

Deloitte.

| **servicenow**



**ORCHESTRATING ENTERPRISE
CYBER RESILIENCE AND AI GOVERNANCE**
WITH DELOITTE AND SERVICENOW

Faster response. Stronger oversight.

Audit-ready assurance—across security, risk controls, assets and AI governance.

Cyber risk is rising as enterprises modernize across cloud, on-premises, software-as-a-service (SaaS) and operational technology (OT). As artificial intelligence (AI) becomes embedded in business and security workflows, AI is also changing the risk equation—moving beyond advising to taking action within security workflows, placing more decision-making authority within intelligent systems. Most governance frameworks were not built for this: they assume humans decide and AI simply informs. As AI takes on a more active role, those frameworks need to evolve with clear accountability, human oversight, and real control built-in.

At the same time, evolving regulations and stakeholder expectations demand greater transparency, speed, and control. Yet many security programs remain constrained by fragmented tools and manual processes that slow response and undermine confidence. The result is inconsistent performance with different teams acting on different data and applying different priorities.

Deloitte and ServiceNow help organizations connect security operations, risk and controls, technology asset management (TAM), and AI governance workflows through intelligent automation—strengthening implementation, oversight and audit-ready transparency.

The result: greater visibility, faster and more coordinated response, streamlined compliance, resilience at scale.



Security at a crossroads: Fragmentation, manual handoffs, and mounting complexity

Even with significant investment, many organizations still operate with fragmented tools and manual handoffs that limit visibility and slow responses until an audit finding or incident forces a reactive sprint.

DELOITTE RESEARCH REFLECTS THIS SHIFT:

46%

of surveyed organizations use multi-party, multi-solution cloud ecosystem monitoring to reduce complexity.¹

39%

In parallel, 39% report using artificial intelligence (AI) capabilities in cybersecurity programs to a large extent, often to automate triage and correlate signals across fragmented environments.¹

OUR RESEARCH ALSO SHOWS THAT AI GOVERNANCE IS NOT KEEPING PACE WITH ADOPTION:

Only 21% of organizations have mature AI agent governance, despite 74% planning agentic deployments.²

More than 80% of AI governance failures are internal missteps rather than external attacks.²

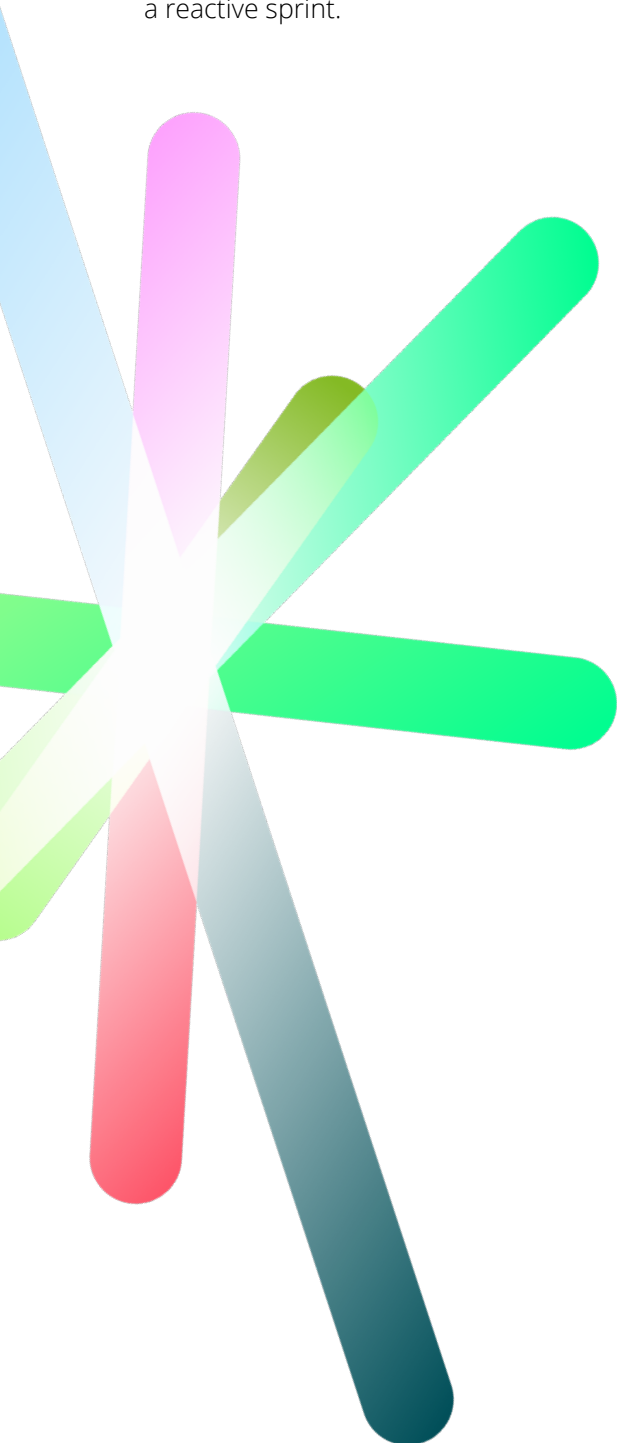
WHEN INCIDENTS OCCUR, THE IMPACT CAN EXTEND BEYOND OPERATIONS:

64%

report loss of confidence in technology integrity.¹

39%

report negative impacts to talent recruitment or retention.¹



A better path forward: Unified, business-aligned cyber resilience and AI governance at scale

A practical response to today's threat and AI-driven environment is to reduce fragmentation and standardize implementation through a unified platform approach. By connecting security, risk, asset, and AI governance workflows—and applying automation to repeatable tasks such as AI system and agent discovery, risk tiering, intake, approval, identity and access review, monitoring, response, and evidence capture—organizations can scale capacity, improve consistency, and strengthen oversight.

In practice, unified workflows can strengthen across the traditional three lines: helping operational Line 1 teams respond and remediate faster; enabling Line 2 to improve governance and controls monitoring; and giving audit-focused Line 3 more consistent, audit-ready evidence especially across cyber and IT risk and controls.

Attackers are also scaling and intensifying extortion: in 2026, ransomware groups have been maximizing extortion pressure on victims to turn out a quick and profitable operation, using multiple layers of extortion, from the threat of data leak to harassing clients and customers to pressure a quick financial settlement.³ This trend has hit multiple sectors hard, with over 5,000 confirmed ransomware attacks by July 2026.⁴

Threat actors such as Qilin and The Gentlemen have been heavily targeting downstream third-party service providers, realizing that disrupting transaction services forces faster payouts over traditional data encryption alone. Further, weak supply chain management means that a single breach on a service provider can lead to several high-value targets.⁵

This increases the need for faster detection, integrated response and repeatable implementation across teams and environments.

DELOITTE AND SERVICENOW HELP CLIENTS MOVE FORWARD



A single operational view of assets, AI systems and exposure across IT, OT, cloud, and AI-enabled environments



Repeatable, automated workflows for faster detection, response and governance



Improved transparency for executives, boards, and regulators



Proactive risk reduction enabled by integrated data and orchestration



Governance that combines policy-based rules with transactional workflows, so responsible AI requirements can be operationalized and enforced



Why ServiceNow

ServiceNow provides an intelligent workflow platform that helps bring security operations, risk/controls, TAM, and AI governance processes into a more connected operating model—so work moves faster and oversight becomes easier.

ServiceNow's AI Control Tower (AICT) can serve as an operational backbone for AI governance across five domains: discover, govern, secure, observe, and measure.

AICT can be extended through complementary capabilities such as Veza for identity and access, Armis for runtime, and asset security—helping organizations discover, govern, secure and measure AI use through connected operational workflows.

Because ServiceNow's platform is built for extensibility, these integrations are examples rather than requirements—Deloitte can adapt the same governance workflows to your existing security and identity tools. Organizations aren't required to adopt a specific product stack to achieve lifecycle-based AI governance.



CLIENTS USE THE PLATFORM TO SUPPORT OUTCOMES SUCH AS:

Unified workflows

Connect teams and processes across security, risk, asset management, AI governance, IT, and the business

Automation at scale

Reduce manual tasks and improve consistency in execution

Lifecycle-based AI governance:

Support discovery, risk assessment, approvals, monitoring, intervention, and evidence capture across AI systems and agents

Enhanced visibility

Enable reporting and transparency aligned to risk, compliance, and AI governance needs

Coordinated response

Improve speed and collaboration when vulnerabilities or incidents occur

Deloitte's unified workflow approach links Security Operations, Integrated Risk Management (IRM), TAM, and AI governance—connecting what you know (assets), what you do (response) and what you can prove (governance and assurance).

Why Deloitte

Deloitte brings experience across cybersecurity, risk and controls, and AI governance to help organizations extend their existing ServiceNow environment—not create a separate governance stack. AI assets can be registered in the same configuration management database (CMDB)—a shared system of record for technology assets, configuration items and their relationships—as other technology assets. AI risk can be managed through existing IRM controls and policy libraries, and AI telemetry can feed directly into Security Operations for monitoring and response.

We help clients combine policy-based governance—the rules for responsible AI—with transactional governance—the workflows that make those rules operational from discovery and approval through monitoring, evidence capture and remediation.

The two need to work together: policy without workflow does not enforce anything, while workflow without policy has nothing to enforce.

This approach enables organizations to govern AI based on potential consequence and impact—not simply the technology involved—while extending the asset, risk, and security foundation they already have.

Together, these capabilities help organizations implement, integrate, drive adoption, and sustain AI governance at scale so outcomes continue beyond go-live.



Deloitte and ServiceNow: Strong governance, sharp controls, clear accountability

Deloitte and ServiceNow work together to help clients unify their security operations, risk and controls, TAM, and AI governance workflows—enabling organizations to continually strengthen cybersecurity posture, AI governance and resilience through scalable automation, visibility and control while driving operational efficiency.

WHAT THIS CAN LOOK LIKE IN PRACTICE:

Modernized security operations and AI governance with more consistent, measurable workflows for discovering, assessing, monitoring, and responding to cyber and AI-related risk

Streamlined compliance and audit readiness through policy-based governance, transactional workflows and integrated evidence trails across AI assets, controls, and use cases

Improved risk governance with clearer accountability and cross-functional transparency—from AI discovery and approval through ongoing monitoring and remediation

Reduced complexity, cost, and operational friction by extending asset, risk, and security workflows to AI governance—limiting duplicate tooling, manual handoffs, and fragmented oversight

More proportionate controls across five governance domains: strategic alignment, lifecycle and compliance, identity and access, runtime security, and value and performance

OUTCOMES YOU CAN OPERATIONALIZE

1

Cyber, risk, and controls experience you can run with

Deloitte brings deep cyber experience, regulatory knowledge, IRM and operating model capabilities together to help organizations strengthen governance, streamline evidence control and testing, and improve transparency for executives, regulators and internal assurance functions. This experience also helps organizations identify and manage emerging risks, including unmanaged AI agents, non-human identities, unclear ownership and AI-driven decisions that may be difficult to explain or evidence.

2

Intelligent automation for unified security operations

By connecting asset, risk, and security workflows on ServiceNow, organizations can automate repeatable activities such as intake, triage, escalation approval, and evidence capture. This helps reduce swivel-chair activities, strengthen ordination, and improve the speed and consistency of execution across security operations.

3

Cyber resilience as a catalyst for growth

When security, risk and technology teams operate from shared data, organizations can make faster, risk-informed decisions, improve stakeholder confidence, and turn responsible cyber resilience into an enabler of innovation and growth.

4

Governing AI by consequence, not technology

AI governance should apply proportionate controls based on AI system use, autonomy, data, access, and potential impact—not simply the technology involved.

Deloitte can help organizations use ServiceNow AI Control Tower as an operational backbone to discover, assess, approve, monitor, and measure AI systems and agents across their lifecycle. Connected capabilities such as Veza for identity and access and Armis for runtime and asset security can extend coverage across the five governance domains: strategic alignment, lifecycle and compliance, identity and access, runtime security, and value and performance.

Capabilities: How Deloitte and ServiceNow deliver value together



Technology Asset Management (TAM)

Gain real-time visibility and governance for digital assets across IT, OT and cloud to help reduce risk, improve spend management, and support smarter decisions—including identifying and addressing unmanaged risks such as shadow IT.



Security Operations

Unify and accelerate incident and vulnerability response with connected workflows and automation, so teams can respond faster and operate consistently across legacy and modern environments.



ServiceNow Integrated Risk Management (IRM): Risk, Controls, and Compliance

Implement and operationalize ServiceNow IRM workflows across risk, controls, audit, and compliance—streamlining evidence and issue management, improving transparency and supporting near real-time monitoring and reporting.



AI governance and AI Control Tower (AICT), Veza and Armis

Establish an operational foundation for responsible AI adoption by discovering AI systems and agents, applying risk-based intake and tiering, managing approvals, governing identity and access, monitoring runtime behavior and value, and maintaining evidence across the AI lifecycle. AICT can be complemented by Veza for identity and access and Armis for runtime and asset security, while extending existing CMDB, ServiceNow IRM, and Security Operations workflows.



Bring it to life: Operationalizing cyber resilience and AI governance

The following use cases illustrate how Deloitte and ServiceNow can help organizations operationalize and build a connected governance foundation needed to scale AI responsibly across industries—including Deloitte's firsthand experience implementing ServiceNow IRM internally.

Deloitte streamlines global operations and advance AI governance with ServiceNow Integrated Risk Management (IRM)

Deloitte is not only a strategic ServiceNow alliance—we are also a customer, applying ServiceNow IRM in our own environment as we advance AI governance. Deloitte has also applied ServiceNow AI Control Tower, Security Operations and Veza internally to help discover, govern, secure and measure enterprise AI use.

With implementing ServiceNow IRM, we streamlined operations for 300,000+ professionals and realized double-digit productivity gains across multiple business units, demonstrating how enterprise-scale workflow standardization and governance can support AI-enabled operations.

A global quick-service restaurant (QSR) company modernizes security and operational workflows

A QSR company unified cybersecurity and restaurant operations through a single global ServiceNow platform. Deloitte helped integrate security across 13+ domains, streamline digital workflows, and enable a more consistent experience across markets—connecting security and operations on one global platform across a distributed footprint.

A life sciences organization unifies eight ServiceNow environments to accelerate innovation

A life sciences organization engaged Deloitte to help it unify eight ServiceNow environments. The client was able to achieve 90% out-of-the-box adoption and improved governance, transparency, and user experience. By consolidating and standardizing, the organization simplified operations and increased adoption.

A telecommunications provider transforms risk and cybersecurity with an integrated risk platform

A global telecommunications provider engaged Deloitte to help it elevate its cybersecurity and risk posture through a ServiceNow-powered integrated risk platform. By unifying risk, privacy, and cybersecurity operations, the organization accelerated audit evidence requests by 50%, standardized 1,200+ control objectives and eliminated 125+ legacy customizations—improving audit responsiveness, reducing technical debt and supporting more continuous compliance.

A health plan provider operationalizes AI governance

A health plan client engaged Deloitte to help it establish a phased AI governance operating model using ServiceNow AI Control Tower. Within a 90-day phased rollout, the client implemented AI intake, automated risk tiering, multistage approvals and live monitoring dashboards—helping create a more consistent, transparent approach to governing AI use.



Demonstrated experience and delivery at enterprise scale

Deloitte brings the governance, delivery discipline, and run-state experience to help organizations not only implement workflows but sustain adoption and measurable outcomes at enterprise scale.

Deloitte and ServiceNow offer experience and scale in helping clients unify security, risk, asset and AI governance workflows—supported by:



Award-winning scale and talent:

~2,000
practitioners

11,000+
certifications in the US

access to

12,000+
ServiceNow-certified
practitioners

30,000+
certifications
worldwide

including

81
Certified Technical
Architects (CTAs)

20
Certified Master
Architects (CMAs)

with presence in

150+
countries

13
regional and global
delivery centers

Global Elite Partner status and long-standing transformation experience, including 10,000+ ServiceNow-led project implementations and 6,000+ clients served worldwide

Extensive delivery track record across thousands of ServiceNow-led implementations

Broad talent and certifications supporting enterprise deployments and operations

Recognition by leading industry analysts for cyber and risk-related services

Experience extending established asset, risk, controls, and security operations foundations to support AI governance without creating a separate governance stack

Turning cybersecurity investment into measurable outcomes

Our clients typically measure progress through outcomes such as:



Faster and more consistent incident and vulnerability response



Improved audit responsiveness and compliance confidence



Better visibility into asset exposure and control coverage



Reduced manual effort and operational friction across teams



Increased executive transparency and decision support



More consistent AI discovery, risk tiering, approval, monitoring, and evidence capture



Improved ability to govern AI use proportionately based on potential impact and consequence

Ready to unify cyber resilience with intelligent workflows?

Connect with the Deloitte ServiceNow alliance team to discuss your current security, risk, asset and AI governance operating model—and identify where integrated workflows and automation can drive the fastest value.



Adnan Amjad

aamjad@deloitte.com

*US Cyber Offering Portfolio Leader
Deloitte Consulting Services LLP*



Krishnakant Dave

kdave@deloitte.com

*Americas ServiceNow Alliance Leader
Deloitte Consulting Services LLP*



Ertem Osmanoglu

eosmanoglu@deloitte.com

*ServiceNow Cyber Leader
Deloitte Consulting Services LLP*

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this document. Product names mentioned in this document are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Deloitte is not responsible for the functionality or technology related to the vendor or other systems or technologies as defined in this document. As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2026 Deloitte Development LLC. All rights reserved.

Endnotes

1. Deloitte Global, The Global Future of Cyber Survey, 4th Edition: The Promise of Cyber, 2024.
2. Deloitte, US Annual Cyber Threat Trends Report, 2025. (Deloitte is currently compiling 2026 report data).
3. Deloitte, internal sources, 2026.
4. Ransomware.live. "Ransomware stats" (online) through July 2026.
5. Dutta, T. "Qilin Led Ransomware Attack Claimed to Compromised 104 Organizations in August" Cyber Security News, 2025.

