How xtype Automates Compliance Reporting

For Highly-Regulated ServiceNow Customers

Why regulated enterprises struggle to extract regulatory, risk and compliance data from ServiceNow and how xtype's native cross-instance Compliance Automation platform eliminates the pain of reporting.

BY

Dan Schoenbaum
EVP, Compliance Solutions

Part One

The Compliance Reporting Crisis

A ServiceNow estate built for service delivery is now being asked to answer questions it was never designed to answer at audit speed, across every instance, and on a regulator's clock.

Compliance Data Lives In Servicenow

Getting it out is another story

For highly-regulated enterprises running ServiceNow, regulatory, risk and compliance reporting has become one of the most difficult and expensive challenges customers face. Organizations across healthcare, life sciences, financial services and many other industries are spending millions of dollars and thousands of staff hours trying to extract, reconcile and present compliance data, often from multiple ServiceNow production instances that were never designed to work together.

As ServiceNow utilization deepens across the largest enterprises, multi-instance reporting was never a known challenge at the time of implementation. Meanwhile, the regulatory landscape evolves rapidly, putting ever more pressure on organizations to produce robust data and reporting on demand.

At one global financial services company, the journey began in 2018 when GDPR went into effect. A single compliance analyst was tasked with building the organization's first data privacy compliance framework from scratch by attending conferences, building manual spreadsheets and learning the regulation in real time under enormous pressure. What started as one policy and a handful of reports has since grown into an enterprise-wide compliance operation spanning multiple regulations, regions and hundreds of reports.

The pattern is the same everywhere: **compliance starts small, compounds quickly, and overwhelms the teams and systems that were never built to handle either the scale or the complexity.**

> **xtype Perspective**
>
> The problem isn't that ServiceNow lacks compliance data, it's that cross-instance reporting and governance aren't provided out of the box. That's the layer regulators are now asking about, and the layer xtype was purpose-built to deliver.

By the Numbers – A Preview of What's Ahead

~2,000
REQUESTS / YEAR
Regulatory data requests processed by a single $20B healthcare system

3–4 wk
PER AUDIT PREP
Manual stitching across systems and instances for every audit cycle

$2–5M
ON CUSTOM ETL
Industry-wide spend to recreate cross-instance views

What's Inside

Part One frames the crisis. Part Two shows what it does to the platform team. Part Three explains why ServiceNow GRC can't close the gap alone – including a new failure mode emerging from AI agents. Part Four shows how xtype turns compliance into a property of the platform itself.

The Three Problems

Volume, Cost & Access

The Volume Problem

The sheer volume of regulatory, compliance and risk requests is staggering. The numbers from enterprise ServiceNow customers paint a clear picture:

- **A major healthcare organization** ~100 regulatory requests per month for security metrics alone – over 1,200 per year, costing several million dollars annually to service.
- **A large financial services firm** with six ServiceNow instances produced 112 compliance reports in 12 months – half net-new – at 2–3 months per custom report.
- **A $20B healthcare system** processes ~2,000 regulatory data requests per year, with 40% of staff time consumed by fulfilling them.
- **A global financial services company** manages compliance across five regions and frameworks (GDPR, CCPA, LGPD, PCI DSS), with 120+ ServiceNow compliance reports created over eight years.

The Cost Problem

Compliance reporting costs extend far beyond staff time. Enterprises are paying for:

- **Custom ETL pipelines:** $2–$5 million industry-wide attempting to build cross-instance data extraction and transformation.
- **Licensing overhead:** Compliance teams forced to buy access to data inside Business Continuity Management, IRM and similar modules.
- **Audit preparation:** 3–4 weeks per audit. The FDA requires 24–48 hour turnaround during which teams stitch data from multiple systems by hand.
- **Regulatory penalties:** Strict liability regulations at $142,000 per incident across 10+ state-level frameworks.
- **Internal budget politics:** Compliance budgets sit with the CRO or CISO. Divisions negotiate 10–25% annual increases just to fund report customizations.
- **Expertise scarcity:** Compliance-and-platform expertise is hard to obtain internally or from ServiceNow due to competing roadmap priorities.

The Access Problem

Auditors, GRC analysts, risk managers, SecOps and regulatory compliance teams cannot directly access the ServiceNow data they need. Platform owners become a mandatory bottleneck for every request. **The result: regulatory, risk and compliance reporting becomes a costly, time-consuming exercise, not because ServiceNow lacks the data, but because cross-instance reporting isn't available out of the box.** Compliance leaders end up funding custom dashboards, ETL pipelines and GRC workarounds, spending millions to recreate views the underlying data already supports. This is exactly the gap xtype's compliance automation closes.

> "
>
> *Our CISO asks for a regulatory, risk and compliance dashboard and we have no good answer. We pass our audit every 6–12 months, but our business needs to know our compliance posture daily.*
>
> **Enterprise Servicenow & xtype Customer, Life Sciences & Healthcare**

Part Two

The Platform Team Under Siege

Hired to drive modernization. Spending the week pulling screenshots for auditors. The platform team's strategic mandate is being eaten alive by tactical compliance work.

The Inbound Request Overload

While compliance and audit teams struggle to get the data they need, ServiceNow platform owners bear the operational burden of servicing every request. The platform team was hired to drive strategic initiatives such as modernizing workflows, implementing new modules and improving the enterprise's ServiceNow investment. Instead, they're drowning in tactical compliance work.

Based on customer advisory board findings and direct customer conversations, the teams demanding regulatory, risk and compliance data from the platform owner include:

Department	What They Need from ServiceNow
IAM (Identity)	Access is complex, fluid and impossible to manage manually across instances. Traditional security tools don't focus on ServiceNow.
Audit	Risk-based audit planning, control testing evidence and documented approval trails for every change.
GRC	Plug-in data across multiple instances; GRC modules are not multiinstance enabled and do not report against standard controls.
Risk	Risk-based audit planning, control testing and continuous evidence collection.
SecOps	Change records, access logs, incident response data and remediation tracking.
Regulatory Compliance	Framework-specific evidence for GxP, 21 CFR, DORA, SOX, NIS2 and more
Information Management	Data-at-rest compliance and access controls across acquired instances
SQA	Quality system validation and batch record access governance.

When priorities collide

While the platform team services these inbound requests, the strategic backlog grows: workflow modernization, AI agent deployment, new module rollouts and instance consolidation all wait, widening the gap between what the business asks for and what compliance leaders can deliver.

Tactical Work Displaces Strategic Work

Every request that lands on the platform team's desk pulls them away from higher-value work. The pattern is consistent across industries:

- **Short turnaround demands:** Audit and compliance teams need data within days – sometimes hours – forcing platform owners to drop both operational and strategic projects.
- **Screenshot requests for attestations:** Auditors frequently need visual evidence – screenshots of configuration settings, access control lists and change approval chains – that require a platform admin to manually navigate and capture.
- **One-off report building:** Custom compliance reports typically take 2–3 months to build, cannot be reused across environments and do not scale with the pace of new compliance mandates. Each audit cycle restarts the same manual process from scratch. Many auditors reject existing reports outright and require their own, creating significant additional burden.
- **Cross-instance reconciliation:** With no native multi-instance reporting, platform owners manually query each instance, export to Excel and reconcile data using VLOOKUPs. This process that can take weeks for a single compliance report.
- **Fragmented semi-automated workflows:** ServiceNow GRC generates lists of which controls to test, but the process fragments from there: compliance teams manually create tracking lists in spreadsheets and SharePoint, generate testing forms, execute tests, then feed results back into custom reports for half-year and year-end reporting to the Head of Compliance, CRO or CISO. Remediation plans live in separate systems entirely, requiring manual consolidation upstream.

One life sciences company reported that **30–40% of compliance staff time** is consumed by servicing inbound data requests. Another healthcare company with 15 ServiceNow developers still cannot keep up with the volume and cannot find additional qualified developers to hire.

The Real Cost

Platform teams are spending millions on workarounds, burning thousands of staff hours, and still can't answer a simple question from their CISO: "Are we compliant across all instances?"

The Departments Pulling on the Platform Team

The platform team isn't fielding requests from one place. They're servicing eight or more functions in parallel, each with its own urgency, framework, and definition of "evidence". Every request resets the queue:

8+
FUNCTIONS IN PARALLEL
IAM, Audit, GRC, Risk, SecOps, Reg Compliance, IM, SQA

15
DEVS INSUFFICIENT
One healthcare company has 15 SN devs – still can't keep up

30–40%
OF STAFF TIME
Lost to servicing inbound regulatory data requests

Part Three

Why ServiceNow GRC Falls Short and Why It Matters More Every Year

Many organizations assume ServiceNow's built-in GRC module should solve their compliance reporting challenges. In practice, GRC was designed as a **risk register, not an evidence engine**. It records controls but does not verify them across instances. **The critical insight:** GRC, IRM, Policy & Compliance, and Audit Management modules are **not multi-instance enabled** because each instance has its own GRC module, policy library, and evidence. The gap is compounded by M&A; one biotech company reported **60% of their multi-instance complexity came directly from acquisitions**.

What GRC Delivers	What Regulated Enterprises Need
Registers risks and controls	Verifies controls are actually enforced across all instances.
Manages third-party vendor compliance	Audits the platform itself – who has access, what changed, are policies passing.
Works within a single instance	Aggregates compliance data across 3–15+ production instances.
Provides policy workflow management	Delivers real-time compliance dashboards with drift alerts.
Requires manual evidence collection	Auto-generates audit evidence packages mapped to SOX, HIPAA, 21 CFR, GxP.

The Regulatory Landscape Is Becoming More Complex

Regulatory pressure is accelerating. **NIS2, OCC, DORA, OCR, FTC and FedRAMP** are pushing enterprises to demonstrate continuous compliance, not point-in-time audit readiness. **FDA 21 CFR Part 11** requires documented access controls, audit trails, validated change control and e-signature integrity continuously. Geography compounds it: CCPA, GDPR, LGPD and PCI DSS each mapped to specific regions and tracked per jurisdiction.

AI Agents Inside ServiceNow: A New Failure Mode

The risk sharpens in a validated pharma instance with an FDA inspection on the calendar. Or in a tier-1 bank under DORA. Or in a healthcare provider with a CCO who reports to the audit committee quarterly. The moment an AI agent commits a change inside one of those instances, six control frameworks can fail simultaneously:

- **GxP §11.10(a)** – change must be validated before reaching a validated instance
- **21 CFR Part 11 §11.10(e)** – independent audit trail, not "the AI logged its own work"
- **SOX ITGC** – separation of duties between developer, reviewer, approver (the AI was all three)
- **DORA Article 9** – traceability to authorization source external to the executing system
- **SOC 2 CC6/CC7** – independent review of changes before production
- **NIST 800-53 CM-3/CM-4** – documented impact analysis

xtype enforces these controls at the platform layer. Every change, human-initiated or AI-generated, passes through cross-instance validation, independent audit trails captured outside the executing instance, and separated approval workflows before it reaches a regulated production environment.

> **xtype Perspective**
>
> *Regulators have moved from sampling to continuous expectation, and AI agents are accelerating the deadline. Compliance has to become a property of the platform, not a project that runs against it.*

Part Four

How xtype Automates Compliance Reporting

Audits become a query, not a project. xtype is already inside every instance requiring no ETL, no new connectors, no waiting on the platform team.

Three Reports That Form a Complete Audit Package

xtype is a ServiceNow Elite Build Partner with native cross-instance access to every ServiceNow production environment. Unlike tools that require new connectors, ETL pipelines or data extraction, xtype is already inside every instance reading governance metadata directly from the platform.

xtype's compliance suite produces three core reports, each building on the data foundation of the one before:

1

Access Certification & SoD

Who has access, and are there conflicts? Identifies orphaned accounts, segregation of duties violations, and privileged access across all instances.

2

Change Authorization Trail

Was every change properly authorized? Validates the full approval chain (from request through CAB review to implementation) and flags broken or self-approved changes. Where change data lives outside ServiceNow, the challenge multiplies, and xtype reaches across that boundary.

3

Control Testing Status

Are compliance controls passing everywhere? Tests that each control is enforced on every instance and produces a board-ready view that replaces the regular "Excel exercise."

3–4 wk → hrs

Audit prep time, collapsed

Auto-generated evidence packages mapped to GDPR, SOX, PCI, ISO 27001, HIPAA and 21 CFR Part 11.

The Benefits of Automating Compliance With xtype

Measurable Wins, End-to-End

xtype's compliance automation platform delivers measurable improvements across every dimension of the compliance reporting problem for the people who own compliance, the people who run the platform, and the enterprise that depends on both.

For Compliance, Risk & Audit Teams

- ✓ **Real-time compliance dashboards**
  Always-on, role-based views of control status, drift alerts, and risk scores. When the CISO asks for compliance status, the answer is a click away.

- ✓ **Automated evidence collection**
  Audit packages mapped to GDPR, SOX, PCI, ISO 27001, HIPAA, and 21 CFR Part 11. Audit prep collapses from 3–4 weeks to hours.

- ✓ **AI-ready change governance**
  Every change (human-initiated or AI-generated) passes through cross-instance validation, independent audit trails and separated developer/reviewer/approver workflows. Satisfies GxP §11.10(a), 21 CFR Part 11 §11.10(e), SOX ITGC, DORA Article 9, SOC 2 CC6/CC7 and NIST 800-53 CM-3/CM-4 simultaneously.

- ✓ **Cross-instance visibility & self-service**
  Every control, every access record, every change trail across all ServiceNow instances is accessible to IAM, Audit, GRC, Risk, SecOps and Regulatory Compliance without filing a request with the platform team.

- ✓ **One report, dual audience**
  Internal stakeholders (CRO, CISO, CEO, ELT, Board) get real-time posture summaries; external auditors get full evidence packages without maintaining separate report sets.

For ServiceNow Platform Teams

- ✓ **Eliminate the request bottleneck**
  Stop servicing hundreds of ad-hoc compliance data requests per month. Stakeholders self-serve through automated dashboards.

- ✓ **Reclaim strategic focus**
  Platform engineers shift back to modernization and innovation, and not screenshots and one-off builds. Reusable report templates replace the quarterly scramble.

- ✓ **No new infrastructure**
  xtype is already inside every instance through its native cross-instance read layer. No connectors, no ETL, no extraction.

For the Enterprise

- ✓ **Reduce compliance reporting costs by millions**
  Eliminate custom ETL pipelines, reduce report-building headcount, and cut licensing overhead for data access.

- ✓ **Lower audit risk & gain predictability**
  Continuous monitoring catches drift before auditors do. Move from reactive, fire-drill audit prep to a proactive, always-ready compliance posture, whether the change came from a developer or an AI agent.

Ready to Modernize Compliance?

Audits become a query, not a project

See how xtype eliminates the compliance reporting bottleneck across your ServiceNow estate, and turns risk, regulatory and compliance reporting into a real-time, always-ready capability.

Book a Demo | **Visit xtype.io**

xtype.io | info@xtype.io

xtype is the automated governance platform for ServiceNow. xtype Enterprise governs every change across the estate in real time. xtype Compliance delivers auditor-ready evidence mapped to the frameworks that matter. Together, what Enterprise governs, Compliance proves. Move fast and stay compliant.