servicenow

Why technology, cyber, and privacy risk management are critical for digital transformation

How ServiceNow Integrated Risk Management helps you embrace the digital future

Organizations that effectively manage IT risk and respond in real time to emerging threats can confidently embrace the benefits of digital transformation.

Managing IT risk is more important than ever

For many organizations technology, cyber, and privacy risk are managed under the umbrella of information technology (IT) risk. Today, information technology is the engine that powers business innovation and competitive advantage. Organizations across the globe are accelerating digital transformation to deliver extraordinary customer experiences, radically increase productivity, and unlock new business insights. And while digital transformation isn't new, recent events and fundamental shifts in customer and employee expectations have resulted in dramatic acceleration as businesses respond to emerging realities such as hybrid work. This trend is only set to continue, with digitized processes and remote engagement models becoming the norm rather than the exception.

To achieve digital transformation, you need to effectively manage IT risk

While digital transformation is a huge opportunity, it's also an enormous risk. As organizations see an explosion of new systems and applications, there's a corresponding explosion in things that can go wrong. Managing this IT risk—whether that's technology risk, cyber risk, or regulatory risk—is imperative. Organizations that effectively manage IT risk and respond in real time to emerging threats can confidently embrace the benefits of digital transformation, while those that don't face business disruption, reputational and legal consequences, and a fundamental barrier to innovation.

Digital transformation is rapidly escalating IT risk

As an IT leader, you know that IT risk comes in many flavors. And digital transformation makes the risk landscape even more complex and dynamic:

- **Digital transformation** is dramatically increasing the pace of change and the volume of technologies that need to be understood and managed. Failure to follow well-defined processes to bring these technologies onboard creates both technical and business risk, particularly as more and more of your critical business functions move online.
- **Cyber risks continue to spiral upward,** with threats becoming ever more sophisticated—even AI-driven. Ransomware, system breaches, and data theft represent what is often an existential threat to organizations, and digital transformation significantly increases the attack surface with new applications, systems, and processes, hybrid clouds, and work-from-home models.
- **Rapidly expanding regulatory requirements**—and the specter of non-compliance—are exacerbating IT risks. And it's not just about SOX, HIPAA, PCI DSS, and other established frameworks. Data privacy is an overriding concern, with GDPR, CCPA, and other data protection regulations at the forefront. We're also seeing a tidal wave of environmental regulations, which have major implications for IT risk and beyond.

THE IMPACT OF DIGITALIZATION ON RISK

80%
of organizations report that digitalization is a strategic business objective today

61%
believe their risk profile has changed or will change significantly due to risks created by digitalization

14%
feel very confident that their organization will be able to control risks created by digitalization

Source: OCEG survey: The Impact of Digitalization on your Enterprise Risk Profile

Existing IT risk and compliance management approaches can't keep up

Why? Because they don't scale to the challenge of digital transformation:

- **IT risk and compliance exists in silos** across the organization, without a consistent, comprehensive framework for addressing the totality of IT risk. Risk is often managed in individual lines of business, with this redundancy leading to poor visibility, flawed risk management strategies and decision-making, and a lack of skilled resources to identify and respond effectively to risks.

- **Risk management typically relies on time-consuming manual processes,** including emails and spreadsheets. This further reduces visibility, makes the resourcing problem even worse, and leads to unacceptably high risk management costs. Ultimately, this means that these existing processes can't keep pace with rapidly expanding digital transformation initiatives.

- **Existing approaches are reactive,** relying on periodic attestations and audits to trigger risk responses. Because these approaches only look at a discrete point in time, there's no way to continuously monitor risk and proactively address new and emerging issues. This leaves organizations highly vulnerable, radically increasing their risk profile in the face of rapid digital change and escalating cybersecurity threats. And it leaves employees overwhelmed, frustrated, and ultimately burned out.

Are you ready to manage technology, cyber, and privacy risk and seize the digital future?

3 pillars for transforming IT risk management

At ServiceNow®, we work with organizations around the world to help them effectively manage IT risk as they accelerate their digital transformation programs. Based on the experience of our customers, we've identified three key pillars for success that allow them to proactively manage technology risk, cyber risk, privacy risk, and regulatory risk:

1. **Break down manual risk silos** through automation and integration. Replace spreadsheets and manual processes with end-to-end workflows, and automatically identify changes in your risk posture with integrated reporting on data consolidated in a single platform.

2. **Continuously monitor risks** rather than relying on periodic snapshots. Proactively identify risks and compliance issues by instrumenting workflows and continuously monitoring controls, and leverage automation to respond to issues in real time.

3. **Pre-emptively identify privacy and data loss risks** by using automated workflows to screen applications, projects, processes, and vendors that process personal data before they are implemented or onboarded. Then continuously monitor to identify and act on emerging privacy risks resulting from process changes or the addition of new data sources.

Let's look at each of these in more detail.

REAL-WORLD RESULTS

Bank with operations across 70+ countries manages all IT risk on a single platform with ServiceNow

A British bank operating in more than 70 countries struggled with IT risk management because it tried to manually manage multiple silos with SharePoint, Excel, and PowerPoint. When it had to comply with new UK operational risk regulations, things reached the breaking point.

By replacing manual systems and processes with a unified, automated ServiceNow solution on the Now Platform*, the bank was able to take control of its IT risk and rise to the challenge of the new regulations while lowering costs.

68%
of technology controls (630+ controls) are continuously monitored across all critical business processes

issues automatically created and assigned to correct owners

$6M
cost reduction through offboarding thrid party that previously supported manual risk processes

> “We were able to create a single system of action for technology risk and control management as well as meet the requirements of the new operational resilience regulations.

The average cost of a data breach is now more than $4 million[1]

Pillar 1

Break down manual risk silos

When you operate in silos with manual tools and processes, you don't have the visibility, scale, or consistency you need to effectively manage the risks of digital transformation. There's no easy, cost-effective way to:

- Consolidate information about critical business services, assets, and vulnerabilities to provide a unified view of risk.
- Implement formal best-practice risk management frameworks with consistent policies, controls, and indicators
- Automatically identify changes across the business that may increase risk
- Accurately assess their business impact based on affected services, type of data, and other factors
- Drive collaboration across teams because there is no common taxonomy or shared definition of what a high risk is
- Respond to ever-increasing regulatory reporting requirements
- Confidently understand and manage your overall risk posture

And the cost of getting this wrong can be enormous. For example, the average cost of a data breach is now more than $4 million[1], and fines for data privacy violations can reach into the tens—or even hundreds—of millions of dollars.

The ServiceNow difference

- A unified platform to manage all of your technology, cybersecurity, privacy, and regulatory risks,
- A single system of record for your entire IT estate, including infrastructure, applications, services, and processes.
- Define and apply consistent policies and controls across your business.
- Get fast time to value with accelerators for common risk management frameworks, including CIS, ISO, and NIST.
- Automate gathering of risk indicators, attestations, and other risk data.
- Easily integrate risk data from a wide range of third-party systems and applications.
- Automatically prioritize risks using comprehensive business and technical context already available in the Now Platform®.
- Leverage consolidated risk data to simplify regulatory reporting.
- Easily and consistently extend risk management to new systems as you accelerate digital transformation.

Pillar 2

Continuously monitor risk

When you manage IT risk manually, you're slow to detect new risks and even slower to respond to them. However, even if you integrate and automate your risk management processes, you still haven't solved the problem if you rely on periodic audits and attestations. With the pace of change in today's IT environments, a delay of weeks or months in detecting a risk just isn't acceptable. For example, unpatched security vulnerabilities are an open door for malicious actors—and there's no time to lose.

That's why it's critical to continuously monitor for risks and identify non-compliances in real time. By detecting issues as they happen, you have the opportunity to close the risk window, driving appropriate responses to mitigate these issues before they affect your business. Otherwise, it's like waiting for the replay instead of seeing the action unfold on the field.

The ServiceNow difference

- ✓ Access a comprehensive database of risk data that's constantly updated as changes happen.
- ✓ Automatically monitor Key Risk Indicators (KRIs) and test controls in real time.
- ✓ Embed risk indicators directly into your core IT processes and familiar user experiences such as employee portals.
- ✓ Automatically generate issues when there is an increased risk score, new risk, or compliance violation.
- ✓ Use smart issue management to automatically assign issues to the right individual or team for action.
- ✓ Quickly drive robust mitigation processes with cross-functional workflows that span multiple teams.
- ✓ Accelerate responses with AI-driven remediation recommendations.
- ✓ Simplify audits by automatically gathering accurate, up-to-date evidence

Pillar 3

Pre-emptively identify privacy and data loss risks

Privacy is top of mind for businesses as they seek to protect customer, employee, and third-party data. The impact of privacy violations is significant—they not only affect your brand and reputation, but they also lay you open to multimillion dollar fines for violating data protection regulations.

Digital transformation is increasing privacy risks, creating a growing attack surface as well as more opportunities to mismanage data internally. However, privacy management practices are not keeping pace. Organizations lack visibility across growing data silos and tools. Manual processes and the lack of digitally skilled employees increases risk even further. As a result, businesses are stuck in a reactive mode, trying to stem privacy issues while lacking the tools and processes they need to secure their data.

What is needed is a proactive approach, where data is classified and mapped to new applications, systems, or third parties before they go into production. Through continuous monitoring risks can be identified quickly as these applications, systems, or third parties evolve and access new data sources.

The ServiceNow difference

- ✓ Leverage a unified view of your infrastructure and digital services to classify data, applications, and other elements in your IT environment, creating comprehensive visibility for privacy risks.
- ✓ Proactively screen new applications, projects, vendors, and business processes to determine if they access personal data or other sensitive information.
- ✓ Use automated workflows, real-time indicators, and automated risk assessments to accelerate identification of changes to processes and risk profiles that could have privacy implications, such as accessing new data sources.
- ✓ Continuously collect and monitor information about business applications, identifying emerging privacy risks or compliance failures before they become audit findings.
- ✓ Automatically generate impact assessments, so you save time by only focusing on areas where further privacy screening is required.
- ✓ Accelerate privacy issue responses by using AI to assign issues to the right teams and to identify possible remediations based on similar issues in the past.

Why ServiceNow?

Faster time to value.
Out-of-the-box accelerators, workflow automation, numerous third-party integrations, and automated collection of data from other key ServiceNow applications such as Strategic Portfolio Management, IT Operations Management, IT Asset Management, and Security Operations get you up and running fast.

More confident decision making.
Get an accurate, real-time view of IT risks across your business, providing decision-grade information that allows you to build trust with your customers, employees, and third parties.

Manage all of your IT risks in one place.
Break down silos with comprehensive visibility of your entire IT estate and operational processes to consistently and efficiently manage technical risks, cyber risks, privacy and data loss risks.

Automation.
Respond more quickly and intelligently to rapidly growing and evolving IT risks while increasing productivity and lowering costs.

Real-time information.
Continuously monitor risk instead of relying on periodic audits and attestations. Proactively respond to emerging risks rather than reacting once your business is already impacted.

And, no matter where you are in your journey, we can help you to safely manage IT risk, profitably growing and evolving to reap the benefits of digital transformation.

To find out more about ServiceNow Integrated Risk Management and how it can help you embrace the digital future, visit us at www.servicenow.com/risk

Read our solution briefs to explore our products in more detail: Effectively manage tech and cyber risk and compliance and Identifying and managing privacy risks

Sources

1. Cost of a Data Breach Report 2021 https://www.ibm.com/security/data-breach

About ServiceNow

ServiceNow (NYSE: NOW) is the fastest-growing enterprise cloud software company in the world above $1 billion. Founded in 2004, its goal is to make work easier for people. Our cloud-based platform and solutions deliver digital workflows that create great experiences and unlock productivity for more than 6,200 enterprise customers worldwide, including approximately 80% of the Fortune 500. For more information, visit **www.servicenow.com**.