NEWS RELEASE

ServiceNow Brings Agentic Monitoring to Every Control in the Enterprise at Machine Speed

2026-11-10

AI agents configure compliance checks, interpret results, and act on failed controls in real time, giving risk and audit leaders always-on proof that controls work

Monitoring now reaches beyond ServiceNow to the cloud, container, identity, SaaS, and on-premises tools organizations have connected, with every control orchestrated in one place

SANTA CLARA, Calif.--(BUSINESS WIRE)-- **ServiceNow (NYSE: NOW)**, the Super Intelligence Control Tower for business reinvention, today announced agentic capabilities for continuous control monitoring in ServiceNow **Integrated Risk Management** (IRM). Monitoring now extends beyond the **ServiceNow AI Platform** with 100+ out of the box integrations to the systems organizations are connected to, from cloud and containers to identity, SaaS, and on-premises tools. AI agents configure checks, interpret results, and act on failed controls based on an organization's control narratives, across those systems and all lines of defense on a single platform. CISOs, Chief Risk Officers, and audit leaders receive an always-on risk and compliance posture with evidence that controls are working wherever they run, and workflows resolve issues at machine speed.

Agentic capabilities for continuous control monitoring in ServiceNow Integrated Risk Management

Risk moves faster than the audit cycle. A cloud misconfiguration, a failed vendor control, or a drifting AI model can open new exposures in minutes, across tools no single team owns. Boards and regulators expect proof that controls work today, everywhere they run. Assurance built for a slower, more contained environment can't keep pace. ServiceNow helps organizations move to a new model that monitors controls across the enterprise, with agents that can act at machine speed on what they find instead of only reporting it.

“ServiceNow is closing the gap between what an organization’s last audit showed and what’s true today by making assurance a live signal across the enterprise,” said Vasant Balasubramanian, Group Vice President and GM of Risk, Super Intelligence Control Tower, and ESG, ServiceNow. “Agentic continuous control monitoring watches every control an organization has connected and explains what a failure is. We’re empowering risk and audit leaders with assurance that moves as fast as the business to effectively manage risk in the agentic era.”

Continuous control monitoring engine reaches every connected system

AI agents configure, interpret, and act. Agents help teams set up checks, interpret results, and spot a control that is drifting or has failed. When something breaks, ServiceNow flags it, opens a ticket, and can remediate automatically within defined policies. Owners and governance, risk, and compliance (GRC) teams get to remediation faster, with less manual effort between detection and fix.

Monitoring extends to everything an organization plugs in. **ServiceNow IRM’s** continuous control monitoring works with the Super Intelligence Control Tower. Super Intelligence Control Tower governs how AI is built and used across the enterprise, and agentic monitoring shows in real time whether the controls around that work are holding. ServiceNow IRM already monitors controls in security operations, IT service management, IT asset management, and the Configuration Management Database (CMDB). 100+ pre-built integrations now extend that reach to third-party cloud, container, AI, SaaS, on-premises and business tools, and to every connected asset, including OT, IoT, and medical devices. As part of the Context Engine, Access Graph brings the full lifecycle of human, machine, and AI agent access into monitoring, so ServiceNow can verify that access is revoked the moment an employee or agent leaves. Evidence from every source flows into a central layer around the clock, so audit-ready proof is always current rather than assembled after the fact.

Orchestration brings every control into one view. Control orchestration maps each control to the tools that enforce it across connected systems, showing what is in place and how it performs. Compliance Graph connects signals across those systems to show what is actually at risk. When a control breaks, it is flagged, ticketed, and can be remediated automatically. IRM becomes a system of assurance and trust: always on, always audit-ready. Control owners see what needs their attention and respond in the tools they already use so attestations get done faster.

Map a control once, and it counts across every framework. Unified control mapping links each control to the equivalent requirements across regulations and standards such as SOX, PCI-DSS, ISO 27001, HIPAA, and the EU AI Act. An access control tested for SOX also counts toward the matching PCI-DSS and ISO 27001 requirements, so it is tested once and counts everywhere. When auditors ask for evidence, they get framework-specific results drawn from a single control repository.

“Resilience used to be about recovery. Now it's adaptability,” said Jackson Munuo, Global VP of Technology Risk & Control, CNA Insurance. “With AI workflows, we can anticipate things much faster, react more accurately.”

Assurance for every line of defense

Agentic continuous control monitoring serves each of the three lines of defense that risk programs depend on, meeting users where they are in whichever communication, collaboration, and project management platforms they use. Business units on the first line can monitor their own controls before compliance teams approach them. Risk and compliance leaders on the second line see failed controls surfaced, assigned, and acted on in the channels their teams already use, with a complete audit trail and context on what was exposed. Internal audit on the third line gets complete test results with supporting evidence instead of samples, plus the ability to run independent monitoring for added assurance. The result is fewer surprises, less audit scramble, lower audit cost, and reduced risk exposure, so the business can focus on growing faster.

“Compliance has long been treated as a periodic exercise - test, document, move on until the next audit cycle. What ServiceNow is describing is a genuine, closed loop: a control fails, an agent interprets why, a ticket is opened with remediation instructions, the fix is verified, and the risk register closes itself. That full lifecycle, running continuously across cloud, identity, and on-premises systems rather than within a single platform, is what separates agentic continuous control monitoring from the dashboards most GRC tools have offered until now.” - Philip D. Harris, Research Director, Governance, Risk, and Compliance Solutions, IDC

Availability

General availability of Agentic AI for Continuous Controls Monitoring is expected in Q1 2027.

About ServiceNow

ServiceNow (NYSE: NOW) is the Super Intelligence Control Tower for business reinvention. The ServiceNow platform integrates with any model, any cloud, and any data source to orchestrate, govern, and secure work across the agentic enterprise. ServiceNow gives customers the enterprise context and control to build and scale confidently. With more than 100 billion workflows running on the platform each year, ServiceNow helps organizations turn fragmented operations into coordinated, autonomous work for IT, CRM, Security, Employee Experience, and more. Learn how ServiceNow puts AI to work for people at **www.servicenow.com**.

Forward-Looking Statements

This press release contains “forward-looking statements” about the expectations, beliefs, plans, and intentions

relating to ServiceNow's agentic AI capabilities and continuous control monitoring. Such statements include statements regarding future product capabilities and offerings and expected benefits to ServiceNow. Forward-looking statements are subject to known and unknown risks and uncertainties and are based on potentially inaccurate assumptions that could cause actual results to differ materially from those expected or implied by the forward-looking statements. If any such risks or uncertainties materialize or if any of the assumptions prove incorrect, ServiceNow's results could differ materially from the results expressed or implied by the forward-looking statements made. ServiceNow undertakes no obligation, and does not intend, to update the forward-looking statements. Factors that may cause actual results to differ materially from those in any forward-looking statements include: (i) delays and unexpected difficulties and expenses in executing the product capabilities and offerings, (ii) changes in the regulatory landscape related to AI and (iii) uncertainty as to whether sales will justify the investments in the product capabilities and offerings. Further information on factors that could affect ServiceNow's financial and other results is included in the filings ServiceNow makes with the Securities and Exchange Commission from time to time.

Media Contact

Nicole Rosenberg
401.594.3673
press@servicenow.com

Source: ServiceNow