Rezilient

WHITE PAPER

The Shared Responsibility Gap

Why ServiceNow Customers Need Independent Backup for Compliance, Resilience, and AI Governance

A guide for CISOs, CIOs, GRC leaders, and ServiceNow platform owners

Published by Rezilient Corp.
Learn more at rezilient.co

Back Up Now. Restore Anytime. Always Rezilient.

Executive Summary

ServiceNow has become the system of action for the modern enterprise. It orchestrates IT operations, HR, customer service, security response, finance, and increasingly, via Now Assist and agentic AI, thousands of automated business decisions every day. For most Global 2000 organizations, ServiceNow is no longer a ticketing tool. It is a Tier-1, business-critical platform.

That shift creates a new category of risk. When a platform executes the business, the integrity of the data inside it becomes inseparable from the integrity of the business itself. A misfired workflow, a bad upgrade, a rogue integration, or an AI agent acting on stale data can silently corrupt records across ITSM, CMDB, HRSD, and GRC in minutes, often before anyone notices.

The uncomfortable truth for security and compliance leaders is this: ServiceNow operates under a Shared Responsibility Model. ServiceNow protects the infrastructure, the hypervisor, and the platform. The customer, not ServiceNow, is responsible for protecting the data, the configurations, and the compliance evidence inside their instance.

Native ServiceNow backups are available, but they are primarily designed for disaster recovery, retaining only 14 days of weekly fulls and 7 days of differentials, and cannot be used to restore a single corrupted record, field, or workflow without rolling the entire instance back in time.

This paper is written for CISOs, CIOs, GRC leaders, and ServiceNow platform owners navigating a new regulatory landscape including DORA, NIS2, NYDFS Part 500, the EU AI Act, and updated SEC, HIPAA, and FINRA expectations, in which independent, immutable, surgically recoverable backup is no longer optional. It is a control.

What this paper covers

- The Shared Responsibility Model for ServiceNow and where customer accountability begins.
- Why traditional approaches, including platform rollbacks, data warehouse replication, and DIY scripts, fail under modern compliance and AI risk.
- A requirements checklist for compliance-grade backup and recovery.
- How Rezilient Restore closes the gap with immutable, off-platform, surgical recovery; offering a straightforward path to a 30-day PoC pilot.

1. The New Compliance Reality

Over the last 36 months, regulators on both sides of the Atlantic have moved the definition of operational resilience from "best effort" to "provable control." The implication for security and compliance leaders is direct: you can no longer treat the SaaS platforms that run the business as black boxes. You are expected to demonstrate with evidence that the data powering critical workflows is recoverable, immutable, and auditable.

1.1 A shortlist of what has changed

Framework	What it now expects
DORA (EU)	Article 12 requires ICT-related incident recovery with tested backup procedures, segregation from production, and evidence of restore capability for financial entities, including their critical SaaS providers.
NIS2 (EU)	Expanded scope to medium and large entities across 18 sectors, with explicit obligations for backup management, crisis response, and supply-chain security.
NYDFS Part 500 (US)	Section 500.13 mandates secure, segregated data backups and Section 500.16 requires a written incident response and business continuity plan with tested recovery.
EU AI Act	Article 9 (risk management) and Article 12 (logging) require traceability and retention of data used by high-risk AI systems, directly implicating Now Assist and other agentic AI inside ServiceNow.
SEC Cyber Disclosure (US)	4-business-day disclosure of material cyber incidents. Without surgical recovery and an audit trail, material-impact assessments become slow and indefensible.
HIPAA / HITECH	§164.308(a)(7) Contingency Plan requires data backup, disaster recovery, and emergency mode operations for ePHI, which increasingly lives in HRSD, CSM, and workflow records.
SOX (ICFR)	Requires preservation and integrity of financial records and supporting evidence, including configuration and workflow data that governs financial processes.

The common thread across these frameworks is no longer "do you have a backup?" It is "can you prove on demand, with an immutable chain of custody, that you can restore the exact data, configuration, and audit context required to continue operating and to satisfy an examiner?"

1.2 Why ServiceNow is now in scope

ServiceNow is the operational substrate for functions that sit squarely inside these regimes: ITSM incident response, CMDB-driven change management, HR case data (PHI, PII), customer service records, third-party risk workflows, and GRC evidence of control operation. When a regulator asks "show me the state of this control on that date," the answer lives inside ServiceNow, and the burden of proof lives with the customer.

2. The Shared Responsibility Model, Unpacked

Every major SaaS platform, including AWS, Salesforce, Microsoft 365, and ServiceNow, operates on a variant of the shared responsibility model. The headline is always the same: the vendor is responsible for the security and availability of the service; the customer is responsible for what they put into it. In practice, most security leaders understand this for infrastructure-as-a-service. Fewer have internalized it for SaaS platforms of record.

2.1 What ServiceNow owns, and what you own

ServiceNow's responsibility	The customer's responsibility
Physical data center security and availability	Integrity and recoverability of customer data and configurations
Platform uptime, patching, and hypervisor-level resilience	Protection against user error, admin error, and malicious insider action
Infrastructure-level backup for full instance disaster recovery	Granular, record-level, and field-level recovery of business data
Encryption of data in transit and at rest	Retention of backup data beyond the 14-day platform window
Access controls (the mechanisms)	Access policies, entitlements, and evidence of their enforcement
Application code and upgrade delivery	Testing, configuration, and change management inside the instance

2.2 The 14-day native backup window

ServiceNow's native backup provides up to 14 days of weekly full backups and 7 days of differential backups. This window is engineered for infrastructure-level disaster recovery; the scenario in which the platform itself has a catastrophic failure. It is not designed to answer the questions a compliance team actually faces:

- "Show me the exact state of this change record as of 90 days ago."
- "Roll back the 4,200 records this misconfigured workflow corrupted last Thursday, but leave everything else untouched."
- "Prove that this Now Assist–generated decision was based on un-tampered source data."
- "Produce a 7-year retention copy for our regulator, sealed and verifiable."

The core insight

ServiceNow's platform backup is excellent at what it is designed for: rebuilding the service after an infrastructure failure. It was never designed to be the customer's compliance backup. Treating it as such is the most common, and most costly, assumption in the ServiceNow ecosystem today.

3. The Risk Landscape in 2026

Three forces are converging to make SaaS data loss, especially ServiceNow, a board-level concern.

3.1 SaaS data loss is now the norm, not the exception

87%	90%	79%
of organizations experienced SaaS data loss in the past 12 months	of IT professionals reported a SaaS data loss event last year	mistakenly believe their SaaS vendor is fully responsible for backup

These are not storage outages. The dominant root causes accounting for the majority of SaaS data loss events are human error, malicious insiders, misconfigured integrations, and increasingly, automated processes (including AI agents) acting on the wrong inputs. Organizations frequently do not discover the damage until an auditor, a customer, or a failed downstream process surfaces it, weeks or months after the fact.

3.2 The cost curve is steepening

$4.44M	$9,000/min	$400B	2.3x
IBM — global average cost of a data breach	Average enterprise cost of downtime	Annual downtime cost across Global 2000 (Splunk)	More costly when gaps are discovered during an incident vs. prepared

Organizations that invest in independent recovery ahead of time consistently recover faster and cheaper. Mature backup and recovery programs have been measured at up to 45x faster mean time to recovery versus ad hoc, data-warehouse-based recovery attempts.

3.3 AI and automation compound the risk

Agentic AI inside ServiceNow, including Now Assist, virtual agents, and workflow studio automations, has changed the blast radius of a single bad decision. An AI agent can touch thousands of records in seconds, across CMDB, HR cases, customer records, and GRC evidence. If the inputs are stale, poisoned, or misinterpreted, the output is a silent, platform-wide integrity event. Gartner forecasts that by 2028, roughly 75% of enterprises will experience a material AI-related data loss or integrity event.

4. Why Traditional Approaches Fall Short

Most ServiceNow customers already have something they call "backup." In practice, it is usually one of four patterns, some of which was valuable for its original purpose, but each of which leaves a meaningful compliance and recovery gap that could result in data loss and expensive downtime.

4.1 Relying on ServiceNow's platform backup

As covered in Section 2, platform backup is infrastructure disaster recovery. It does not support record-level restore, is limited to 14 days, and cannot be used as the legal system of record for compliance retention. Rolling an entire production instance back to "yesterday" to recover a single corrupted table is operationally untenable, every other team working in that instance loses a day of work.

4.2 Existing tools & partial solutions

Tools like SnowMirror, Perspectium, and native data export jobs are excellent for analytics, BI, and reporting. They are not backup. Standard relational databases and warehouses are mutable by design; an admin, a schema change, or a broken pipeline can alter or drop data without a chain of custody. When a corruption event occurs, recovery becomes a custom SQL engineering project: diff the warehouse against production, write reconciliation scripts, test them against a non-production instance, and manually re-import. It is neither surgical nor auditable, and it exposes the compliance team to mutable, non-tamper-evident evidence.

4.3 Custom solutions that export to a data warehouse or data lake

Strong engineering teams can write custom scripts against the ServiceNow Table API to extract data. The initial build is not the hard part, the maintenance is. A compliance-grade backup and recovery system needs to handle schema evolution, biannual ServiceNow upgrades, custom tables, reference field integrity, attachment handling, immutability guarantees, key management, retention policy enforcement, audit logging, legal hold, and the workflow for surgical restore. Industry estimates place sustained engineering investment at 6–18 months for an initial custom build, with a recurring tax of 20-40% of an FTE to maintain. In nearly all cases, that engineering capacity is better spent on platform modernization and on the core business.

4.4 Doing nothing

The most common posture, ”we haven't lost data yet”, is increasingly difficult to defend. 79% of IT and security leaders operate under a mistaken mental model of who is responsible for SaaS data protection. The organizations that discover the gap during an actual incident pay, on average, 2.3x more to recover than those who were prepared. In a post-DORA, post-SEC-disclosure environment, "we assumed ServiceNow had it" is not a control narrative that holds up in front of a regulator or a board.

Reframing backup

Backup is no longer insurance against downtime. It is the evidence layer that proves the business is in control of its own data, whether to regulators, to auditors, to the board, and increasingly to its customers. The question is not whether you have a backup. It is whether you can defend it.

5. Requirements for Compliance-Grade ServiceNow Backup

Based on conversations with security, compliance, and ServiceNow platform leaders at regulated enterprises, the following seven requirements consistently separate a compliance-grade backup program from a nice-to-have data copy.

5.1 Immutable and off-platform

Backups must be stored outside the ServiceNow instance and outside the control of any single administrator, on storage that is tamper-evident and write-once (WORM). This is a baseline expectation under DORA, NYDFS 500.13, and most modern audit frameworks. It also neutralizes the insider-threat and ransomware-in-SaaS scenarios.

5.2 Continuous and schema-aware

Nightly exports are insufficient when AI-driven workflows can touch thousands of records per minute. Backup must run continuously, capture every change, and follow ServiceNow schema evolution automatically, including custom tables, reference fields, and application-specific extensions (HRSD, CSM, ITOM, GRC, SecOps, Now Assist).

5.3 Surgical, record- and field-level recovery

A compliant recovery capability must allow you to restore an individual record, a specific field, a workflow state, or a defined set of records affected by an event, without disturbing adjacent data or requiring a full instance rollback. This is the single largest operational gap in platform-native backup.

5.4 Defensible audit trail and chain of custody

Every backup, every retrieval, every restore, and every access to backup data must be logged, signed, and produced on demand in a format that an auditor or examiner will accept. "We have backups" is a posture; "here is the signed, time-stamped chain of custody for the restore that resolved incident #4712" is evidence.

5.5 Retention aligned to the regulation, not the platform

HIPAA requires 6 years. SOX typically 7. FINRA Rule 4511 requires preservation of business records for 6 years. DORA imposes long-horizon reconstructability for critical services. Backup retention must be configurable per table or record type to match the regulation that governs it, not capped at the platform's 14-day operational window.

5.6 AI governance: reversibility and traceability

For every agentic AI action inside ServiceNow, the organization should be able to answer three questions: what data did the model see, what did it change, and can we reverse it cleanly? This is now table stakes under the EU AI Act and is rapidly becoming so under sectoral regulators in financial services and healthcare.

5.7 Native experience and low operational drag

A backup solution that requires its own console, its own admin team, and its own training is a solution that gets underused. Compliance-grade backup should be operable from within the ServiceNow experience your platform team already knows, with the data and controls visible to the people who are accountable for them.

6. How Rezilient Restore Closes the Gap

Rezilient Restore is a purpose-built backup and recovery layer for ServiceNow, designed around the seven requirements above. It sits off-platform, captures every change immutably, and gives operational and compliance teams a way to prove, and, when necessary, to undo any change inside the instance. Full product detail is available at rezilient.co.

6.1 Core capabilities

Capability	What it does	Why it matters
Continuous Backup	Change-level capture of every table, record, and configuration change across the instance.	Eliminates the 14-day ceiling and the nightly-snapshot blast radius.
Precision Recovery	Restore at the table, row, or column level, without a full instance rollback.	Resolves the single largest operational failure mode of platform-native backup.
Schema-Aware	Automatically follows ServiceNow schema changes, custom tables, and application-specific data models.	No manual re-mapping after every upgrade or customization.
Immutable, Off-Platform Storage	WORM-grade, tamper-evident storage outside the ServiceNow instance and outside single-admin control.	Meets DORA, NYDFS 500.13, and ransomware-resilience expectations by default.
Audit-Ready Retention	Configurable retention per table (e.g., 7 yrs for financial records, 6 yrs for ePHI).	Turns backup into usable compliance evidence, not just a file.
AI Governance Layer	Records the pre- and post-state of every change made by Now Assist and workflow automation with point-in-time reversibility.	Directly supports EU AI Act traceability and sectoral AI oversight expectations.

Capability	What it does	Why it matters
Native UX & Alerting	Operates within the ServiceNow experience your platform team already uses; configurable alerts for drift, bulk change, and anomalous activity.	Minimizes operational drag and increases actual usage.

6.2 How it fits into the Shared Responsibility Model

Rezilient Restore is not a replacement for ServiceNow's platform backup. It is the customer-side control that the Shared Responsibility Model assumes you have. ServiceNow continues to handle the platform; Rezilient handles the data, the evidence, and the recovery workflow that the regulation requires.

6.3 Military-grade Encryption & Data Privacy

The third architectural choice that defines Rezilient Restore — alongside off-platform storage and immutability — is zero-knowledge encryption with customer-held keys.

Every record, field, attachment, and configuration captured from your ServiceNow instance is encrypted at rest using AES-256 — the symmetric algorithm specified by NIST FIPS 197 and accepted as the cryptographic baseline by NYDFS Part 500.15, GDPR Article 32, DORA, OSFI B-13, and U.S. federal data-protection programs. The encryption keys are supplied and held by the customer. Rezilient never sees them, never stores them, and cannot derive them.

The practical implication is direct. If Rezilient's backend were ever compromised — by an external attacker, a malicious insider, or a third-party order for compelled production — the data the attacker reaches is mathematically unreadable. Rezilient itself cannot decrypt, search, index, or model your data. The chain of custody we produce for compliance evidence remains verifiable; the underlying data stays sealed to everyone but you. Your data is restorable on demand by you, and only by you.

For a regulated buyer, this collapses several lines of risk into a single architectural decision. It satisfies cryptographic-control requirements across the regimes mapped in §1 without bolt-on tooling. It removes Rezilient as a confidentiality dependency from your data-protection model. And it aligns directly with the data-sovereignty expectations of Canadian, EU, UK, and APAC supervisors. Your auditor does not have to take our breach posture on faith.

6.4 Business outcomes

- **Always-On Protection:** continuous capture closes the gap between incident and last-known-good state.
- **Targeted Recovery:** no full instance rollback; no collateral damage to other teams.
- **Full System Fidelity:** records, configurations, attachments, reference integrity restored together.
- **AI Governance:** reversibility & traceability for automated and AI change inside the instance.
- **Defensible Compliance:** immutable storage and retention aligned to the regulation.

7. Addressing Common Objections

Security and compliance leaders reasonably push back on any new layer in the stack. The five objections below are the ones we hear most often from CISOs, CIOs, and GRC leaders evaluating Rezilient.

1. "ServiceNow already backs up my data."

ServiceNow's platform-level backup is engineered for infrastructure disaster recovery and retains only 14 days. It cannot surgically restore a single record, field, or workflow without rolling the entire instance back in time — which disrupts every other team sharing the instance. Compliance retention, surgical recovery, and AI governance evidence require a dedicated, independent data layer.

2. "We've never suffered a data loss or corruption."

Nearly 90% of IT professionals reported a SaaS data loss event in the past year, and organizations frequently don't realize data is missing until an auditor asks for it. Organizations that discover gaps during an active incident pay 2.3x more to recover than those that were prepared. And under DORA, NIS2, and the EU AI Act, independent backup has moved from insurance to a legal compliance control.

3. "We already back up into a data warehouse."

Data replication is excellent for BI and reporting, but it is not purpose-built backup. Warehouses are mutable by design and cannot provide the immutability, chain of custody, or surgical restore workflow that regulators expect. Recovering from replicated data is a custom SQL engineering project, not a recovery procedure.

4. "We'll build it ourselves."

Most engineering teams can script an initial extract. The cost is in sustained maintenance through ServiceNow's biannual upgrades, schema changes, and every new compliance requirement. A credible build is 6–18 months of sustained engineering plus an ongoing operational tax. Rezilient delivers an enterprise-grade, compliance-ready capability in days — freeing engineering to work on the core business.

5. "We don't have budget for a separate solution this cycle."

The cost of downtime ($9,000 per minute on average for large enterprises; $400 billion annually across the Global 2000) dwarfs the cost of prevention. A single material incident can move a company's share price by up to 9%, and organizations without demonstrable resilience face materially higher regulatory fines. You do not need approved budget today to begin: a 30-day Proof-of-Concept pilot in a non-production environment lets you experience Rezilient Restore, and build an internal case, before committing.

8. Getting Started — The Rezilient Restore Pilot

The fastest way to validate Rezilient against your environment is the Rezilient Restore Pilot: a structured, no-commitment 30-day program in a non-production ServiceNow instance. The pilot is designed to produce real evidence for a real buying decision, not a slide deck.

What the pilot covers

- Connection to a non-production ServiceNow instance (sub-prod, dev, or clone of prod) in under one business day.
- Continuous, schema-aware backup across any selected tables, whichever are relevant to your use case.
- At least three live recovery scenarios of your choosing (e.g., full table restore, row-level restore, or column or field level restore).
- Compliance evidence pack: retention policy walkthrough, regulator-ready audit trail, and backup & restore activity reports.
- A joint readout at day 30 with your platform, security, and compliance stakeholders.

What you will be able to demonstrate

- A defensible answer to the Shared Responsibility question from your next audit or board review.
- Measured mean time to recovery for surgical restores in your own environment, not a vendor benchmark.
- A working AI governance control for Now Assist and agentic workflows, mapped to your regulatory obligations.
- An internal business case grounded in your own data, not projections.

Next step

Visit **rezilient.co** to request the Rezilient Restore Pilot, or share this paper with your ServiceNow platform owner, CISO, or GRC lead to start the internal conversation.

Who should be in the room

A successful pilot typically includes representation from four groups: the ServiceNow platform owner (often a platform architect or VP of IT operations), the security leader responsible for SaaS risk (CISO or deputy), a GRC or compliance representative for the regulations most material to your business, and where relevant, the AI governance or data governance lead responsible for Now Assist and agentic automation.

Appendix A. Compliance Mapping Summary

The following table summarizes how Rezilient Restore capabilities map to the obligations most commonly cited by security and compliance leaders evaluating ServiceNow data protection.

Obligation	Requirement	How Rezilient addresses it
DORA Art. 12	Tested backup and restore, segregation from production, evidence of recovery capability.	Off-platform, immutable backup with documented, testable surgical restore.
NIS2	Backup management and crisis response controls across expanded sectors.	Continuous capture, defined RTO/RPO playbooks, and evidence exports.
NYDFS 500.13	Secure, segregated backups of nonpublic information.	WORM-grade, off-platform storage outside single-admin control.
EU AI Act Art. 9 & 12	Risk management and logging for high-risk AI systems.	Pre/post-state capture for every agentic AI action, with reversibility.
SEC Cyber Disclosure	Timely, defensible impact assessment.	Point-in-time data state for scoping material impact within disclosure windows.
HIPAA §164.308(a)(7)	Contingency planning, data backup, disaster recovery, emergency mode for ePHI.	Retention and restore for HRSD and workflow data handling ePHI.
SOX (ICFR)	Preservation and integrity of financial records and supporting evidence.	Immutable retention of financial-process workflow and configuration data.
FINRA Rule 4511	6-year preservation of business records.	Per-table retention policies aligned to record class.

Appendix B. Sources and Further Reading

- IBM Security, Cost of a Data Breach Report; Gartner research on AI and data governance risk.
- Spanning / Kaseya, State of SaaS Data Protection; Splunk, The Hidden Costs of Downtime.
- EU DORA (Regulation 2022/2554), Articles 11–14; NIS2 Directive (Directive 2022/2555).
- EU AI Act (Regulation 2024/1689), Articles 9 and 12; NYDFS Cybersecurity Regulation, 23 NYCRR Part 500.
- HIPAA Security Rule, 45 CFR §164.308(a)(7); FINRA Rule 4511 — General Requirements for Books and Records.

About Rezilient — Rezilient provides purpose-built, compliance-grade backup and recovery for ServiceNow, with immutable off-platform data, surgical restore, and an audit trail regulators will accept. Learn more or request a pilot at **rezilient.co**.

Back Up Now. Restore Anytime. Always Rezilient.