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

Welcome! We're glad you're here.

MARCH 3, 2026

Agenda

1. Welcome & why execution-readiness matters

2. The **4-pillar** playbook for execution-ready ServiceNow workflows

   - Pillar 1: Minimum CMDB + CSDM foundation required
   - Pillar 2: Execution-ready ITAM controls in ITSM workflows
   - Pillar 3: Practical guardrails that limit blast radius
   - Pillar 4: Audit-ready traceability by design

3. Key takeaways & next steps (inc. Q&A)

Meet your speakers

James Dalley
Director, Solutions Success

Flexera

Clayton Starko
Director, Solutions Architecture

Flexera

Before we begin

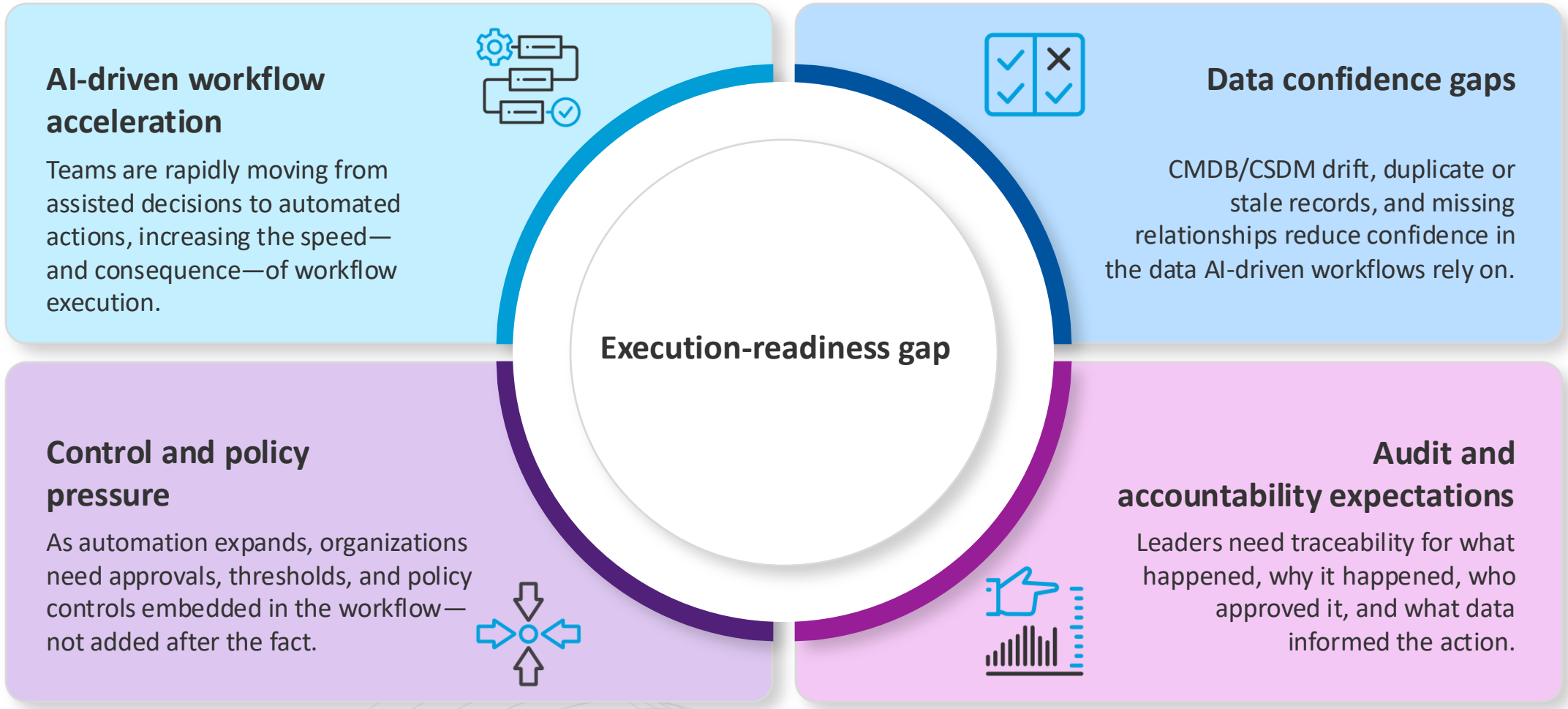
This session is being recorded. After the webinar, we will share a link to the recording, along with any relevant materials.

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.

Why execution-readiness matters now

AI is accelerating workflow decisions—but safe execution depends on trusted data, embedded controls, and traceability.



Where AI-driven workflows break first

Most failures happen in the execution conditions layer—not the workflow logic itself.

Why this matters?

AI workflows usually fail when they act on low-confidence data, execute without embedded controls, or leave behind weak evidence trails. The workflow may run—but the outcome is still wrong, risky, or hard to defend.

1 Data foundation gaps

Know

- CMDB/CSDM drift creates inconsistent context for decisions
- Duplicate, stale, or orphaned records reduce confidence
- Missing relationships break service-aware automation

Results Poor inputs lead to low-confidence decisions and avoidable rework.

2 Control gaps in workflow

Control

- Approvals and thresholds are missing or inconsistent
- ITAM, entitlement, and policy checks are not embedded
- Exception handling is unclear, manual, or too late

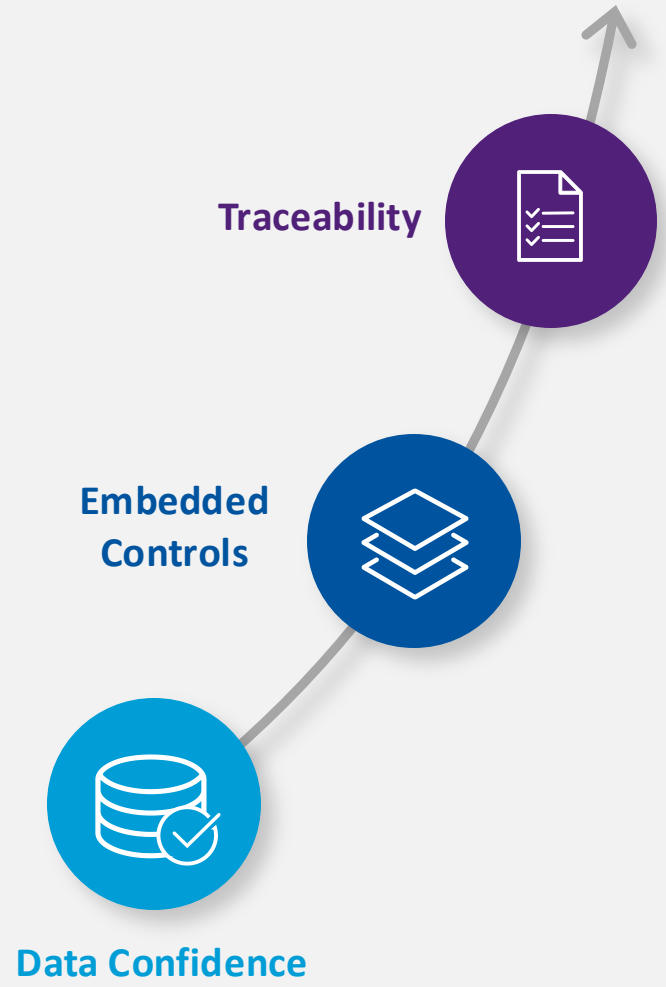
Results Workflows execute faster than governance, increasing blast radius.

3 Traceability gaps

Prove

- Teams cannot easily show what happened and why
- Approval history and decision context are fragmented
- Auditability is added after execution instead of designed in

Results Low trust in automation and limited ability to scale safely.



flexera

Pillar 1: Minimum CMDB/CSDM foundation required

The minimum data standard and operating model needed for safe workflow execution

People

Ownership and accountability

1. Data owners
Assign owners for CI and service data domains.
2. Data stewards
Define stewardship for quality, exceptions, and certification.
3. Outcome accountability
Tie accountability to workflow decision quality.

Process

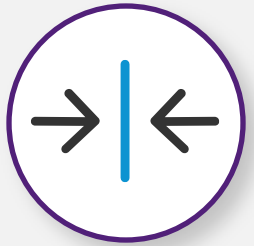
Minimum standard + certification discipline

1. Minimum action standard
Require owner, service alignment, lifecycle state, confidence score, and critical relationships.
2. Certification cadence
Review high-impact services and workflow-critical CIs on a defined schedule.
3. Continuous improvement
Manage data quality as a product with backlog and governance reviews.

Platform

Confidence signals and action-ready context

1. Decision-visible confidence
Expose confidence signals where workflows make decisions.
2. Relationship integrity
Prioritize complete, accurate relationships for service-aware automation.
3. Action-focused KPIs
Track confidence, duplicates, staleness, and orphaned CIs.



Execution-ready CMDB/CSDM is not **“perfect data.”** It is **trusted, governed, decision-usable data** for the workflows you expect to act.

flexera

Pillar 2: Embed ITAM controls in ITSM workflows so automation can act safely

ITSM workflows move faster when ITAM controls are built into the execution path—not handled later through manual reviews, rework, or audit cleanup.

1

Action context

Know what the workflow is acting on

- Identify the request/change/fulfillment action
- Capture service, asset, and business context before execution
- Determine impact level to guide controls and approvals

Better decisions start with the right context

2

Embedded ITAM controls

Apply governance in the workflow path

- Validate policy, entitlement, and license requirements
- Apply thresholds and approval gates by risk/impact
- Route exceptions intentionally instead of bypassing controls

Governance scales when controls are embedded, not externalized

3

Controlled execution + evidence

Move fast without losing control

- Record what happened, why it was allowed, and who approved
- Preserve decision context at execution time
- Create audit-ready evidence for compliance and review

Faster execution with stronger control and audit defensibility

flexera

Pillar 3: Practical guardrails that limit blast radius

Action mode controls

- Use recommend mode for high-risk, low-confidence, or new workflow actions
- Use execute mode for repeatable, low-risk actions with trusted inputs
- Promote workflows from recommend → execute only after control maturity is proven

Thresholds + approval gates

- Define thresholds based on financial, compliance, service, or operational impact
- Trigger approval gates for exceptions, elevated risk, or policy-sensitive actions
- Standardize approval patterns so controls are consistent across workflows

Controlled autonomy and safe execution boundaries

Policy, permissions + segregation of duties

- Enforce policy and permissioning aligned to role and workflow intent
- Apply segregation of duties for sensitive changes and approvals
- Limit who can enable, override, or expand automated execution

Exception + override governance

- Route exceptions intentionally instead of bypassing controls
- Track override reasons, approvers and repeat patterns
- Restrict who can approve exceptions and expand automation scope

flexera

Pillar 4: Audit-ready traceability by design

Traceability by design is the foundational layer

Execution-ready automation requires built-in evidence—not after-the-fact reconstruction.

Improves audit defensibility

Preserves decision context, approvals, and action history so teams can demonstrate control with confidence.

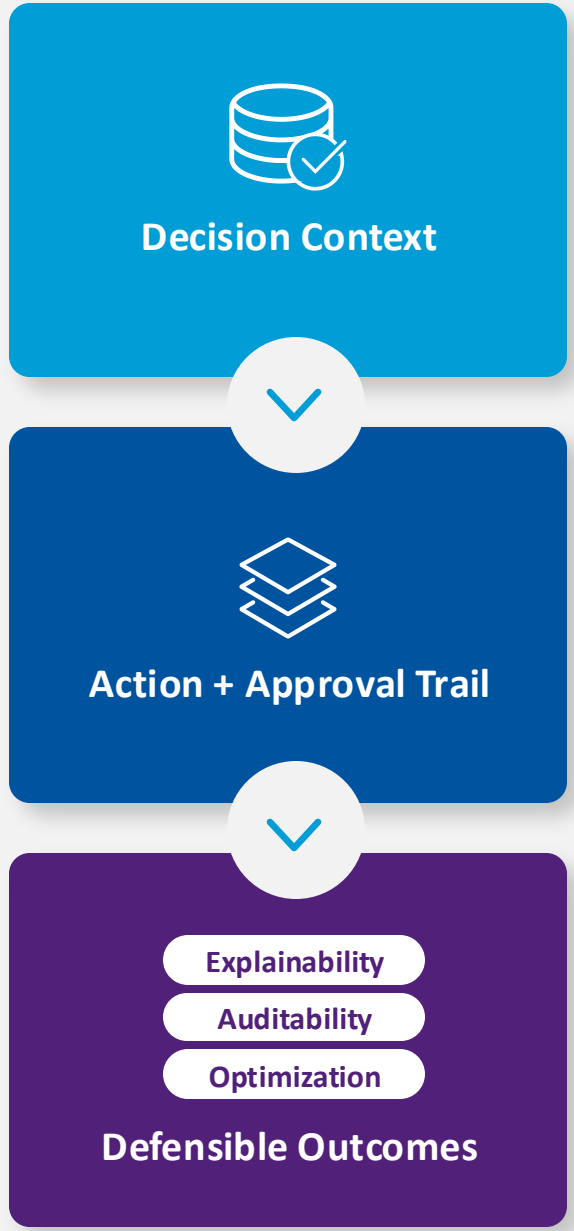
Builds trust in automation

Makes workflow actions explainable to IT, security, compliance, and business stakeholders.

Accelerates continuous improvement

Turns execution evidence into insight—highlighting bottlenecks, repeated exceptions, and guardrail gaps.

Traceability should be designed into workflow execution—not rebuilt later during audits, reviews, or incidents.



flexera

From execution-readiness to measurable outcomes

Turning trusted data, embedded controls, guardrails, and traceability into safe, scalable workflow outcomes

Execution-ready playbook

Organizations that scale automation safely don't start with autonomy, they build execution-readiness first. The four pillars create the conditions for trusted action, faster workflows, and defensible outcomes.

Execution-ready foundation

Build the minimum CMDB/CSDM and operating model required for workflows to act with confidence.

Confidence in workflow decisions

ITAM controls + guardrails in the workflow path

Apply approvals, thresholds, policy checks, and permissions where actions occur—not after the fact.

Safe automation at scale

Traceable outcome layer

Preserve decision context, actions, and approvals so automation is explainable, defensible, and repeatable.

Defensible outcomes and faster optimization

Execution-readiness maturity curve

From **assisted workflows** to **controlled autonomy**—the journey to **safe, scalable automation**

Assisted | Standardized | Controlled | Traceable | Scalable

Execution-readiness is not a destination—it's a discipline.

As maturity increases, organizations move from isolated automation to controlled autonomy with measurable outcomes.

Key takeaways + next steps

Execution-ready automation is a practical discipline—not a one-time project

Key takeaways

1. **Automation readiness is not the same as automation capability**
   ServiceNow can orchestrate action at scale—but safe execution depends on trusted data, embedded controls, guardrails, and traceability.

2. **Start with the minimum standard for safe action**
   Don't wait for "perfect" CMDB/CSDM data. Define the minimum execution-ready foundation for the workflows you expect to act.

3. **Scale automation by operationalizing governance**
   Embed ITAM controls, thresholds, approvals, and evidence into workflow execution so speed and control improve together.

What to do next

1. **Choose 1–2 workflows to assess**
   Start with high-volume or high-impact ITSM workflows where automation is already active (or planned).

2. **Baseline your execution-readiness**
   Assess the four pillars:
   - CMDB/CSDM foundation
   - Embedded ITAM controls
   - Guardrails / blast radius controls
   - Traceability by design

3. **Define a phased path to controlled autonomy**
   Begin with recommend mode where needed, add guardrails and evidence, then promote to execute as maturity improves.

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**

©2026 Flexera

flexera™