sondern als Anzahl der tatsächlich bewerteten Elemente. Das macht den Score vergleichbar über Zeit und zwischen Organisationsbereichen.

Die überarbeitete Eskalationsskala

Hier weicht der BSDI fundamental vom ISACA-Ansatz ab. Die Skala hat nicht vier, sondern fünf Stufen — und die entscheidende Verschiebung liegt zwischen Stufe 3 und Stufe 4:

1. *Stufe 1 — Controlled (0–15):* Blind Spot Debt ist sichtbar, wird aktiv gemanagt und zeigt keine systemischen Muster. Reguläre Governance-Prozesse sind ausreichend.
2. *Stufe 2 — Accumulating (16–30):* Debt akkumuliert schneller als er abgebaut wird. Einzelne Domänen zeigen Rückstand. Erhöhte Aufmerksamkeit und priorisierte Maßnahmen sind erforderlich.
3. *Stufe 3 — Compounding (31–50):* Debt-Elemente beginnen sich gegenseitig zu verstärken. Domänenübergreifende Muster werden sichtbar. Hier ist sofortiges Handeln erforderlich — nicht erhöhte Aufmerksamkeit. Wer in dieser Stufe wartet, bewegt sich auf den Abgrund zu.
4. *Stufe 4 — Critical (51–75):* Die Organisation steht am Rand. Kontrolle über kombinierte Risiken ist eingeschränkt. Die Behebung erfordert dedizierte Ressourcen, klare Verantwortlichkeiten und externe Unterstützung. Jeder weitere Tag ohne Intervention erhöht die Wahrscheinlichkeit eines unkontrollierten Ereignisses.
5. *Stufe 5 — Compromised (76–100):* Kontrolle ist verloren. Blind Spot Debt hat sich in allen drei Domänen materialisiert oder steht unmittelbar davor. Krisenmanagement ersetzt Governance. Die Schadensbehebung ist nicht mehr präventiv — sie ist reaktiv, teuer und öffentlich.

Der entscheidende Unterschied zum ISACA-Modell: Stufe 3 ist nicht die Vorstufe zur Krise. Sie ist die letzte Stufe, in der eine Organisation noch die Wahl hat, wie sie reagiert. Ab Stufe 4 reagiert sie nicht mehr — **sie wird reagiert.**

Und Stufe 5 endet nicht mit „komplettem Reset erforderlich" ohne weitere Erklärung. Sie endet mit der unbequemsten aller Aussagen: Es wäre vermeidbar gewesen — mit Governance, die nicht nur auf dem Papier existiert, sondern tatsächlich gelebt wird. **Governance als zahnloser Papiertiger ist keine Governance.** Es ist eine Illusion von Kontrolle, die im Ernstfall teurer ist als gar keine — weil sie das Gefühl von Sicherheit erzeugt, ohne die Substanz zu liefern. Der Weg zurück führt nicht durch ein Framework — er führt durch Rechenschaft. Gegenüber Behörden, gegenüber Kunden, gegenüber dem eigenen Vorstand, gegenüber den Stakeholdern. Und einer interessierten Öffentlichkeit. Das dauert. Und es kostet mehr, als irgendjemand budgetiert hat. Und ganz sicherlich mehr, als Prävention jemals gekostet hätte.

Conclusio & Ausblick — Was bleibt, was kommt, was fehlt

Dieses Paper hat mit einer Kritik begonnen und mit einem Framework geendet. Das war Absicht. Kritik ohne Konstruktion ist Kommentar. Konstruktion ohne Kritik ist Gefälligkeit. Beides zusammen ist der Versuch, einen Beitrag zu leisten, der über den Status quo hinausgeht.

Der Status quo ist dieser: Organisationen akkumulieren Governance-Schulden in drei Domänen gleichzeitig — Security, Privacy und AI — und behandeln sie als drei separate Probleme mit drei separaten Zuständigkeiten, drei separaten Registern und drei separaten Eskalationswegen. Das Ergebnis ist eine Architektur der blinden Flecken. The Blind Spot Factory läuft auf Hochtouren — nicht weil Menschen böswillig handeln, sondern weil Strukturen, die für eine einfachere Welt gebaut wurden, mit der Komplexität der heutigen nicht Schritt gehalten haben.

Blind Spot Debt ist die Konsequenz. Und er ist messbar, steuerbar und reduzierbar — wenn man ihn sehen will.

Was bleibt

Drei Erkenntnisse aus diesem Paper verdienen es, festgehalten zu werden:

1. Erstens: Security Debt, Privacy Debt und AI Debt sind nicht drei Varianten desselben Problems. Sie haben unterschiedliche Entstehungsmechanismen, unterschiedliche Eskalationsdynamiken und unterschiedliche rechtliche Konsequenzen. Wer sie gleichbehandelt, vereinfacht auf eine Weise, die gefährlich ist.
2. Zweitens: Sie sind trotzdem untrennbar verbunden. Ein Data Breach ist fast immer gleichzeitig ein Security-Ereignis und ein Datenschutzereignis. Ein KI-System ohne Governance ist fast immer gleichzeitig ein Privacy-Problem und ein Security-Problem. Getrennte Governance kann kombinierte Risiken strukturell nicht erkennen.
3. Drittens: Messbarkeit ist keine akademische Übung. Der Blind Spot Debt Index ist kein Selbstzweck — er ist ein Kommunikationsinstrument. Er übersetzt akkumuliertes Risiko in eine Sprache, die Vorstände, Aufsichtsbehörden und Geschäftsführungen verstehen: Bewegung, Richtung, Dringlichkeit. Wer Governance ernst nimmt, braucht Zahlen. Wer Zahlen will, braucht Indikatoren. Wer Indikatoren will, muss zuerst die richtigen Fragen stellen.

Was kommt

Die Komplexität wird nicht abnehmen. Drei Entwicklungen werden Blind Spot Debt in den kommenden Jahren weiter verschärfen — und verdienen eine vertiefte Betrachtung, die über den Rahmen dieses Papers hinausgeht.

AI Agents und autonome Systeme. Generative KI war erst der Anfang. AI Agents — autonome Systeme, die nicht nur antworten, sondern handeln, entscheiden und mit anderen Systemen interagieren — werden in Organisationen einziehen, lange bevor Governance-Strukturen existieren, die sie einhegen können. Die Fragen, die sich daraus ergeben, sind noch nicht abschließend beantwortet: Wer haftet, wenn ein Agent eine falsche Entscheidung trifft? Wie wird

ein Agent überwacht, dessen Handlungen nicht vorhersehbar sind? Wie wird sichergestellt, dass ein Agent keine personenbezogenen Daten verarbeitet, für die keine Rechtsgrundlage besteht? Diese Fragen werden kommen. Die Antworten sollten nicht warten, bis sie gestellt werden.

Die regulatorische Verdichtung. DSGVO, KI-VO, NIS2, DORA, CRA — die regulatorische Landschaft verdichtet sich. Jedes dieser Regelwerke adressiert Teile des Blind Spot Debt-Problems. Keines adressiert es vollständig. Und keines ist so konzipiert, dass es nahtlos mit den anderen zusammenspielt. Die Konsequenz: Organisationen, die jeden Rechtsrahmen isoliert erfüllen, erfüllen keinen vollständig. Integrierte Governance ist nicht nur effizienter — sie ist die einzige Strategie, die in einer regulatorisch verdichteten Welt funktioniert. Compliance ist dabei nicht das Ziel, sondern die Mindestanforderung: Wer Gesetze befolgt, hat noch keine Governance. Governance bedeutet, aktiv zu steuern wie eine Organisation mit Risiken umgeht — bewusst dorthin zu schauen, wo es weh tut, Verantwortung zu übernehmen, für sich selbst, für das Unternehmen, für die Menschen, deren Daten verarbeitet werden. Compliance fragt: Halten wir die Regeln ein? Governance fragt: Tun wir das Richtige? Wer nur die erste Frage stellt, hat die zweite noch nicht verstanden.

Die menschliche Dimension. Governance Debt ist kein technisches Problem. Es ist ein kulturelles. Frameworks helfen. Indikatoren helfen. Scores helfen. Aber sie helfen nur, wenn Menschen in Organisationen bereit sind, unbequeme Befunde anzuerkennen, Verantwortung zu übernehmen und Entscheidungen zu treffen, die kurzfristig teuer erscheinen und langfristig günstiger sind. Das ist keine Frage der Methodik — es ist eine Frage der Haltung. Und Haltung ist eine Frage von Werten. Werte sind nicht das, was auf hochglanzpolierten Folien zur „Corporate Culture" steht, die irgendwo in einer Ecke verstauben. Werte sind das, was eine Organisation tut, wenn niemand hinschaut. Wenn die Aufsichtsbehörde nicht prüft. Wenn kein Incident droht. Wenn es einfacher wäre, die Augen zu verschließen. Governance, die nur unter Beobachtung funktioniert, ist keine Governance. Es ist Theater.

Was fehlt — und wo weiter hingeschaut werden sollte

Zwei Themen verdienen eine vertiefte Betrachtung, die in diesem Paper nur angedeutet werden konnte.

DORA und der Three Lines of Defence-Ansatz. DORA hat für Finanzunternehmen einen der ambitioniertesten regulatorischen Rahmen für IKT-Risikomanagement geschaffen — inklusive expliziter Anforderungen an das IKT-Drittanbieter-Risikomanagement, Incident-Meldepflichten und Business Continuity. Das Three Lines of Defence-Modell, das DORA als Governance-Struktur voraussetzt, ist dabei mehr als eine regulatorische Anforderung — es ist ein Prinzip, das, konsequent und ehrlich angewendet, Blind Spot Debt sichtbar machen kann.

Die Betonung liegt auf konsequent und ehrlich. Denn 3LoD wird in der Praxis häufig auf IKT und Security reduziert — ergänzt, wo der Regulator explizit hinschaut, etwa bei der Überwachung ausgelagerter wesentlicher bankbetrieblicher Funktionen nach § 25 BWG. Das ist notwendig, aber nicht hinreichend. Wer 3LoD nur dort anwendet, wo der Regulator es verlangt, hat das Prinzip nicht verstanden — er hat die Anforderung erfüllt. Das ist der Unterschied zwischen Compliance und Governance, den dieses Paper von Anfang an zieht.

Was das konkret bedeutet, lässt sich an Beispielen zeigen, die auf den ersten Blick nichts mit IKT-Risikomanagement zu tun haben — und genau deshalb so aufschlussreich sind.

Einstellungsprozesse haben in den meisten Organisationen Regelungen zu Interessenskonflikten — aber wer prüft, dass HR diese tatsächlich einhält? Trainings werden mit Teilnahmequoten gemessen — aber wer prüft, ob die Inhalte tatsächlich rezipiert und verstanden wurden, oder ob der Klick auf "Abschließen" das einzige messbare Ergebnis ist? Vor allem dann, wenn

Abschlussquizzes beliebig oft wiederholt werden können, bis die richtige Antwort durch Ausprobieren gefunden wird — und die Teilnahmequote trotzdem als Nachweis wirksamer Schulung gilt. Eine Kantine, die Daten von Mitarbeitenden verarbeitet — wer hat den AVV mit dem Cateringunternehmen abgeschlossen? Wer prüft die TOMs des Cateringunternehmens? Und wer prüft, ob Vertraulichkeit beim Mittagessen eingehalten wird — ob nicht doch offen über Kundenprojekte gesprochen wird, Bildschirme ungesperrt bleiben, wenn jemand kurz einen Kaffee holt, oder Dokumente auf dem Tisch liegen, die dort nicht hingehören?

Das sind keine akademischen Spitzfindigkeiten. Es sind die Bereiche, in denen Blind Spot Debt entsteht — still, unbeobachtet, unbefragt — weil die erste Linie davon ausgeht, dass es kein Problem gibt, die zweite nicht hinschaut, weil es nicht ihr Kernbereich ist, und die dritte nicht prüft, weil es nicht auf der Agenda steht.

3LoD nach DORA kann mehr sein als eine Anforderung an Einkauf, IT und Security. Es kann das Prinzip sein, das Blind Spot Debt dort aufdeckt, wo er am gefährlichsten ist: in den Lücken zwischen den Zuständigkeiten, in den Annahmen, die niemand hinterfragt, in den Prozessen, die funktionieren — weil noch niemand ernsthaft geprüft hat, ob sie es wirklich tun. Wer 3LoD so versteht, befolgt nicht einfach nur die Buchstaben des Gesetzes nach dem Wortlaut — er hat Governance verstanden.

Die Frage der Proportionalität. Dieses Paper richtet sich an Organisationen, die Governance ernst nehmen. Aber nicht alle Organisationen haben dieselben Ressourcen. Ein Blind Spot Debt Index, der für ein mittelgroßes Finanzinstitut funktioniert, funktioniert nicht zwingend für ein KMU mit drei IT-Mitarbeitenden. Die Frage, wie ein proportionales Framework für Blind Spot Debt aussieht — eines, das die wesentlichen Indikatoren behält, aber den Aufwand auf das Notwendige reduziert — ist offen. Sie ist wichtig. Und sie verdient eine eigene Antwort.

Der letzte Satz

Blind Spot Debt wächst im Stillen. Er akkumuliert in den Lücken zwischen Zuständigkeiten, in den Abständen zwischen Prüfzyklen, in den Entscheidungen, die niemand dokumentiert hat. Er wird sichtbar, wenn es zu spät ist — oder wenn jemand anfängt, die richtigen Fragen zu stellen.

Dieses Paper ist der Versuch, diese Fragen zu stellen. Die Antworten liegen in den Organisationen, die sie stellen.