Best practices for moving from compliance to sustained control in ServiceNow

Welcome! We're glad you're here.

MAY 12, 2026

flexera

Agenda

1. Why ServiceNow data quality matters now
2. Why compliant reports can still hide risk
3. Why ServiceNow data quality breaks down between audits
4. Why cleanup and dashboards are not enough
5. Five governance practices for better ServiceNow data quality
6. How trusted data improves ServiceNow outcomes

flexera

Meet your speakers

James Dalley
Director, Solutions Success

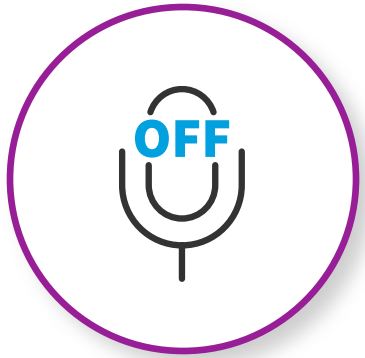
Flexera

Clayton Starko
Director, Solutions Architecture

Flexera

Before we begin

This session is being recorded. After the webinar, we will share a link to the recording, along with any relevant materials.



All attendee microphones and video cameras are turned off.

We encourage you to ask questions! Please type them into the Q&A box at any time during the presentation.

Missed the last three sessions? Here's a quick recap

1

Best practices for building trusted data foundations

Watch on-demand

2

Best practices for managing ITAM risk when ITSM is the foundation

Watch on-demand

3

Best practices for making ServiceNow execution-ready for AI and automation

Watch on-demand

ServiceNow Knowledge confirmed the shift

AI is moving from insight to action

What ServiceNow made clear

Agentic AI is becoming the new operating model

AI is moving from answering questions to recommending, prioritizing, and executing work.

ServiceNow wants to be the system of action

Workflows, approvals, policies, and automation are being positioned as the execution layer for enterprise AI.

AI governance is becoming a control issue

AI Control Tower, Workflow Data Fabric, and governed automation all depend on trusted, contextual data.

Data quality is the limiting factor

If the underlying technology data is stale, incomplete, duplicated, or missing ownership and risk context, AI-driven action becomes risky.

Why Flexera is best positioned to help

Flexera provides the trusted technology intelligence ServiceNow needs to act with confidence.

Source evidence across hardware, software, SaaS, cloud, usage, ownership, and lifecycle

Normalization and reconciliation to reduce duplicate, conflicting, and tool-specific data

Commercial and risk context including cost, license exposure, lifecycle, vulnerability, and business impact

Governed integration into ServiceNow so trusted data can support workflows, decisions, remediation, and AI readiness

Bottom line - ServiceNow can drive the action. Flexera helps make the action trustworthy.

flexera

Poll

With ServiceNow's focus on AI agents and automation, how ready is your data?

Why ServiceNow data quality matters now

Compliance is getting harder to prove

Point-in-time reports do not always reflect the real state of the environment.

AI raises the cost of bad data

Automation can scale the wrong action if the underlying data is incomplete or stale.

Manual cleanup does not scale

Audit prep may fix symptoms, but it does not create sustained control.

Hybrid IT keeps changing

Software, SaaS, cloud, devices, and ownership shift faster than static governance can keep up.

Why ServiceNow reports can look compliant while risk still exists

Compliance reports can show status, but they do not always prove control.

Hidden risk remains when the data behind the report is stale, incomplete, duplicated, or missing business context.

Stale or incomplete Cis
Records exist, but they may not reflect the current environment.

Unclear ownership
Assets, applications, services, and exceptions may not have accountable owners.

Missing technology context
Software, SaaS, cloud, lifecycle, usage, and risk context may not be connected to the record.

Unresolved exceptions
Issues are visible in reports but not always routed through workflow to resolution.

A green report does not always mean the environment is governed.

flexera

Why ServiceNow data quality breaks down between audits

Data quality does not usually fail all at once. It drifts as the environment changes faster than governance can keep up.

Technology changes faster than governance
New software, SaaS, cloud, devices, and integrations enter continuously.

Multiple sources create conflict
Discovery, inventory, procurement, cloud, SaaS, and manual inputs tell different stories.

Normalization is inconsistent
Different tools and teams interpret the same technology differently.

Ownership changes are missed
Owners change, but records do not always keep up.

Exceptions are tracked, not resolved
Issues are documented but not driven to closure.

If ownership, reconciliation, and exception management are not continuous, drift is guaranteed.

Manual cleanup fixes symptoms, not control

Audit prep can improve the report without improving the operating model.

Manual reconciliation may help teams pass an audit or prepare for an executive review, but it rarely fixes why the data quality broke down in the first place.

Why manual cleanup creates hidden risk

Fixes happen too late
Problems are corrected after drift has already created risk.

Root causes remain unresolved
The same data gaps return because the source issue was never fixed.

Teams rely on tribal knowledge
Success depends on people, effort, and workarounds.

Exceptions repeat every cycle
The same cleanup work comes back before the next audit or review.

Confidence stays low
Teams keep questioning the data.

If data quality only improves before an audit, you do not have a data quality program. You have audit prep.

Dashboards show risk. They do not govern it.

Visibility is useful, but visibility alone is not control.

A dashboard does not automatically

- Prove the data is complete or accurate
- Assign ownership
- Resolve exceptions
- Trigger remediation
- Confirm action was completed

Control requires four answers

1. **What changed?**
   Identify the signal or data quality gap.
2. **Why does it matter?**
   Connect the issue to risk, cost, compliance, service impact, or business priority.
3. **Who owns it?**
   Assign clear accountability.
4. **What action is required?**
   Route remediation, approval, exception handling, or risk acceptance through workflow.

The control chain: how to move from compliance to sustained control

Establish trusted source evidence	Identify authoritative sources for hardware, software, SaaS, cloud, ownership, usage, lifecycle, and risk.
Normalize and reconcile continuously	Reduce duplicate, conflicting, and tool-specific interpretations before data drives ServiceNow processes.
Add business and risk context	Connect technology records to cost, compliance, service impact, ownership, lifecycle, and exposure.
Operationalize through ServiceNow workflows	Route exceptions, remediation, approvals, and follow-through where teams already work.
Measure control over time	Track drift, exception closure, manual effort reduction, audit readiness, and risk reduction.

5 governance practices that improve ServiceNow data quality

A practical model for moving from cleanup to control

Practice 1

Define authoritative sources
Clarify where hardware, software, SaaS, cloud, ownership, usage, lifecycle, and risk data should come from.

Practice 2

Set data quality ownership
Assign accountable owners for data domains, exceptions, remediation, and risk acceptance.

Practice 3

Monitor drift continuously
Review duplicates, stale records, missing ownership, conflicting sources, and unresolved exceptions on a recurring cadence.

Practice 4

Prioritize by business risk
Focus first on data gaps tied to audit exposure, critical services, high-cost assets, lifecycle risk, and security impact.

Practice 5

Route action through ServiceNow workflows
Use workflows to assign, escalate, remediate, approve, and measure outcomes

flexera

Better ServiceNow data improves operational control

How trusted technology intelligence improves incident, change, and risk outcomes

When ServiceNow is fed with trusted data

Faster incident response

Teams can identify impacted assets, owners, and services earlier.

Better change decisions

Cleaner CI, software, lifecycle, and dependency data reduces downstream surprises.

Stronger risk response

Teams can prioritize remediation based on business impact, lifecycle exposure, usage, and ownership.

Trusted source evidence

Decision-grade records

Actionable workflows

Govern the data, not just the report

Treat ServiceNow data quality as an ongoing control discipline.

Prioritize the highest-risk gaps

Focus on data that affects compliance, cost, security, lifecycle, and critical services.

Make ownership explicit

Every exception needs an owner, action path, and resolution target.

Measure control over time

Track drift, exception closure, manual effort reduction, and outcome improvement.

Better data quality creates better action, not just better reports

flexera

Before vs. after: From compliance snapshot to sustained control

Before
Compliance snapshot

- Reports look complete, but data quality is uneven underneath
- Manual cleanup is needed before audits and executive reviews
- Ownership is unclear when exceptions appear
- Dashboards show issues but do not always drive action
- Risk builds between reporting cycles

After
Sustained control

- Data is normalized, reconciled, enriched, and governed
- Exceptions are routed to accountable owners
- ServiceNow workflows drive remediation and follow-through
- Compliance, cost, lifecycle, and risk signals are connected
- Teams trust the data enough to act on it

What changes when control improves

Less audit scramble
Teams spend less time cleaning up data before reviews.

Better decisions
Leaders act from trusted technology, ownership, cost, and risk context.

Faster remediation
Exceptions move through workflow instead of sitting in reports.

Stronger AI readiness
Automation is grounded in governed, decision-grade data.

Trusted data makes ServiceNow a stronger control platform

What this enables

Better ServiceNow decisions, stronger governance, and safer automation across technology, risk, compliance, and operations.

Trusted data foundation

Normalized, reconciled, and enriched technology data across hardware, software, SaaS, cloud, ownership, lifecycle, usage, cost, and risk.

Governed intelligence

Context that helps teams understand what changed, why it matters, who owns it, and what action should happen next.

Controlled Action

ServiceNow workflows that assign accountability, route exceptions, trigger remediation, and measure outcomes over time.

Control Maturity

A maturity path from manual data work to AI-readiness

Manual | Reported | Governed | Automated | AI-ready

AI-ready starts with control-ready data

flexera

Poll

Based on what you've seen so far, what's your biggest ServiceNow data quality challenge today?

Q&A

Thank you

About Flexera

Flexera helps organizations understand and maximize the value of their technology, including the rising costs and risks introduced by AI, saving billions of dollars in wasted spend. Our Flexera One platform connects the dots between what technology you have, how it is used, what it costs, and where it creates risk, helping teams take control of the increasingly complex IT estate across cloud, SaaS and on-premises. We are leading the way to unify IT asset management, FinOps and SaaS management with high fidelity data from Technopedia, our proprietary reference library of technology asset data, and intelligent automation fueled by AI. That's why thousands of global organizations rely on the Flexera One platform and Technopedia. Learn more at **flexera.com**

flexera™