Boost cybersecurity resilience with security, risk, and IT working together

Rapidly expanding enterprise attacks from many locations and multiple attack surfaces that include the cloud, have created blind spots that make it difficult for organizations to accurately understand, quantify, and mitigate cyber and IT risk.

When it comes to managing cyber risk and cybersecurity threats, legacy tools and siloed solutions can keep you up at night. Worries such as disconnected technology and teams that make collaboration difficult and managing risk and security ineffective and costly. And the volume of vulnerabilities and alerts that make it impossible to keep up. Manual and inadequate controls don't help.

The combination of ServiceNow® Security Operations and Integrated Risk Management have the power to address these complex threats. As one, they can help continuously manage risk and security across the organization through bi-direction collaboration and shared data, to boost cybersecurity resilience.

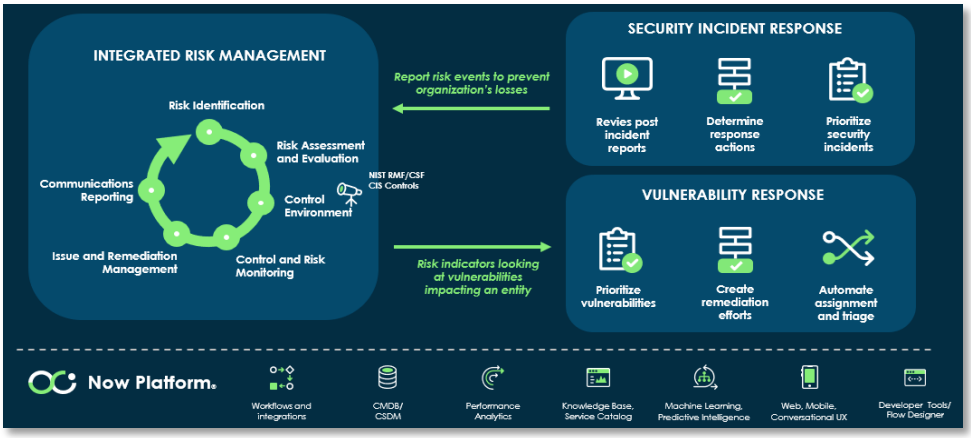


Figure 1: Bi-directional collaboration and shared data are key to a successful security and risk solution.

Realize the benefits of Risk and Security working together

Mitigate security risks and reduce costs by connecting security, risk and IT on an integrated platform - Although you may have systems, technology, processes, and tools in place for technology and security risk management, they often operate in silos with no centralized access to shared data. The processes are disconnected, and control functions are disparate, each having its risk-identification processes, reporting structures, and IT systems. Disconnected teams and data silos make providing assurance for IT and cyber risk or security regulations a herculean effort.

The ServiceNow Platform is the "platform of platforms" for tech and security workflows – it creates a seamless enterprise system of action that connects tools, systems, people, and processes.

ServiceNow empowers organizations to integrate real-time controls and futurize risk and compliance operations by taking the right data to the right people at the right time, to make the right decisions and take the right actions. Whether that is a control owner seeing an issue before it becomes an audit finding or the CIO or CRO having the confidence that the data they bring to the board is an accurate reflection of the organization's security, risk, and compliance posture.

Mitigate cyber threats with security, risk, and IT working together

Integrated Security and Risk

Easily create risk events within Security Incident Response or policy exceptions within Vulnerability Response with a single click - embedding risk management and compliance into familiar user experiences and making it a frictionless part of your daily work.

AI/ML & Automated workflows

Cross-functional workflows and AI/ML foster collaboration and response to issues and tasks.

Continuous Monitoring and Advanced Risk Assessments

Define controls that identify when security best practices are lacking, vulnerabilities or configuration errors on-prem or in the cloud are lingering beyond defined SLAs. Dynamically updated responses in risk assessment ensure risk scores are accurate for a strong risk and security posture.

Accelerate compliance

Use accelerators to implement security regulations or frameworks more quickly for a faster time to value.

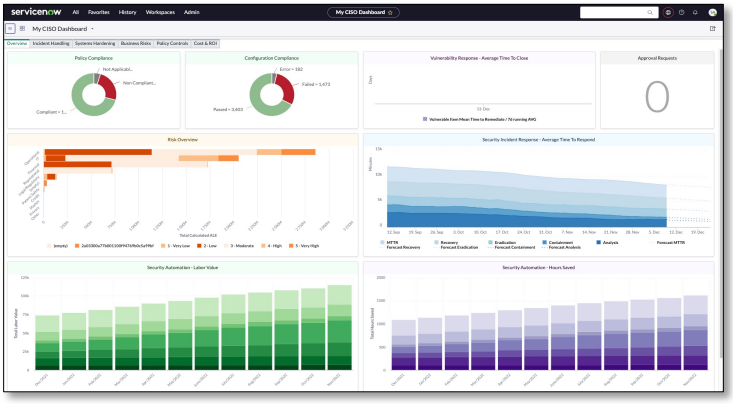
CISO Dashboard

Gain insights into risk or security threats from a single, tailored dashboard.

Single platform and User-Friendly Experiences

A single platform and intuitive workspaces streamline data sharing and bi-directional collaboration between risk and security teams.

Engage the frontline and continuously monitor for a comprehensive real-time view of risk and compliance - We have a singular focus on the employee experience to help engage those that are traditionally forgotten– frontline employees.



Capabilities designed for the front are employee portals, chatbots, and mobile solutions, while workspaces deliver a tailored role-based experience for risk and security teams, the internal audit team, and executive stakeholders.

Enabling all stakeholders in an organization to participate in managing risk, compliance and security provides a more complete view and a more robust cybersecurity posture. The Now Platform enables collaboration across departments and teams.

Figure 2: The CISO dashboard provides insight into security and risk

Proactively anticipate vulnerabilities and mitigate ever-changing security risks - Vulnerability Response and Security Incident Response (SIR) proactively detect and remediate cybersecurity threats. Integrations with SIEM tools within your organization, capture and automatically prioritize incidents, determine appropriate response actions and then perform a post incident review to capture the work done, the lessons learned and impact on your organization. When a security incident is identified that might have a negative impact to the business, you can report a risk event to IRM with the click of a button within the SIR application. Within IRM the risk will be analyzed and prioritized for an appropriate response.

Vulnerability response works with vulnerability scanners to not only identify active vulnerabilities but also mis-configurations. Mis-configurations can also be identified in the cloud. If these linger past the agreed upon SLA a risk and associated issue will be generated within IRM. Policy exceptions in IRM can be generated within Vulnerability Response for any control failures that cannot be addressed. Unpatched vulnerabilities and configuration errors are common pathways for attackers.

Continuously monitor controls within IRM to identify compliance violations, risks, and vulnerabilities. Using dynamically updated responses within risk assessments also helps identify when risk levels change – and keeps risk scores current.

For a faster time to value, use the NIST CSF, RMF, or Cybersecurity Controls Accelerators - delivering out-of-the-box control and indicator templates for common regulations and security frameworks. Real-time visibility is essential for quickly addressing threats or changes to your risk posture. Siloed visibility and governance makes complying with evolving regulations difficult and identifying cyber risk challenging.

Anticipate, prevent, recover, and adapt to business disruptions and uncertainty – The CISO dashboard consolidates insights from Security Operations and Risk for single overview of the risk and security posture of the business. Risks include business continuity issues, vendors, applications, and IT process failure (ex., errors in change management).

Being able to quickly address issues is vital to a rapid recovery. IRM uses AI/ML to intelligently respond to risks including system disruptions. Risk events can be reported by frontline users or identified as part of a business rule or integration with Security Operations.

Enable successful implementations

There are many opportunities to learn not just the product but also implementation strategies for IRM and Security Operations. Now Learning Success Packs help deliver successful outcomes to projects. ServiceNow Expert Services not only assist in the implementation but also recommend implementation methodologies. There are several implementation partners that offer deep technical expertise and domain expertise in the solution you're deploying, ServiceNow Assure is a collaboration between ServiceNow and your selected Professional Services provider. And finally, you can take advantage of live and on-demand implementation and product training.

servicenow.