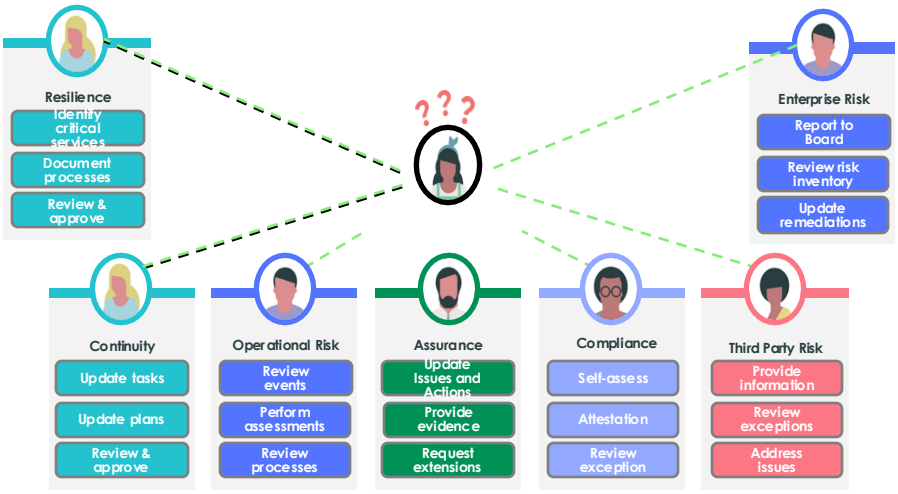
Effectively manage enterprise-wide risk and corporate compliance

Enterprise risks are diverse and evolving. And because they can easily disrupt organizational goals related to strategy and reputation, operations, or finance, enterprise risks require the attention of corporate governance and executive management.

A wide variety of external threats can generate enterprise risks--from competitive pressures to environmental disasters, privacy violations, or supply chain disruption. In fact, according to Gartner, "By 2025, 70% of CEOs will mandate a culture of organizational resilience to survive coinciding threats from cybercrime, severe weather events, civil unrest, and political instabilities.[1]"

But it is not just external threats that enterprises must contend with. Internal operational challenges are endless. The survival of your business may depend on how well you manage these internal operational risks. Too often, teams struggle with working in organizational silos with disparate technology, manual processes, a lack of system integration, and a limited view of risk across the business. The result is hampered visibility, speed, and agility. Add in point-in-time risk assessments that are not based on current data—and it's virtually impossible to make accurate risk-informed decisions.

And finally, most risk solutions are cumbersome and don't offer appealing user experiences, so frontline employees avoid them. This creates a risk intelligence gap for your organization.



The ServiceNow integrated portfolio of risk products bridges the intelligence gap by offering the frontline the ability to effortlessly engage in risk and compliance activities. As part of a single system, ServiceNow provides the speed, agility, and confidence for decision makers at all levels--from the frontline control owner to the third-line audit analyst.

Let's take a closer look at how you can:

- Integrate, manage, and monitor operational and enterprise risk
- Manage and report on corporate compliance and regulatory changes
- Perform internal audits with high-quality data

Benefits

- Get a faster time to value with access to up-to-date data on critical assets
- Recognize changes when they occur through dynamically updated risk scores using automated risk assessments
- Create frictionless experiences for the frontline, enable risk and compliance teams, and support internal audit for a stronger risk and compliance posture
- Proactively manage regulatory changes to maintain compliance without disrupting operations
- Improve the accuracy of audit evidence through integration with your existing ecosystem and ServiceNow applications to keep data current in the platform

1. Gartner Security and Risk Summit 2022

Integrate, manage, and monitor operational and enterprise risk and compliance

Stay on top of risks with continuous monitoring and automated assessments to identify emerging or rapidly changing risks wherever they occur. Flexible, integrated, and aggregated risk assessments use different methodologies based on entity, regulation, risk, or other perspective to assess and roll up scores for a more accurate view of risk. For example, operational risk can be assessed at the transactional, portfolio, business unit or entity level.

Continuous monitoring also helps you identify compliance issues with real-time reporting of controls linked to laws, rules, regulations, and policies.

Taking a continuous, real-time, and data-driven approach to risk and compliance using data already in the platform not only utilizes what you already have but improves decision-making at all levels in the organization.

When risks or compliance violations are identified, issue management tracks issues to completion with a full audit trail. It uses machine learning to route issues to the appropriate teams, group similar issues when possible, and recommend remediation automatically to improve accuracy and response time.

Create a frictionless user experience for the frontline

To effectively manage risk and compliance, all levels of the business must be engaged. Embedding risk and compliance into daily work and integrating it across the enterprise enables the often-forgotten frontline user to acknowledge policies, request policy exceptions, report risk or loss events, and utilize guided assessments. The Employee Center portal is specifically designed to help the frontline with these tasks. Other user-friendly capabilities also make tasks easier. For example, chatbots help you search for policy language or request a policy exception. And for those on the go, mobile interfaces make the experience seem both familiar and easy.

Manage regulatory changes

With the fast-evolving regulatory landscape, keeping an eye on the horizon is essential. To effectively manage current and future regulatory requirements you must first have insight into upcoming changes. Integrating with regulatory feeds are a great way to achieve this. But to proactively manage and plan for updates requires the ability to assess the impact of updates, track issues and changes to regulatory obligations, identify gaps, and successfully implement the changes. ServiceNow Regulatory Change Management accomplishes this using a standardized regulatory taxonomy in conjunction with policy lifecycle management and risk assessment capabilities.

Learn more at servicenow.com/risk

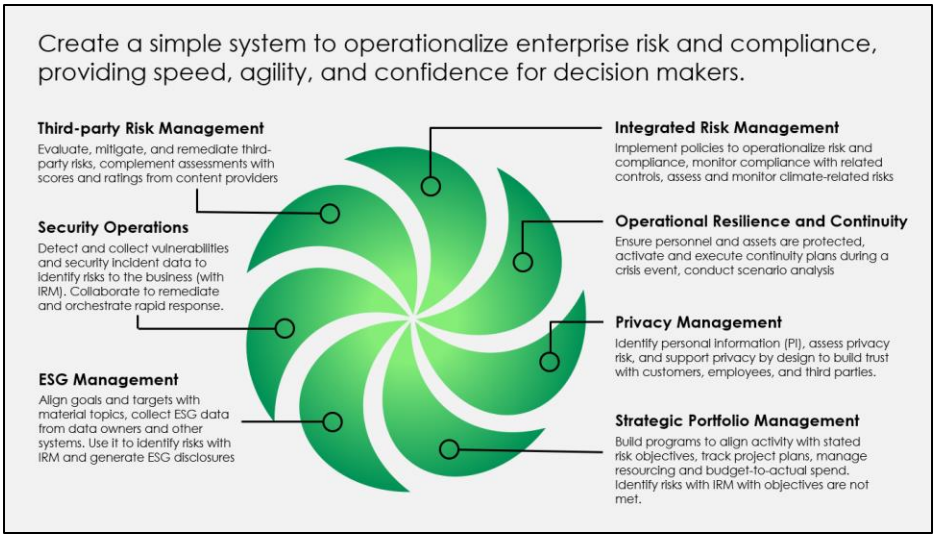
Perform internal audits

Continuous monitoring also improves audit activities. For example, evidence collected during automated control testing, can be used in audit engagements to provide the necessary assurance across a wide variety of regulations, frameworks, and initiatives. The ability to automate testing of some portion of controls allows audit to focus on the much harder population of controls where automation cannot be achieved or achieved easily. It also identifies riskier areas where audit might want to focus more heavily.

However, continuous monitoring, risk assessments, internal audit, and many other capabilities all require accurate, current data. As a single system of record the ServiceNow® AI Platform is the repository to meet these needs.

Integrated across the enterprise

The data in the platform is kept current through integration with third parties, systems of record, and ServiceNow applications that help manage financial services, HR, IT, security, and more. IntegrationHub and supported spokes make many third-party integrations easier.



servicenow.

ServiceNow AI Control Tower: Govern any AI at Scale

In today's fast-moving AI landscape, enterprises are eager to harness AI's transformative potential—supercharging efficiency, elevating customer experiences, and redefining competitive advantage.

Yet, enterprises face some big hurdles in realizing AI's full potential. Fragmented initiatives across departments lead to duplicated efforts and inconsistent governance, wasting valuable resources. Many AI projects fail to align with core business objectives, undermining their potential impact. And the rapid evolution of AI outpaces traditional risk management, creating vulnerabilities and complicating compliance with regulations and frameworks.

Siloed solutions or a single executive champion can't solve these challenges. They need a cross-functional team. That's why many organizations are choosing to create an AI Center of Excellence (CoE). And today's AI CoEs need more than just oversight of AI initiatives—they need a seamless way to connect strategy, governance, execution, and value across the enterprise.

Introducing: The ServiceNow AI Control Tower

Built on the foundation of the ServiceNow® AI Platform, the AI Control Tower (AICT) establishes central oversight across enterprise teams, providing AI visibility & control, driving alignment, and enhancing value. AICT provides organizations with holistic visibility into their AI assets through the onboarding and discovery of AI systems, models, and datasets. Whether your AI is internally developed, sourced from third parties, or embedded in SaaS and external platforms, AI Control Tower delivers the visibility and control you need to scale and govern responsibly.

ServiceNow AI Control Tower is purpose-built for AI CoEs and Chief AI Officers (CAIOs) to align strategy and enable an enterprise-wide vision. Additionally, it provides customized workspaces for all members of the CoE and beyond, including AI stewards, AI product owners, and risk and compliance managers.

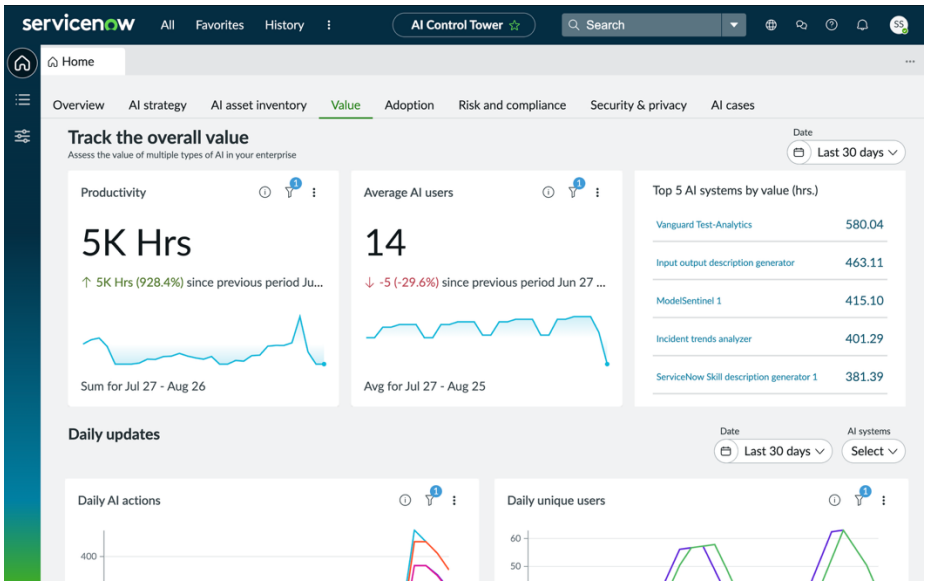


Figure 1: AI Control Tower Workspace – AI Value Dashboard

ServiceNow Stands Out

ServiceNow AI Control Tower is in a league of its own compared to point solutions and hyperscalers. We don't just focus on AI agents or offer fragmented tools. Instead, we empower AI CoEs to harness all AI for real business impact, turning complexity into a strategic advantage.

Built-in technology system of action:

The AI asset inventory in the configuration management database (CMDB) delivers unmatched business context, connecting AI to your enterprise's services and assets - to accurately gauge AI risk to the business.

Market-leading Governance, Risk, and Compliance (GRC):

Recognized by Forrester as a market leader, our GRC capabilities embed governance into the AI lifecycle to help ensure compliance from day one.

Enterprise workflow orchestration:

Cross-functional automation and collaboration unite asset management, Strategic Portfolio Management, IT, Risk, Legal, PMO, Governance, and business teams for seamless AI management.

Unified ServiceNow AI Platform:

Our integrated solution, built on a single AI platform and data model, reduces complexity and total cost of ownership, so you can optimize management of all your data, AI, and workflows in one place.

Develop a robust AI strategy

Set AI goals in integration with Strategic Portfolio Management, capturing AI demand, building roadmaps, running scenario planning, and tracking portfolio progress against strategic targets—all in one place. AI Control Tower models potential impacts and prioritizes projects that deliver maximum value—whether that's driving revenue growth, enhancing customer experience, or boosting operational efficiency.

Automate AI asset inventory

Users can request new AI assets via a structured onboarding process and leverage out-of-the-box APIs to connect to cloud service providers, code repositories & pipelines. It also provides automated discovery from Amazon Bedrock, Azure AI Foundry, Copilot Studio, and GCP Vertex AI. Build an inventory of AI systems, datasets, models, and prompts, and MCP servers as teams adopt them, and keep consolidated control over them. These assets are maintained up-to-date in the CMDB within OOTB classes. This way, your AI CoE has a single platform for AI onboarding through retirement.

Build trust with unified AI governance

Get proactive with risk and compliance scoring, AI risk visibility, and centralized oversight of risk classification.

ServiceNow's market-leading AI risk and compliance capabilities create a holistic governance environment, providing impact assessments, reporting emerging AI risks, managing AI cases, and continuously providing assurance of compliance frameworks. In addition, you can:

- Manage performance against regulatory standards such as NIST AI RMF and the EU AI Act.
- Continuously monitor AI agents (including ServiceNow AI Agents) running with privileged roles, surface, and reduce the attack surface by flagging dormant agents.
- Choose approved third-party model providers (e.g. AWS Anthropic, Azure OpenAI, Google Gemini), and enforce global/regional data routing policies.

Move from ideas to safe, scalable AI execution

AI Control Tower drives end-to-end execution for agents, models, and workflows: intake and approvals, onboarding and deployment, cases, issues, and ongoing operations with real-time reporting. The AI CoE can monitor system and AI skills usage by department and user, and even collect feedback for process improvement. AI Control Tower flawlessly enables product teams and lines of business to create new cases and engage the AI CoE in a real-time fashion for approvals—the result: consistent, governed delivery of AI—every release, every team, every cloud.

Show exactly what value your AI is delivering

The AI Control Tower's Value dashboard consolidates ROI, productivity, cost avoidance, and risk reduction metrics into a single view, tied to every AI system, agent, and workflow in your inventory. Use configurable value templates to standardize how teams report AI users, productivity, top AI systems by value, and spotlight adoption blockers (e.g., policy holds, latency, or access gaps). Drill from portfolio-level impact to a single model's inputs/outputs and owners, then export an evidence pack for executive updates and audit needs. It's a faster path from "we think it helps" to "here's the quantified business value."

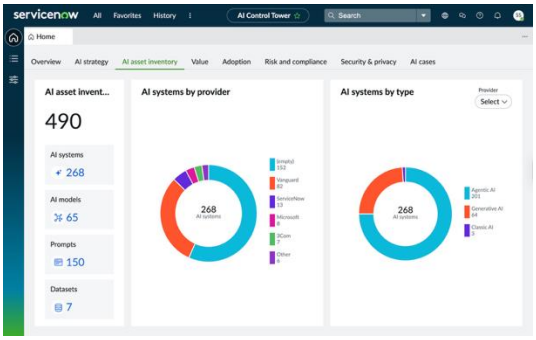


Figure 2: AI Asset Inventory

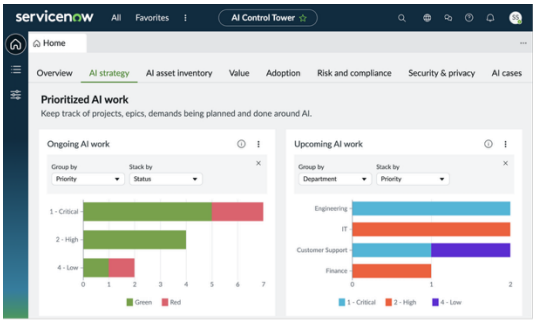


Figure 3: AI Strategy (Integration with Strategic Portfolio Management)

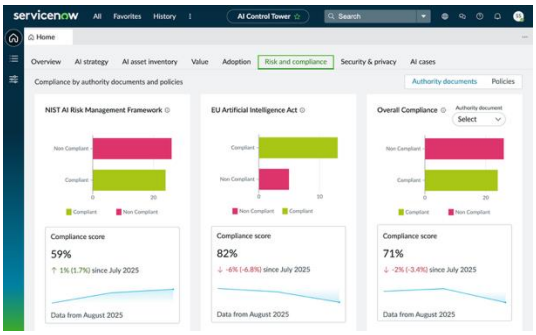


Figure 4: AI Risk and Compliance

The AI Control Tower: Your fast track to AI success

Visit www.servicenow.com/ai-control-tower or contact us to schedule a demo and discover how to drive lasting impact.

SN_Solution Brief_AI_Control_Tower_Aug-21-2025

ServiceNow Security Incident Response

Wanted: Cyber resilience under pressure

Security Operations teams continue to show grace under pressure, every day. With ever-greater reliance on digital systems, the job is getting harder, every day. According to Enterprise Strategy Group Research, security and IT professionals continue to struggle with SOC modernization:

- 70% say it is difficult to recruit additional SOC staff
- Nearly 2/3rds are adopting new tech for automation and orchestration
- Top two priorities are integrating security and IT tools and improving collaboration between security and IT staff
- 81% say MITRE ATT&CK® is an important component of their security posture

Transform investigations and response

ServiceNow® Security Incident Response, a security orchestration and automation response (SOAR) solution, helps you rapidly respond to evolving threats while optimizing and orchestrating enterprise security operations. Security Incident Response eliminates the errors and friction natural to manual handoffs across systems, teams and responsibilities. Integrations, playbooks, dashboards, and a common data model for enterprise case management expedite investigation, response, and remediation across IT, Security, and Risk teams to minimize incident impact, data loss, and exposure. This drives maturity of your security operations, and centralizes case management for threats, data loss events, and more.

Automate away the basics to focus on the critical

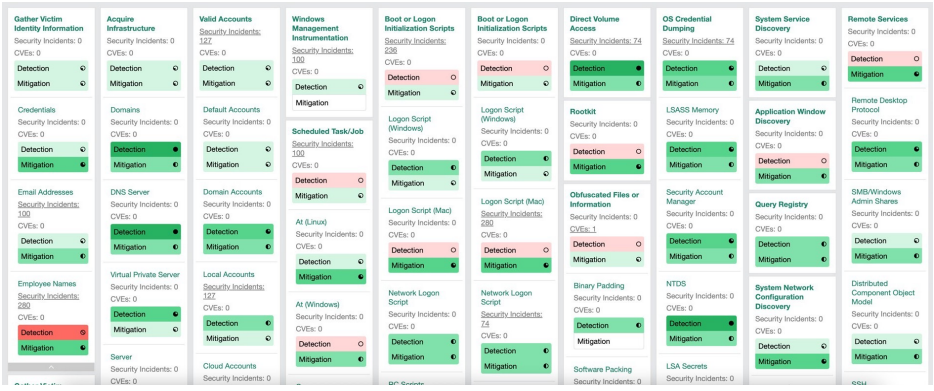
A playbook library gets you started quickly, and hundreds of integrations and apps can be downloaded from the ServiceNow store. Orchestration packs for integrated security products facilitate common actions, such as firewall block requests. For instance, routine phishing and malware response can be fully automated, as well as approval requests and threat enrichment. Within workflows, AI simplifies identification of critical incidents and expedites assignment to the right analysts and responders. A SOC efficiency dashboard provides ongoing visibility into trends and helps identify areas for further automation and risk reduction.

Make your team more satisfied and productive

Automation helps your workforce scale to succeed in a mode of constant change. Security analysts can focus their attention from basic, repetitive duties to more challenging work. At the same time, success and morale go up as integrated intelligence and asset data help prioritize investigations based on risk.

Proactively manage threat exposure using MITRE ATT@CK and threat intel

The MITRE ATT&CK framework is integrated into playbooks and analytics. The latest adversarial and threat insights enable security teams to optimize workflows, tools, and skills against evolving attack techniques to profile and predict active attacker behavior, and guide response. It even tells you where to boost defenses.



Key Features

Now Assists & AI Agents for SIR

Streamline the incident review process gaining contextual understanding in seconds rather than minutes.

Major Security Incident Management

Centralize operations to better prepare and respond to high profile security incidents such as ransomeware, data breaches, targeted attacks

DLP Incident Response[1]

Integrate DLP Incident Response with your DLP tool to reduce exposure and respond quickly to contain data loss events

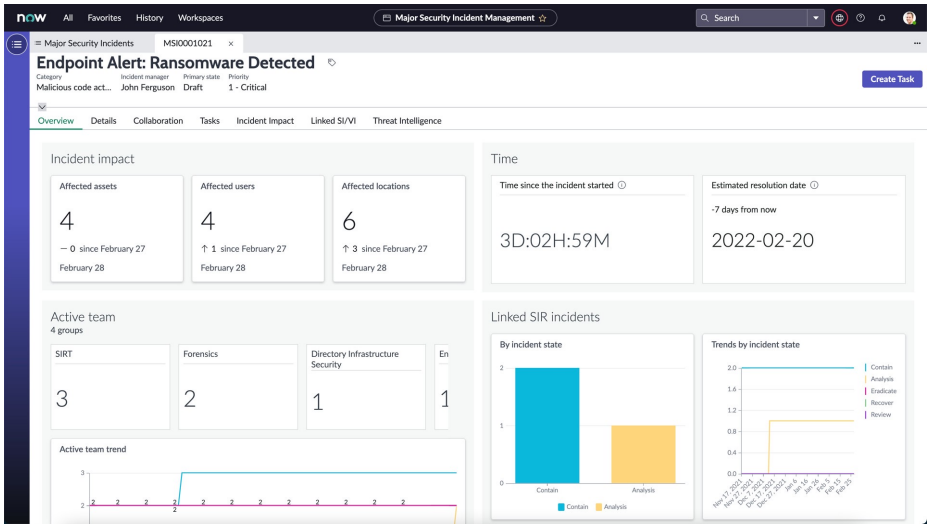
CISO Dashboard

Assess exposure, measure and monitor progress against key metrics, and get real-time, actionable insights about changing security posture

MITRE ATT&CK

Optimize defenses, forecast attack behaviors, predict targets, and define and automate response based on attacker behavior, TTPs, and risk

[1]DLP Incident Response is a product within the ServiceNow Security Operations portfolio.



Major Security Incident Management creates a cross-functional command center.

Modernize Your SOC with ServiceNow
To elevate your security capabilities, Security Incident Response incorporates many process and productivity improvements. Analysts can easily view and track response tasks that run in parallel. The system will remind assignees if their tasks aren't completed on-time per SLA thresholds, or it can escalate tasks if necessary. Incidents are automatically associated with relevant security knowledge base (KB) articles for reference.

Bridge security, risk, and IT to remove friction, risk, and errors
Security teams need to collaborate with IT and risk counterparts for effective investigation, management and resolution of incidents. With Security Incident Response, security teams can access a wealth of contextual information about services, assets, owners, risks, and compliance without extensive integration work. Playbooks pull this information automatically, replacing emails and spreadsheets.

Orchestrate enterprise-wide incidents with ease
Data breaches, ransomware, and zero-day vulnerabilities are just some of the big and breaking problems that trigger crisis response. As regulators shorten disclosure windows, you need to be prepared and ready. With ServiceNow, purpose-built workspaces connect stakeholders from execs to IT to legal to PR in a consistent experience with appropriate data access. This crisis command center supports the collaboration, efficiency, and evidence-handling essential to critical situations.

Elevate your response process with the power of AI
With Now Assist for Security Incident Response and AI Agents security teams can gain contextual understanding of incidents in seconds rather than minutes! With a single click analysts can now get a concise summary of security incidents, automatically generating detailed resolution notes and receiving immediate, relevant answers to specific questions about security incidents. The integrated, interactive AI saves analysts valuable time by streamlining the incident review process, expediting time to resolution and boosting productivity.

Visibility and assessment for continuous performance improvement
Maturity is a journey that each organization travels at their own pace. ServiceNow quantifies processes and captures key metrics and indicators to give you visibility into what is happening, what is working, and what could improve your security posture and performance. Built-in analytics drive role-based dashboards and reporting so leaders and analysts can identify trends early and act—tuning playbooks, protections, staffing, and training to meet this dynamic threat evolution.

Accelerate your team's success with the ServiceNow Security Operations portfolio.

> "Security Incident Response allows SAS to manage the lifecycle of security threats. SAS can now understand the nature of security incidents, spot trends, and deal with bottlenecks.
>
> Threats are identified within 1 minute, contained in less than 10 minutes, and analyzed within the hour.
>
> —Scandinavian Airlines

servicenow

SN_DataSheet_SecurityIncidentResponse_02012024

Transform Enterprise Security

Wanted: Cyber resilience under pressure

ServiceNow Security Operations helps security teams scale faster, smarter and more efficiently, enabling and automating critical collaboration of data and process between IT, security, and risk to effectively respond and remediate threats. It brings in security and vulnerability data from your existing tools and uses intelligent workflows, automation, and a deep connection with IT to streamline security response. ServiceNow Security Operations helps you use the power of the Now Platform to reduce cybersecurity risk and drive cyber resilience.

Transform investigations and response

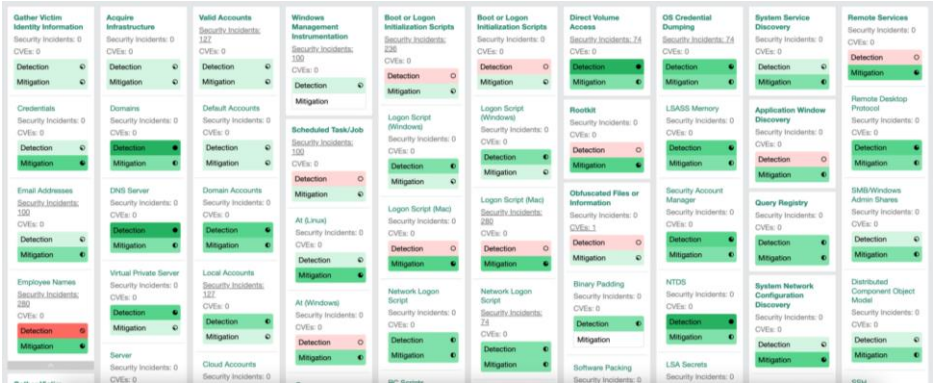
ServiceNow® Security Incident Response, a security orchestration and automation response (SOAR) solution, helps you rapidly respond to evolving threats while optimizing and orchestrating enterprise security operations. Security Incident Response eliminates the errors and friction natural to manual handoffs across systems, teams and responsibilities. Integrations, playbooks, dashboards, and a common data model for enterprise case management to expedite investigation, response, and remediation across IT, Security, and Risk.

Automate away the basics to focus on the critical

A playbook library gets you started quickly, and hundreds of integrations and apps can be downloaded from the ServiceNow store. Orchestration packs for integrated security products facilitate common actions, such as firewall block requests. For instance, routine phishing and malware response can be fully automated, as well as approval requests and threat enrichment. Within workflows, AI simplifies identification of critical incidents and expedites assignment to the right analysts and responders. A SOC efficiency dashboard provides ongoing visibility into trends and helps identify areas for further automation and risk reduction.

Proactively manage threat exposure using MITRE ATT@CK and threat intel

The MITRE ATT&CK framework is integrated into playbooks and analytics. The latest adversarial and threat insights enable security teams to optimize workflows, tools, and skills against evolving attack techniques to profile and predict active attacker behavior, and guide response. It even tells you where to boost defenses.



Orchestrate enterprise-wide incidents with ease

Data breaches, ransomware, and zero-day vulnerabilities are just some of the big and breaking problems that trigger crisis response. As regulators shorten disclosure windows, you need to be prepared and ready. With ServiceNow, purpose-built workspaces connect stakeholders from execs to IT to legal to PR in a consistent experience with appropriate data access. This crisis command center supports the collaboration, efficiency, and evidence-handling essential to critical situations.

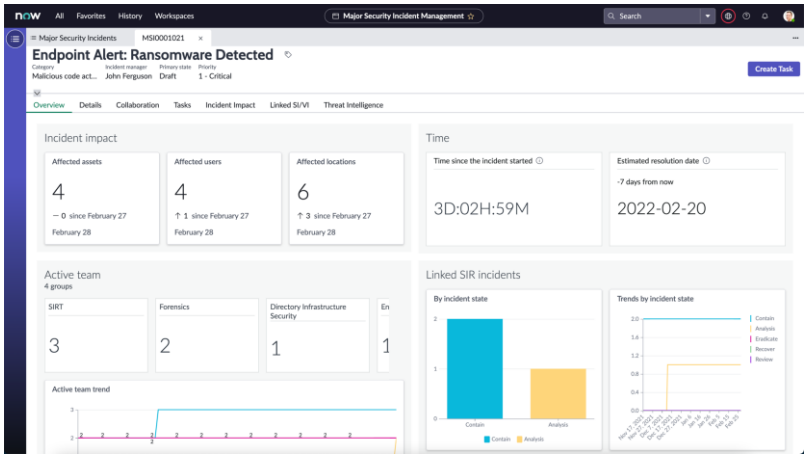
Key Features: Incident Response

- Major Security Incident Management
- DLP Incident Response[1]
- CISO Dashboard
- MITRE ATT&CK
- Proven Playbooks

Key Features: Vulnerability Response

- Modern collab spaces
-
- Expansive visibility
-
- Automation, not backlogs
- Prioritization your way
- Vulnerability Solutions Management
- Performance analytics

[1]DLP Incident Response is a product within the ServiceNow Security Operations portfolio.



Major Security Incident Management creates a cross-functional command center.

Modernize Your SOC with ServiceNow

To elevate your security capabilities, Security Incident Response incorporates many process and productivity improvements. Analysts can easily view and track response tasks that run in parallel. The system will remind assignees if their tasks aren't completed on-time per SLA thresholds, or it can escalate tasks if necessary. Incidents are automatically associated with relevant security knowledge base (KB) articles for reference.

Bridge security, risk, and IT to remove friction, risk, and errors

Security teams need to collaborate with IT and risk counterparts for effective investigation, management and resolution of incidents. With Security Incident Response, security teams can access a wealth of contextual information about services, assets, owners, risks, and compliance without extensive integration work. Playbooks pull this information automatically, replacing emails and spreadsheets.

Harden the attack surface exploding across cloud, infrastructure, and applications

According to the Enterprise Strategy Group (ESG) Security Hygiene and Posture Management report, nearly 7 out of 10 respondents admitted to a cyber breach resulting from exploitation of unknown, unmanaged, or poorly-managed internet-facing assets.

Vulnerabilities pose a serious threat to business reputation and data security. Methods to exploit vulnerabilities are growing more sophisticated, with cybercriminals increasingly leveraging machine learning and artificial intelligence to thwart traditional vulnerability response mechanisms.

One of the operational dilemmas for security teams is their dependency on IT teams and tools for scanning and asset data and for actual patching or mitigation of issues. It really takes a team. And almost every organization's security and IT teams struggle to keep up with the sheer volume of vulnerabilities in an ever-increasing, ever-diversifying attack surface.

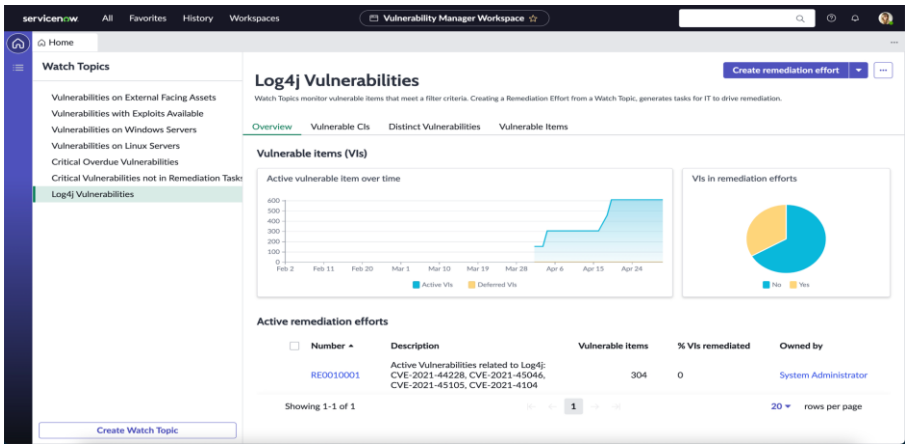
Transform operations with ServiceNow risk-based vulnerability management

ServiceNow Vulnerability Response synthesizes asset, severity, exploit, risk, and threat intelligence insights into automated workflows for fast, reliable prioritization and remediation. App integrations on the store plug in multiple cloud, application testing, penetration testing, vulnerability assessment, OT/IT discovery, and asset management tools for fast time to visibility across your evolving attack surface.

> “Security Incident Response allows SAS to manage the lifecycle of security threats. SAS can now understand the nature of security incidents, spot trends, and deal with bottlenecks.
>
> Threats are identified within 1 minute, contained in less than 10 minutes, and analyzed within the hour.
>
> —Scandinavian Airlines

Coordinate with application owners, developers, and the risk team

With broad DevOps and Agile adoption, internal software developers present a special challenge. Our included ServiceNow Application Vulnerability Response unites your processes and teams to improve security at the speed of software development. You can prioritize vulnerabilities and coordinate fixes with developers in deployed applications. You can also identify, prioritize, and remediate vulnerable misconfigured software with ServiceNow Configuration Compliance.



Security and IT teams build trust with a collaboration space for vulnerability, risk, and remediation activities.

Use in-depth IT and asset insights to prioritize and build up an accurate CMDB

In the ESG survey, the top source of prioritization and patching data is vendor products in use, especially those with high-criticality. When used with the ServiceNow Configuration Management Database (CMDB), Vulnerability Response provides a comprehensive view of all vulnerabilities affecting a given asset or service, as well as the current state of all vulnerabilities across the organization.

Respond efficiently across security and IT when critical vulnerabilities appear

When critical vulnerabilities are found, Vulnerability Response can automatically initiate emergency response workflows that notify stakeholders and create high-priority patch requests for remediation owners.

Vulnerability managers can create watch topics to help them quickly identify risky vulnerabilities, such as a high risk score, specific critical CVE, exploitable vulnerabilities, overdue tasks, and more, allowing for easier, more precise monitoring. Stakeholders can continuously monitor real-time status of patching progress and ensure process visibility across security and IT.

For maximum impact on vulnerability risk, you can also easily identify the most beneficial activities with Vulnerability Solution Management. It works by matching vulnerability scan data against Microsoft or Red Hat's solution databases to recommend which to deploy based on supersedence. Once the best solution is found, use Patch Orchestration to complete the last mile of the vulnerability journey: automating the patching process via 3rd party patch tools.

Transform Enterprise Security

Security Incident Response and Vulnerability Response are part of the ServiceNow Security Operations portfolio. To learn more, please visit: **www.servicenow.com/sec-ops**

> "With ServiceNow, Prime has created a highly structured, efficient process. We know exactly where each vulnerability stands and what IT is doing to fix it.
>
> — Prime Therapeutics

servicenow

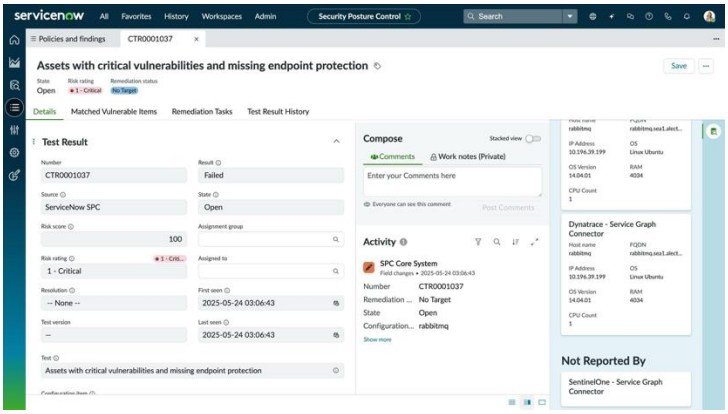
ServiceNow Security Posture Control (SPC)

Gain visibility and management of your growing attack surface

Two questions every cybersecurity team needs to answer are: what assets are we responsible for protecting and where are our coverage gaps? According to the *EntryZero*, 76% of organizations in 2024 were compromised via an unknown, unmanaged, or poorly managed internet-facing asset. It is critical to monitor which assets are protected or managed by security tools, such as endpoint protection, anti-malware, endpoint management, encryption etc. When these assets are deployed in public cloud infrastructure, any accidental configuration errors risk exposing assets to the internet and should be strictly monitored.

Although there are vendors offering products in the category of 'Cyber Asset Attack Surface Management' (CAAASM), some things to consider include:

- Does the product offer an end-to-end solution for detecting security gaps and managing response workflows
- What level of investment and upkeep is needed to integrate and leverage products with their own databases?
- Can the solution be integrated seamlessly into existing vulnerability management programs? Does is require custom mapping of alerts to GRC control objectives?



Introducing ServiceNow Security Posture Control

Security Posture Control is a CAASM solution that provides an end-to-end solution offering asset security detection, response, and compliance that unifies attack surface coverage data, and helps to identify the highest risk gaps.

Detection

Security Posture Control provides visibility into asset security coverage gaps such as missing endpoint protection agent or missing configuration & patch management agent on enterprise assets, including on-prem devices and cloud-based virtual machines. This also includes assets with high-risk combinations involving missing security tools, vulnerabilities, internet exposure etc.

Security Posture Control leverages the vulnerability data gathered from third-party vulnerability assessment tools, including Qualys, Rapid7, Tenable and more, to identify high-risk assets.

Key Highlights

Frictionless Approach
Security Posture Control uses API-connectors (Service Graph Connectors) to collect asset data from multiple security and IT tools to generate the insights.

CMDB maturity
Operationalize Security Posture Control through Service Graph Connectors integrating with various tools to help mature CMDB asset data.

Asset risk engine
SPC acts as a central risk calculator by using security configs, asset data, vulnerabilities, and IRM exceptions to identify risky assets.

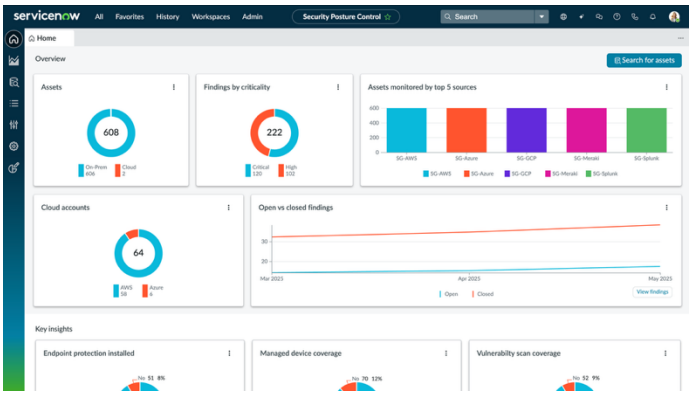
Integrated platform
Security Posture Control comes with built-in better together use cases with CMDB, Integrated Risk Management (IRM), and Vulnerability Response.

Response
ServiceNow captures asset and cloud security findings in Configuration Compliance, enabling automated workflows for issue assignment, group, remediation, and exception management. Because findings are linked to MCDB Cis, ownership identification and change request handling are built-in

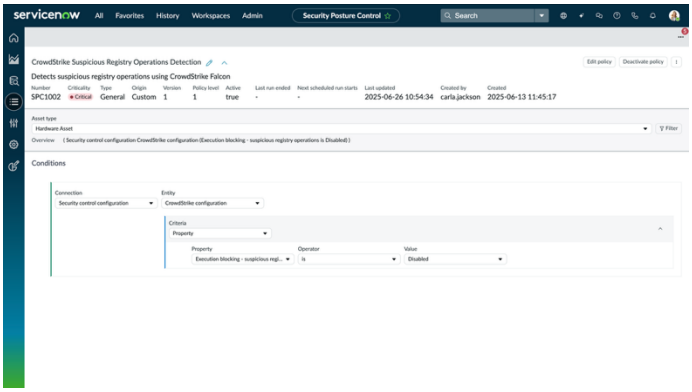
Compliance
The built-in integration between Configuration Compliance and Integrated Risk Management lets compliance managers view real-time control status based on SPC policy evaluations.

SPC includes out-of-the-box policies to detect assets with the following security gaps:

- Assets missing security tools (e.g. endpoint protection, antimalware, etc.)
- Unmanaged assets (assets missing configuration and patch management agent or endpoint management solution)
- Assets missed by vulnerability scanners
- Assets missing security tools and having critical vulnerabilities
- Cloud assets exposed to internet and having critical vulnerabilities and/or security tool coverage gaps



Customers can also create their own policies and custom insights based on asset metadata, security tool configuration data, and vulnerability data to monitor assets violating internal security standards.



Better together with Vulnerability Response

Customers using ServiceNow Security Posture Control and Vulnerability Response together can benefit from the built-in capabilities that allow vulnerability managers to define remediation targets and risk scores for vulnerabilities, based on policy violation data from Security Posture Control. For example, assets missing endpoint protection or cloud assets facing internet with critical security tools missing can be prioritized for remediation/patching of vulnerabilities.

ServiceNow Risk Management

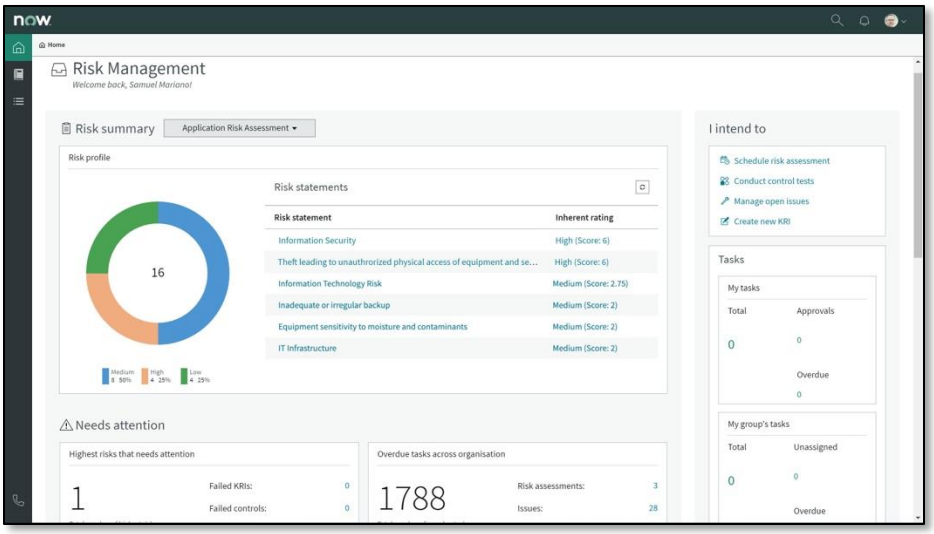
Managing IT and business risk across the enterprise

With the increasingly complex business environment and threat landscape, it has become essential to identify, assess and manage risks more holistically. Risk is inherent as organizations deal with products, services, processes, systems, technologies, vendors, people and more. Risks arising from any of these can cause business disruption, impacting strategic objectives and resulting in financial losses and reputational damage.

ServiceNow Risk Management helps identify risks across organizational siloes through continuous monitoring and the Advanced Risk Assessment engine. The engine is built to address risk through an integrated risk framework. The framework provides the ability to quickly identify, prioritize, and react to a wide variety of risks emerging throughout the organization with a single lens and common language. This unique approach enables you to do business with confidence knowing the risks and opportunities.

Respond to risks in real-time with ServiceNow

ServiceNow Risk Management helps you detect and assess the likelihood as well as business impact of an event based on data aggregated across your extended enterprise; and respond to critical changes in risk posture.



Risk Management homepage highlights enterprise risks

Risk Management works closely with Policy and Compliance, Audit, Vendor Risk, Business Continuity Management, and Continuous Authorization and Monitoring.

- Policy and Compliance Management - Automate best practice lifecycles, unify compliance processes, and provide assurances around their effectiveness.
- Audit Management – Scope and prioritize audit engagements using risk data and entity information to eliminate recurring audit findings, enhance audit assurance, and optimize resources around internal audits.

Identify risks in real-time

Configure real-time business and IT service performance data and identify vendor requirements to enable automated controls testing. Define thresholds as indicators for continuous monitoring of your extended enterprise

Increase performance

Risk management embedded in automated cross-functional activities eliminates work interruptions

Unparalleled user experience

An intuitive risk management workspace is tailored to your unique needs, with navigation streamlined for just what a Risk Manager cares about.

Effectively communicate risk

Real-time insights and role-based dashboards make reporting at all levels easier and faster.

Improve strategic planning and decision making

Fine-grained business impact analysis, task management, and contextual alignment with the CMDB on a single platform provides cross-functional visibility to identify, prioritize, and appropriately respond to risks

Stay on top of risks

Mobile interfaces provide the information you need to do your job anytime and anywhere.

Extend your ServiceNow investment

The single platform of engagement offers orchestration, easy integration, data ingest and publication

- Vendor Risk Management – Consolidate risks associated with third parties alongside enterprise risks for a holistic view across the extended enterprise.
- Business Continuity Management and Operational Resilience – Identify and track the risks associated with business disruptions and disasters as a key part of a robust integrated risk management program.
- Continuous Authorization and Monitoring – Automate the processes that support risk management frameworks including NIST RMF used to achieve certifications such as CMMC, bring systems on-line faster, and enable continuous authorization.

The importance of risk management

Compressing the time to identify, prioritize, and respond to changes in your risk and compliance posture is imperative. To do so you need to continuously monitor data across your extended enterprise to speed detection of emerging risks. Automating the appropriate remediation and risk treatment actions across business and IT processes breaks down the silos and ensures a rapid response.

The ServiceNow AI Platform's collaboration engine and issues management capabilities work across risk and compliance applications, and with the Vendor Portal to create a shared understanding and facilitate timely decisions.

Create a risk register

Establish a standard taxonomy across the business, risk, compliance, and audit with a risk register or risk catalogue that can be broken down to a granular level. This provides the flexibility to drill down as you navigate your maturity journey. It also drives clear ownership. Having an inventory of all risks and controls in a centralized repository or risk universe makes it easier to aggregate risks at various levels of the hierarchy, providing visibility into the areas that need focus.

ServiceNow is uniquely positioned to connect the risks and controls to lines of business, functions, assets, processes, business services and many other components in the Configuration Management Database (CMDB) - providing business context. ServiceNow Risk Management enables you to create and map risks and controls to the flexible enterprise hierarchy, reflecting today's matrixed organization.

Automated risk assessments

Evaluate inherent risk, the effectiveness of the control environment, and residual risk through manual or automated risk assessments. The built-in Advanced Risk Assessment engine is flexible enough to support multiple risk frameworks simultaneously, irrespective of whether it is top-down or bottom-up, quantitative or qualitative, simple or complex in nature.

ServiceNow Risk Management powers real-time risk assessments using automated factors that can fetch information on any data point in the ServiceNow AI Platform. Automation will enable you to be agile in responding instead of muddling through with stale data.

Implement real-time monitoring

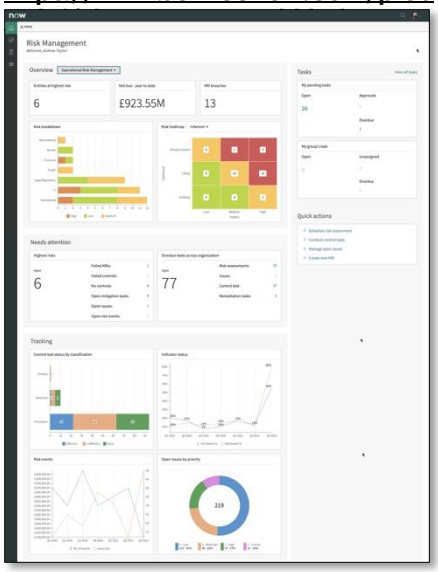
ServiceNow Risk Management identifies non-compliant controls, monitors high-risk areas, and manages the Key Risk Indicator (KRI) and Key Control Indicator (KPI) library with automated data validation and evidence gathering.

Because data from applications across the enterprise is consolidated in the ServiceNow AI Platform you can gather any information and move from a point in time methodology to continuously monitoring risk for any department or function.

Provide visibility at all levels

Interactive real-time dashboards provide overviews of your risk and compliance posture. The ability to provide decision-makers, at all levels of the business, with up-to-date information regarding the organization's risk posture is critical in a risk management program. You will have all the information necessary to make informed decisions to manage risk effectively. The platform also enables users to easily create their own reports.

Learn more at:
https://www.servicenow.com/prod



The Risk Management workspace for Operational Risk Managers

servicenow

SN_DataSheet_Risk-Management_MAY_2022

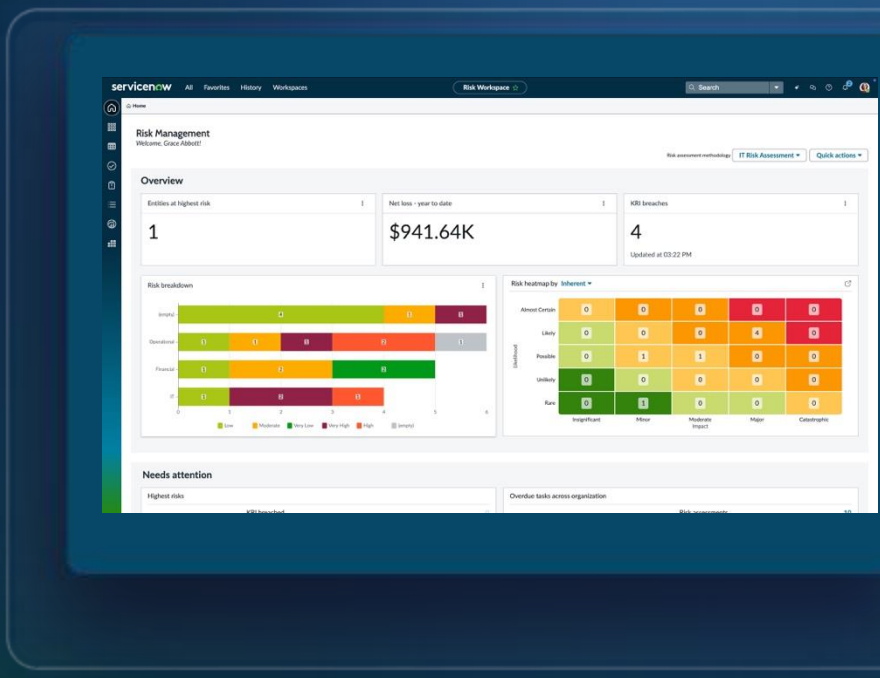
Integrated Risk Management

Turn risk into resilience

Overview

ServiceNow Integrated Risk Management (IRM) unifies governance, risk, and compliance on a single AI-powered platform. It replaces manual, fragmented processes with automated workflow and real-time visibility, connecting IT, security, and the business for more holistic risk management.

With IRM, organizations accelerate risk response, streamline compliance, and improve decision-making to drive operational resilience, reduce regulatory exposure, and build trust with customers and regulators.



Key features

1. **Policy & Compliance Management**
   Manage a centralized governance framework, manage the full policy and control lifecycles, and automate compliance testing.
2. **Regulatory Change Management**
   identify upcoming regulatory changes, assess their impact, and implement changes to mitigate risks and non-compliance.
3. **Compliance Case Management**
   Report, investigate, track and resolve issues and exceptions related to compliance.
4. **Risk Management**
   Identify, assess, and continuously monitor risks using qualitative and quantitative metrics and benchmarks.
5. **Continuous Authorization & Monitoring**
   Automate control testing, continuously monitor for compliance violations, and generate issues and action plans.
6. **Audit Management**
   Simplify audit planning and execution with automated workflows, evidence collection, and real-time reporting.

Benefits

See everything that matters

Get a connected, real-time view of risks, controls, and compliance across the enterprise so you can prioritize what's most important and make more confident decisions.

Stay audit-ready

Embed compliance into daily workflows, automated control testing, and centralized audit evidence collection mean no more scrambling when regulators and auditors come calling.

Scale trust with built-in governance

Establish consistent governance, monitor for emerging risks, and align with evolving regulations to scale compliance and trust as your organization grows.

75%

Reduced control attestation time

700+

Hours/year saved in risk management

Learn more about Integrated Risk Management

Contact us

View demos

Core capabilities

Unified Data Model

A single source of truth for risk and compliance data.

AI & GenAI Automation

AI Agents and Now Assist automate assessments, issue summarization, and monitoring for faster decision-making.

Continuous Controls Monitoring

Detect failing controls between assessments using performance analytics.

Smart Assessment Engine

Automate tailored risk assessments with flexible templates and dynamic scoring.

Role-Based Dashboards

Real-time insights tailored for executives and all three lines of defence.

Integration Hub

Connects with systems of record and external data sources.

Mobile & Portal Access

Consumer-grade UX for accessibility across devices.