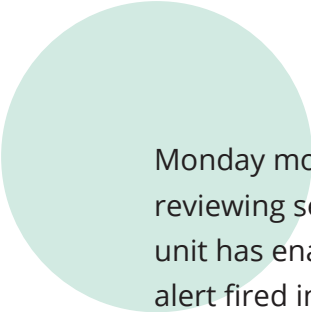


DIGITALLY
ENABLING THE

CYBER DEFENSE FUNCTION

Leveraging automation for both cyber risk and compliance programs amplifies visibility through tighter integration of an organization's IT asset inventory, cyber posture, and dependencies across the enterprise resulting in reduced risk and operational complexity





Monday morning, 8 a.m.—an IT risk and compliance analyst is tediously reviewing server compliance and hardening logs and discovers that a business unit has enabled remote access to a critical server. Thirty minutes earlier, an alert fired in the security operations center that hints of a possible intrusion but is obscured amongst a myriad of security warnings. At 9:15 a.m., a threat intelligence professional fires off an email about a new and active campaign targeting remote access, only to have it buried in the usual torrent of emails in his superiors' inboxes.

This is a very typical example in modern enterprises of IT professionals missing an opportunity to immediately identify and correlate essential details to manage a threat and associated risk. Does the security team have near-time access to infrastructure configurations? What type of data is on a potentially affected server? Is it sensitive customer data that must be reported? What critical business operations does the server support, and how big a hit could the business take if the server is taken offline? What business unit and business owner is responsible for the application(s) on that server?

Welcome to a day in the life of a typical enterprise IT and security function, where it is difficult to separate the signal from the noise (quite a bit of noise), resulting in missed opportunities, unheeded policies, and unread messages—all of which unnecessarily increase and blur organizational risk.

The risk is real. Deloitte's *The Future of Cyber Survey 2019* found that 90 percent of organizations had breaches of sensitive production data in test and development environments in the past year.¹

That's because many organizations are challenged in simply mapping the totality of their IT footprint, where sensitive data resides, who has access to it, and what applications rely on that data.

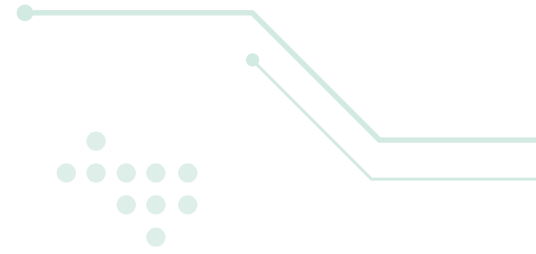
At times, it's equally daunting to identify ownership, asset criticality, and—of those—which might be vulnerable to specific threats and campaigns. Adding to the challenge is a lack of clarity on which policies and controls go unheeded or are ineffective as well as what laws, regulations, or standards have potentially been violated or are out of compliance.

Fortunately, enterprise workflow automation and integration can help address these challenges and reduce risk.



Deloitte has been rapidly innovating with solution provider ServiceNow to bring such a technology solution to bear on this risk management problem. The solution can provide IT managers greater visibility into risk and helps enable them to manage it more strategically—that is, to allocate resources to the areas of the organization that need it the most.

The business challenge



As the world becomes more connected, cyber threats grow in number and complexity—and not just because of malware. Much of the risk comes from within the organization through global expansion, diversification of products/services, mergers and acquisitions, business process outsourcing, and increased reliance on technology to support critical operations.

In response, many organizations deploy multiple risk, compliance, and security solutions to help manage the many dimensions of this ever-expanding cyber footprint. Many companies deploy dedicated teams to separately monitor for security incidents, scan IT assets for vulnerabilities, review access controls, perform due diligence on entities they acquire, and keep tabs on vendor performance.

In many cases, however, these teams work in isolation or, at best, have informal communication channels that may inhibit how they collaborate and limit the information they share with each other.

“ Oftentimes, we see organizations conducting important activities in silos, ”

says Mark Nicholson, principal with Deloitte & Touche LLP’s cyber risk services. “That can make it harder to address common concerns and leaves potential security gaps that may be addressed in one area but not another.”

Gaining a complete understanding of your organization’s risk posture depends on better visibility into four main areas:

- 1** The organization’s IT assets (including hardware, software, cloud services, and associated metadata like owner and application/server mapping)
- 2** The risks associated with each asset, taking into account how critical the asset is to operations, the data involved, any third-party support, and the asset’s physical location
- 3** The controls in place to protect and maintain the security, reliability, and integrity of the asset
- 4** Risk intelligence related to the risk posture of each asset, including any known control gaps, vulnerabilities, and associated security incidents

Broader visibility across these areas can allow organizations to strategically assign cybersecurity resources to assets that need them the most.

ServiceNow Security Operations, IT Asset, and Risk Management modules equate to a first-of-its-kind comprehensive cloud-based solution. It can deliver automation and coordinate critical workflows and practices needed to both understand and manage cyber risk. Further integration helps to allow for cross-program sharing to break down silos, optimize collaboration, and enable enterprise-level reporting and analysis.

The technology challenge

Automation is a powerful capability that offers unprecedented advantages to security organizations. But it often presents a configuration challenge that organizations should address for best results.

“The out-of-the-box workflows provided by ServiceNow align with leading practices.”

However, as with any technology implementation, modifications may be needed to tailor them to an organization’s specific business practices, industry requirements, and regulatory expectations,” explains Dan Williams, managing director at Deloitte & Touche LLP focused on technology strategy.

How new technology helps solve the problem

At its core, ServiceNow helps solve the challenges of an increasingly complex and siloed cybersecurity operation by acting as a “platform of platforms.” In other words, it connects multiple automated solutions with minimal disruption to existing IT investments.

“ServiceNow is like the plumbing that allows data to flow freely across different risk and compliance programs,” Williams says. Leveraging this helps give the organization a clear understanding of what the most important (and riskiest) assets are and why. This type of insight allows the risk treatment for each IT asset to be tailored considering how important the asset is to the organization and its ongoing operations.

This kind of integration provides a single view into a variety of potential issues, including:

- What risks are inherent to a specific asset
- End-of-life and license expiration(s)
- The criticality of an asset
- The volume and types of data contained within the asset
- What controls may be missing from an asset
- What vulnerabilities exist for an asset
- If a third party supporting an asset lacks a data privacy program
- How these deficiencies may adversely affect operations
- Accurate business IT accountability (ownership) details

ServiceNow also integrates workflows and task management to surface the most critical issues to the right people at the right time.

Additional benefits to the security organization and other departments include:

- Near real-time data providing enhanced, multi-dimensional visibility into risk
- Optimized collaboration and information-sharing for each department or job function around common goals
- Increased efficiencies across programs, reducing the time required to aggregate data for enterprise reporting and analysis

These benefits can give IT and security staff more time to spend on running the organization instead of routing issues and performing administrative tasks.



A financial services company suffered a data breach when hackers intercepted unencrypted transaction data handled by a third-party vendor.

Afterwards, the company turned to Deloitte to help implement ServiceNow for risk management.

Now, the company runs ServiceNow's Vendor Risk Management solution to help ensure that all vendors remain compliant with company and industry standards for data security, including in-transit encryption.

The company can now see what vendors handle what IT assets and how they manage data on those assets. The result is a comprehensive overview of the company's risk profile, giving IT managers a powerful tool for protecting the company's most valuable asset: its customers' data.

The enterprise value proposition

The benefits of a platform of platforms for cybersecurity don't stop with the security function; they can extend to the entire enterprise.

ServiceNow provides a single source of truth for IT assets that present the highest risk to the organization; which in turn helps IT prioritize resources for the IT assets that need them most. **The solution also can benefit:**

- Legal and compliance leaders, by giving them visibility into IT assets that harbor sensitive or personally identifiable information (PII), as well as those most vulnerable to attacks resulting in theft of PII
- Business continuity functions, by providing visibility into the IT assets that support critical business operations with near real-time information on critical assets that have experienced service disruptions
- Finance departments, by identifying which IT assets have undergone significant changes that may affect the integrity of financial data

“This integrated solution, if done correctly, doesn't just benefit the CIO, ”

says Williams. “Other C-suite leaders also gain access to risk intelligence that may be invaluable to their respective functions, allowing them to do their jobs more effectively as well.”





Getting started

An important first step in transitioning to an integrated risk management solution such as that offered by ServiceNow is getting everyone on the same page. This means that all program owners agree upon a common data model that includes:

- A single source of truth for an organization's IT assets
- A shared list of business needs and prioritization for meeting them
- Standardized definitions for various types of risk to ensure that everyone agrees on what they are and how to manage them
- A common controls library so that similar type IT assets receive a standard set of controls
- A shared policy framework to give users consistent levels of IT access across platforms and software based on their job functions

Choosing an experienced integration collaborator such as Deloitte, who understands your unique industry needs and regulatory requirements, can greatly aid this process.

The bottom line

As your organization's cyber footprint continues to grow, gaining full visibility into IT assets and the risk they carry often becomes more challenging. Fragmented systems and siloed functions developed to support these assets don't typically come with the tools or processes needed to communicate well with each other, compounding this problem.

Automating and integrating all solutions and programs in ServiceNow—with implementation support from Deloitte—can break through silos and provide the visibility IT and other departments need to keep their critical business assets secure.

For more about how workflow automation can help save time and free up resources for your organization, visit:

<https://www2.deloitte.com/us/en/pages/about-deloitte/solutions/servicenow.html>

or contact:

Mark Nicholson, manicholson@deloitte.com

Advisory Principal • Deloitte & Touche LLP

Daniel Williams, danwilliams@deloitte.com

Advisory Managing Director • Deloitte & Touche LLP

Mehdi Houdaigui, mhoudaigui@deloitte.com

Senior Manager • Risk and Financial Advisory • Deloitte & Touche LLP

¹ Deloitte, "The Future of Cyber Survey 2019," <https://www2.deloitte.com/us/en/pages/advisory/articles/future-of-cyber-survey.html>, accessed April 5, 2020.

As used in this document, "Deloitte" means Deloitte & Touche LLP, which provides audit, assurance and risk and financial advisory services and Deloitte Consulting LLP, which provides strategy, operations, technology, systems, outsourcing and human capital consulting services. 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.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication 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 publication.