

ServiceNow's Operational Resilience solution helps financial institutions find, contain, and respond to AI threats with visibility and control

2026-10-21

ServiceNow's Operational Resilience solution helps financial institutions find, contain, and respond to AI threats with visibility and control

By Alexis Bliek, Head of Risk, Compliance & Security Go-to-Market for Financial Services, ServiceNow

From boardrooms to event floors, financial services leaders consistently ask the same question: how do we see and govern the AI already running inside our walls?

Picture a third-party security camera in a bank's branch lobby. The bank may not know it, but an AI model inside the device is quietly sending video footage to an outside endpoint. The camera arrived through a standard vendor contract that did not disclose the use of AI. It records clients every day, close enough to capture a wire transfer form or an account number on a relationship manager's screen. One ordinary camera on the wall has become rogue AI.

The camera is not an isolated case. According to new research on **The State of Agentic Security**, security leaders at banks are more likely than the global average to say they maintain a complete, accurate inventory of their AI agents. Yet the research uncovered they are actually less likely to find unknown or unregistered agents running in production. Despite their perceived readiness, 91% of banks experienced an agentic security incident in the past year, and only 32% of those financial institutions contained the incident in under 24 hours.

The solution: operational resilience, from discovery to recovery

ServiceNow's new Operational Resilience solution helps financial institutions find and respond to undisclosed AI in one place. It brings risk, security, IT, third-party risk management, business continuity, and AI governance together on the ServiceNow AI Platform.

In the camera example, here is how it could work. ServiceNow can surface the device, its AI models, and its outbound traffic before anyone outside the bank does, and map every access path it holds, including non-human identities. The Super Intelligence Control Tower can integrate and record the model and apply the bank's AI policy to it, while the security team contains the device and revokes access.

On the same record, risk and compliance teams see the obligations the camera touches. Third-party risk management can flag the vendor for reassessment and show every other asset it supplies. Business continuity activates the branch's plan so operations can keep serving clients.

Because the platform runs continuously, tracking every asset as it connects and changes, an undisclosed AI like the one in the camera surfaces long before it becomes a surprise. Every team sees the same event, from the same data, at the same moment. Much of the record the regulator will ask for is captured as the response runs.

Operational Resilience helps surface undisclosed AI agents before a breach

In many bank environments today, undisclosed AI often comes to light only after a breach.

At that point, the CISO needs to know what the device is, what its AI is doing, and who has access. The head of AI governance needs to know where models sit among every other AI tool, model, and agent in the bank, and whether it meets the bank's AI policy. The CRO needs to know which critical services and obligations it touches and whether the bank remains inside tolerance. The third-party risk team needs to know what else that vendor supplies. Branch operations need to know whether a branch can keep serving clients, and what to tell them.

Each answer has historically lived in a different tool owned by a different team. Context gets lost in every handoff, and every new device, identity, and agent widens the gap. Meanwhile the regulator's clock runs: four hours under DORA and 72 hours under NYDFS and APRA, for example.

With ServiceNow, every capability shares one data model and one AI layer, the same one that already maps the bank's critical services, their assets, and their obligations. When your bank's security flags undisclosed AI, it can see the branch, the services that branch supports, the vendor, and the policies that apply. That context is what turns an alert into a decision.

Because the platform also runs the bank's other workflows, a response can trigger action anywhere, from IT to CRM workflows.

Governance and security must be built in from the start

ServiceNow and NVIDIA's **2026 Banking AI Maturity Index** found that 100 percent of banks surveyed use AI, but only 24 percent have AI testing, auditing, and risk processes in place to match. Insurers show the same pattern: **only 21 percent** have governance to match their AI use. The space between those numbers is where undisclosed AI lives.

When discussing AI governance best practices in the latest **AI Maturity research**, BMO stressed that governance shouldn't be added after the fact. It should be built into AI from the start. "The nonnegotiable is clear accountability, strong AI and data governance, and continuous monitoring with human oversight," said Ahieron Srikandamohan, Senior Manager, Product Lead, Digital & Innovation, BMO.

ServiceNow brings AI governance, risk and security, and frictionless service workflows together for 1,500 financial institutions worldwide. **CNA Insurance** shows what that looks like in practice.

The insurer unified incident management, change control, infrastructure operations, and GRC into one operational core on the ServiceNow AI Platform. With unified governance and automation, CNA can test controls across their entire 900-application portfolio. AI-driven risk scoring surfaces issues automatically through CMDB integration, without needing manual assessment or back-and-forth with other business units, identifying risks before auditors do and responding to regulatory changes in hours instead of days.

Availability

The Operational Resilience solution for financial services is available today.

Additional Information

ServiceNow recently joined executives at SIBOS and InsureTech to discuss how financial institutions can approach AI with governance and resilience at the center. Learn more about our perspective on **AI, trust, and the future of financial services**.