Field Talk - 17 November 2026

Wrong Tools for the Job: Challenges in Operationalising Data and AI Governance

Shane P McNamee

Ground Rules & Practitioner Framing

PERSPECTIVE

Operational Fit

The underlying issue is rarely that these tools are inherently bad; rather, the challenge lies in the operational fit.

All shared experiences are anonymised practitioner accounts, not vendor or partner marketing material - I have no dog in that fight.

DOMAIN CONTEXT

Enterprise Scope

The context stems from varied practitioner experience navigating the GDPR, the AI Act, the Digital Services Act (DSA), and various other governance implementations across complex enterprise environments, in the public and private sector.

Part 1: How We Got Here

The Post-GDPR Privacy Tech Boom

2018 - DEADLINE DRIVEN

Compliance Surge

The 2018 GDPR implementation created an unprecedented compliance deadline, spawning an entire privacy management market almost overnight. Budget allocations were largely driven by fear of substantial regulatory fines.

EXPANSION AND M&A

Platform Consolidation

GRC platforms grew rapidly through aggressive acquisitions, quickly expanding their footprint into privacy management from elsewhere, or beyond core privacy management into ethics, ESG, and third-party risk management.

STRUCTURAL MISMATCH

Tooling Precedes Process

Complex enterprise tooling arrived well before organisations had mature, established processes to actually procure - let alone govern - these tools, forcing operational teams to adapt their workflows to the software.

Part 1: How We Got Here

Same Playbook, New Buzzwords

Every privacy/GRC vendor pivoted to 'AI governance'

Legacy vendors and new entrants alike rushed to rebrand existing compliance features to capture expanding AI risk management budgets - similar expansions are seen in other geos and related digital regulations.

01 / ‘MARKET LEADERS’

OneTrust: Visionary in Gartner's first AI Governance MQ (2026)

Leveraged its massive market footprint to quickly position existing data inventory tools for AI model tracking.

02 / GRC EXTENSION

Riskonnect bolted AI risk onto its GRC platform (July 2025)

Integrated AI risk indicators directly into established enterprise risk management and audit modules.

03 / AI AS ‘EASY MODE’

TrustArc launched 'Arc' - an 'AI easy button' for privacy

Provided streamlined assessment templates targeted at privacy officers facing increased oversight demands.

04 / PURE-PLAY STARTUPS

Purpose-built AI GRC startups (Credo AI, Trustible, etc.) pile in

Niche entrants offering continuous model evaluation, algorithmic fairness auditing, and automated AI compliance.

CRITICAL MISMATCH

Structural Governance Mismatch

Even competing vendors acknowledge that adding AI modules to legacy platforms results in a "bolted-on" architecture.

Reduces critical AI governance to an inadequate point-in-time questionnaire.

Part 2: Four Failure Modes

Failure Mode 1: The Bolt-On Problem

Static governance frameworks cannot support dynamic, high-velocity AI model and tool lifecycles.

Legacy GRC Tools	Dynamic AI Systems
Static Paperwork	Continuous Retraining
Fundamentally designed for point-in-time, static documentation.	Models continuously experience retraining and drift post-deployment.
ASSUMED SYSTEM STATE	**OPERATIONAL LIFE-CYCLE**
Fixed Operational Scope	Expanding Scope
Assumes code base and privacy parameters remain unchanged once reviewed.	Data flows and model applications evolve dynamically in real-time environments.
GOVERNANCE OUTCOME	**GOVERNANCE REQUIREMENT**
Annual Checklists	Continuous Oversight
Treats compliance as a periodic, manual paperwork exercise.	Demands automated, high-velocity, real-time risk management.

Part 2: Four Failure Modes

Failure Mode 2: The Consolidation Trap

"One fewer vendor" — procurement loves it, practitioners inherit it.

FAILURE MODE BREAKDOWN

Platform Fragmentation & The Human ETL Layer

01 / ARCHITECTURAL INCOMPATIBILITY

Modules built by acquisition often feature incompatible data models, making cross-module reconciliation a tedious manual process.

The resulting platform fragmentation is frequently worse than using separate tools.

02 / LICENSING & COST ESCALATION

Adding privacy/AI governance to an existing GRC/privacy license appears to be a consolidation win on paper.

In practice, costs escalate rapidly as modules and usage expand while practitioners serve as the human ETL layer.

Part 2: Four Failure Modes

Failure Mode 3: Lock-In and Renewal Economics

01

Proprietary Formats & Data Captivity

Your ROPA, assessments, and historical compliance records live in proprietary formats.

02

Opaque Pricing Models & Renewal Shock

Platforms utilise quote-only pricing models with module-based expansion, leading to documented patterns of renewal price shock.

03

High Switching Barriers & Hostage Records

High switching costs are paid in loss of historical audit trails rather than just subscription fees. Vendor lock-in becomes an intentional business model - the system bought to evidence compliance effectively holds compliance records hostage.

FAILURE MODE 04

The Tool Becomes the Job

PRIMARY IMPACT

(Human) Bandwidth Consumption

Practitioners become dedicated platform administrators rather than governing data and AI risk.

Part 2: Four Failure Modes

ADMINISTRATIVE OVERHEAD

Complex platforms require months-long implementations and heavy consultant involvement. Ongoing administration quickly becomes a dedicated standing role, forcing privacy and governance teams to maintain the platform instead of governing data.

CAPACITY & RISK MISALIGNMENT

Small teams end up paying for enterprise sophistication they lack the capacity to operationalise, spending valuable governance bandwidth managing the tool's operation rather than mitigating organisational risk.

Time Before Value: Implementation & Administration Overhead

Reviews report multi-month implementation timelines before privacy teams experience operational benefit.

3 Months

OneTrust Privacy Automation

Average implementation timeline (industry reported)

2 Months

OneTrust Tech Risk & Compliance

Average implementation timeline (industry reported)

Practitioner Friction & Ongoing Maintenance

Practitioners report substantial upfront and ongoing configuration burdens, spending weeks setting up and mapping workflows and schemas.

Sunk Cost Lock-In

This very cost, in time and money, adds considerable friction to any discussion of reevaluating or replacing a tool or vendor

PART 3: PRACTITIONER INSIGHTS

War Stories

Real-world, anonymised practitioner experiences and operational challenges encountered in data and AI governance.

Illustrative accounts reveal the practical friction, implementation hurdles, and unexpected overhead faced by organizations navigating enterprise vendor ecosystems.

Case Study: OneTrust as a Practitioner

01

Sales Promise vs. Operational Reality

What you were sold vs. what you got - unsuitability can reveal itself post-deployment

02

Implementation Friction

Implementation/configuration pain points, differ by organisation but normally there

03

Commercial Trajectory

Module cost escalation or intransparent renewal spike

04

Cost and Complexity of Fine-Tuning

How and how much it takes to get a tool that works for your organisation

05

Data Architecture Mismatch

The ROPA / assessment data model vs. organisational reality

06

AI Governance Module

AI governance module experience - mapping to actual model risk

BALANCED TAKEAWAY

Credit where due for scale and DSAR automation capabilities.

PRACTITIONER EVALUATION

Case Study: Training as a Compliance Tool

01

Geographic Focus - Global Course for Local Need

Early days of the GDPR gold-rush meant a lot of global generic privacy and GRC training was sold as GDPR-specific

02

Dominant Players, Network Effect

Though the EU (cleverly) avoided rubber-stamping particular trainers, IAPP dominated in-practice

03

Proliferation of Certifications

The sudden increase both in courses available and those who have completed them, makes rating them difficult

04

CPD - The Quality Paradox

Quality, and the perception thereof, can be negatively impacted by none or by clear commercial incentive

05

The ‘Tick Box’ Reputation

Streamlined, widely accepted vendor solutions tend to favour minimally disruptive tick-box approaches

06

Cultural Approach to Governance

Legacy and dominant providers de facto drive culture

BALANCED TAKEAWAY

A Common Baseline

Acknowledging challenges in the details, IAPP does provide a universally recognised baseline and a shared professional vocabulary for diverse teams to align on core privacy and governance standards.

PART 4: WHAT WOULD BETTER LOOK LIKE?

Principles, not product recommendations

This section outlines core architectural and operational principles for right-sizing and better procurement in data and AI governance.

Focusing on pragmatic strategy over vendor-driven software selection to build sustainable, adaptable frameworks.

Principles for Choosing (or Surviving) Tooling

01 **Map your workflows and needs** before you demo anyone's software

02 **Buy for your team's actual size,** not your future ambition

03 **Demand data portability** in the contract, not just the brochure

04 **Prefer purpose-built over retrofitted tools** where regimes differ

05 **Fund the humans;** a tool without a dedicated owner is shelfware

CORE AXIOM **Buy the tool, don’t let the tool buy you.**

PROCUREMENT CHECKLIST

Rethinking Vendor Vetting

Move past standard vendor marketing demos with high-visibility criteria designed for data and AI system governance.

Better Questions for Procurement

01 What is the total cost including implementation, admin, and multi-year renewals?

02 Have we given real consideration to options beyond the top 1-3 market dominant vendors?

03 Who at the vendor is accountable when modules or data structures change?

04 How does this specific tool handle a model or system that updates monthly?

05 What does a real implementation timeline look like based on customer references?

06 Can we run a paid pilot on OUR actual workflows rather than THEIR demo data?

Caveats & Nuance

01 / Enterprise Value

Legitimate Vendor Strengths

- These platforms do real things well at enterprise scale (e.g., cookie scanning, high-volume DSAR automation, regulatory intelligence).
- Consolidated record-keeping genuinely assists with complex regulatory audits.
- Can be the only hope for particularly small teams.

02 / Market Reality

Pragmatism & Marketing

- Look first to who you have in-house, or could bring in-house.
- Vendors criticising other vendors is also marketing - maintain healthy skepticism.
- The lack or weakness of bespoke solutions won’t be solved until the market prefers them.

Field Talk - 17 November 2026

Takeaways & Closing Discussion

01

Tools amplify existing process; they cannot substitute for missing process

02

Post-GDPR sales patterns are repeating in AI governance; at an accelerated pace

03

Vendor lock-in is a fundamental data problem before it becomes a financial problem

04

Allowing tool maintenance to become the primary job is a quiet operational failure

05

Demand data portability early; evaluate system dynamics constantly

THANK YOU

QUESTIONS OR COMMENTS WELCOME