COMPLIANCE DATASHEET

NIST and Your ServiceNow Data

How Rezilient Restore helps organizations back up, recover and evidence ServiceNow data under NIST CSF 2.0 and SP 800-53 Rev. 5.

NIST CSF 2.0 · SP 800-53 REV. 5 | PR.DS-11, RC.RP-03 · CP-6, CP-9, CP-10 | MAPPED TO REZILIENT RESTORE

WHY SERVICENOW IS IN SCOPE

Backups created, protected, maintained and tested

The NIST Cybersecurity Framework 2.0 is the common language for cyber risk in the United States, and SP 800-53 is the control catalog behind many state and local government programs, contractors and financial institutions. Both put backup and recovery in plain terms.

Teams that run on NIST often run incidents, changes, vulnerabilities and assets on ServiceNow. ServiceNow protects the platform, and its native backup is built for infrastructure disaster recovery, with a 14-day window and full-instance restore. The backup and recovery control for that data is yours.

> "Backups of data are created, protected, maintained, and tested".
>
> NIST CSF 2.0 · PR.DS-11

Feb 2024

CSF 2.0 published, with backups as outcome PR.DS-11.

NIST CSWP 29

All baselines

CP-9 System Backup and CP-10 Recovery sit in the low, moderate and high baselines.

NIST SP 800-53B

14 days

ServiceNow's native backup window, built for platform disaster recovery.

ServiceNow platform documentation

REQUIREMENT TO CAPABILITY

Contingency planning family · continued on page 2

REFERENCE	NIST REQUIREMENT	REZILIENT RESTORE CAPABILITY
CSF PR.DS-11	**Create and protect backups** Backups of data are created, protected, maintained and tested.	**Continuous capture, stored off the platform.** Every change to protected tables is captured and kept in immutable storage outside the instance.
SP 800-53 CP-9	**Back up at a set frequency** Back up user-level and system-level information and system documentation at frequencies you define.	**Frequency you set.** Capture is continuous, so frequency supports any recovery point objective you write down.
SP 800-53 CP-9(1)	**Test backup integrity** Test backup information to verify media reliability and information integrity.	**Restore tests you can actually run.** Record, field or table restore in a non-production instance, with the result exported as evidence.
SP 800-53 CP-9(8)	**Encrypt the backups** Cryptographic mechanisms to prevent unauthorized disclosure and modification of backup information.	**Keys stay with you or ServiceNow.** AES-256 (NIST FIPS 197) in transit and at rest, with keys held only by you or ServiceNow. Rezilient can never read your data.
SP 800-53 CP-6	**Store it separately** An alternate storage site for backup information, separated from the primary site.	**An independent, off-platform copy.** WORM-grade storage outside the instance and outside single-administrator control.

REQUIREMENT TO CAPABILITY, CONTINUED

CP-10, RC.RP-03 and SA-9

REFERENCE	NIST REQUIREMENT	REZILIENT RESTORE CAPABILITY
SP 800-53 CP-10	**Recover to a known state** Recovery and reconstitution to a known state, consistent with recovery time and recovery point objectives.	**Undo the change, not the instance.** Restore records, fields or tables to a known point in time without rolling back everyone else's work.
CSF RC.RP-03	**Verify before you restore** The integrity of backups is verified before they are used for restoration.	**Pre-state and post-state for every record.** See exactly what a record looked like at the restore point before you restore it.
SP 800-53 SA-9	**Oversee external services** Providers of external system services meet your security requirements, and you monitor their compliance.	**Closes the shared responsibility gap.** ServiceNow protects the platform. Rezilient gives you an independent copy of the data inside it.

Four questions an assessor could ask

Q1
Frequency
What backup frequency did you define for ServiceNow under CP-9, and how does it support your recovery point objective?

Q2
Testing
When did you last test ServiceNow backup information for integrity, and what did the restore show?

Q3
Separation
Where is the alternate storage site for ServiceNow backups, and is it outside the reach of the platform's own administrators?

Q4
Known state
Can you recover a corrupted table to a known state without reconstituting the whole instance?

How it works

01
Connect
Install in ServiceNow and link off-platform storage. Live in under one business day.

02
Capture
Continuous, schema-aware change capture across ITSM, CMDB, HRSD, CSM, GRC, SecOps and custom tables.

03
Restore
Record, field, table or workflow level, inside the native ServiceNow experience.

04
Prove
Chain-of-custody exports and audit-ready evidence on demand.

Enforcement screen. Regulators have announced 3 public actions and settlements that cite NIST CSF / SP 800-53 against 3 organizations we have confirmed as ServiceNow customers, about $11 million in total (2025 to 2026). These are evidence of regulatory exposure, not a claim that ServiceNow data was involved. Source: Rezilient review of public regulator records, 31 Oct 2026.

What this datasheet does not claim. No product makes an organization NIST compliant on its own, and CSF is a framework of outcomes rather than a certification. Rezilient Restore supports the backup, recovery, testing and cryptographic controls in the contingency planning family for the data in ServiceNow. Governance, access control, supply chain risk and the other control families remain part of your wider program.

Run a real restore test in 30 days

The 30-day Rezilient Restore trial runs in your non-production instance, live in under one business day, with no commitment. You keep the evidence.

Back Up Now →

rezilient.co/contact-us

Requirement text is summarized from NIST CSWP 29 (CSF 2.0, February 2024) and NIST SP 800-53 Rev. 5; quoted text is verbatim. This datasheet is for information only and is not legal advice. ServiceNow and Now Assist are trademarks of ServiceNow, Inc. © 2026 Rezilient Corp. · Naples, FL · info@rezilient.co · rezilient.co/compliance/nist · v1.4 · 2 / 2

Back Up Now. Restore Anytime.
Always Rezilient.