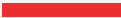


---

ULTIMATE GUIDE

# IT Risk and Compliance Management

A guide for the next era of risk and compliance management, including best practices and strategies for IT and security teams.



# The Ultimate Guide to IT Risk and Compliance Management

## Contents

Introduction .....	3
Chapter 1: Exploring risk management .....	4
Chapter 2: Understanding compliance management .....	9
Chapter 3: Challenges of navigating compliance today .....	13
Chapter 4: Compliance and risk management: Key differences and benefits .....	18
Chapter 5: Best practices for risk and compliance .....	21
Chapter 6: How to choose the right compliance and risk solution: Today and tomorrow .....	24
Chapter 7: How Tanium improves compliance and risk management .....	28
Take a free risk assessment .....	32





# Introduction

Organizations face a complex and multifaceted risk landscape shaped by rapidly evolving technologies, cyber threats, and regulations. Digital transformation, remote work, AI, and cloud migration have significantly expanded the threat surface in recent years. For the majority of organizations, digital innovation is outpacing the ability to mitigate risks and maintain regulatory compliance.

**Just 2% of executives say their company has implemented cyber resilience controls across their organization, with only 15% currently measuring the financial impact of cyber risks.<sup>1</sup>**

Today, organizations also face significant gaps in their risk preparedness, regulatory compliance confidence, and measurement of cyber risk. This comes as AI progresses at a remarkable speed and is reshaping all aspects of organizational and cybersecurity operations.

Organizations that continue relying on traditional risk and compliance frameworks face an array of internal and external threats, from AI-driven social engineering attacks to shadow AI. Simultaneously, emerging frameworks like the E.U.'s AI Act now require organizations to process and use data responsibly and align with new ethical standards. Yet many organizations are deploying AI without a firm understanding of the underlying data powering their systems, putting them at risk of regulatory penalties and compliance risks.

In light of this, organizations must shift their approach to risk and compliance management—two distinct disciplines that have traditionally operated in silos. Risk management focuses on mitigating uncertainty, while compliance management ensures adherence to regulatory and industry standards.

However, the two fields are deeply interconnected, with compliance increasingly depending on fast, accurate risk detection and mitigation. The modern approach involves integrating risk and compliance management while leveraging AI and machine learning (ML) to instantly detect anomalies and proactively mitigate risks.

This guide serves as a roadmap for the next era of risk and compliance management, covering their key differences and benefits as well as best practices and strategies for choosing an effective solution. It also explains how AI transforms risk and compliance through real-time data analysis, pattern detection, and security automation.

By integrating risk and compliance management into a single unified approach, organizations can more effectively tackle emerging cyber threats and regulatory demands with greater confidence and agility.



# Exploring risk management



## What is risk management?

Just as it sounds, risk management involves anticipating and addressing potential uncertainties that threaten the organization's objectives.

While each organization approaches risk management slightly differently, the process generally involves continuously collecting, analyzing, and monitoring activities and infrastructure to stay ahead of potential threats.

## Why risk management is important

Uncertainties are inherent in everyday operations and often can't be fully controlled. However, with proper planning, organizations can reduce their impact and recover quickly.

For example, all organizations today face a growing risk from cyberattacks like ransomware, phishing, and SQL injection, among others. Risk also changes by the second, with threat actors constantly adjusting their tactics and exploiting vulnerabilities. However, with a comprehensive risk management plan in place, driven by automation and real-time visibility, organizations can have an easier time responding to environmental changes and preventing threat actors from achieving their goals.

In short, risk management helps to:

- **Protect resources** like sensitive data and critical assets from unauthorized access
- **Ensure operational stability** and continuity
- **Avoid reputational harm** and customer loss
- **Minimize financial loss** from data breaches and regulatory penalties

# Components of risk management

Risk management comprises six components, including:

1. **Defining risk appetite** or establishing the amount of uncertainty the organization is willing to accept across specific categories like cybersecurity, operations, and compliance

For example, this may include determining how much downtime or disruption the organization can safely handle, how vulnerable it is to cyber threats, and how much risk it will accept with data leaks and information exposure.

2. **Identifying and measuring risks** like software vulnerabilities, configuration errors, cyberattacks, and data center outages

To effectively assess risk, organizations must dive deep into their software, hardware, and partner supply chains and assess risk accordingly. It also helps to assign a cyber score to all components in their supply chain.

3. **Prioritizing risks** by identifying the probability of each one occurring, as well as their severity and how they might impact individual processes

At this stage, the aim is to gain a comprehensive understanding of the organization's threat surface. This step requires focusing on the most critical risks and strategic goals and assigning them scores on a weighted scale of one through ten.

4. **Collecting risk management data** and storing it in a centralized risk register or repository

The risk register should provide a complete overview of all known threats facing the organization. This should be a living document that evolves over time and helps authorized stakeholders with planning and guidance.

5. **Creating a plan for each risk** to reduce uncertainty and improve decision-making

Simply collecting risk management data isn't enough. Organizations must develop specific strategies and actions to prioritize and manage each risk and prevent it from escalating into larger issues.

6. **Monitoring risks and outcomes continuously**, while also considering the effectiveness of each risk management strategy

Continuous monitoring will enable the organization to create a linear graph that indicates how risk and compliance are improving or worsening over time. This can serve as a vital resource to key stakeholders like IT leaders and executives who want to track progress and understand the impact of their organizational risks.

**Did you know?** Several frameworks exist that can help streamline risk management. Some common examples include the Committee of Sponsoring Organizations (COSO) Enterprise Risk Management Framework, the Factor Analysis of Information Risk (FAIR), ISO 31000, and the National Institute of Standards and Technology (NIST) Risk Management Framework.

## Common types of organizational risks

Organizations face a variety of risks across numerous categories. The way these risks are treated often varies depending on the industry and specific priorities for each organization.

Some common types of organizational risks include:



**Cybersecurity risks** threaten sensitive data, networks, and systems. Examples include ransomware, malware, social engineering, insider threats, and brute force attacks.



**Operational risks** affect core functions and stem from various internal or external sources.

For example, 93% of organizations have suffered a cybersecurity breach because of weaknesses in their supply chain or from third-party vendors.<sup>2</sup> Additionally, organizations face growing risks from shadow IT—or unreported systems, devices, and software.

Shadow AI is also increasing, with workers leveraging unauthorized AI tools and platforms to streamline tasks. In fact, nearly 5% of employees have leaked confidential data into public chatbots, enabling that data to be incorporated into public AI models.<sup>3</sup>

**35% of organizations don't regulate how employees use AI chatbots at all.<sup>4</sup>**



**Financial risks** center around monetary loss and instability. Typical examples include fraud and data theft.

**The average cost of a data breach is around \$4.88 million, a 10% increase from last year.<sup>5</sup>**



**Legal risks** center around potential liabilities from violations of laws and regulations, like the Health Insurance Portability and Accountability Act (HIPAA) and the E.U.'s General Data Protection Regulation (GDPR). Violating a data privacy law like GDPR can result in significant fines of up to 4% of annual global turnover.<sup>6</sup>



**Compliance risks** relate to industry standards, internal policies, and local or global regulations. Failing to comply with regulations may result in fines, reputational damage, and operational disruptions.

# Limitations of traditional risk management solutions

Historically, risk management has fallen squarely on individual leaders across departments like finance, operations, compliance, and IT. Risk managers also play a big role in traditional enterprise risk management by safeguarding organizational objectives and operations.

However, the problem with traditional risk management is that it's heavily siloed. And in today's ultra-connected world, organizational leaders and risk managers can no longer afford to work in isolation. Risks that start in one department, like unprotected endpoints or ransomware attacks, can easily spread and impact entire organizations. Additionally, traditional risk management is slow and inefficient due to manual processes and data silos that hinder a comprehensive view of enterprise risk and create delays in addressing risk events.

Today's enterprise risk management (ERM) platforms often promise a streamlined approach to managing uncertainty. However, ERM can be exceedingly expensive and overly complex to implement and support, making it a burden for overstretched and understaffed teams. In addition, a lack of continuous improvement can hinder its effectiveness.

**17% of executives don't see the benefits of ERM exceeding the costs and feel there are too many other pressing needs.<sup>7</sup>**

To better understand the implications of adopting ERM, it's essential to weigh the advantages and disadvantages. The following table outlines the pros and cons of enterprise risk management, providing a clearer picture of its potential benefits and challenges to help highlight why ERM, despite its promises, can often be ineffective in practice.

Pros of ERM	Cons of ERM
<ul style="list-style-type: none"><li>• Integrates risk management</li><li>• Improves risk awareness</li><li>• Enhances decision-making</li></ul>	<ul style="list-style-type: none"><li>• Costly to implement</li><li>• Overly complex/requires training</li><li>• Time-consuming to deploy</li><li>• Requires having a risk-aware culture</li></ul>





## Key takeaways from chapter 1

- Risk management is all about identifying and minimizing uncertainties before they impact operations.
- A comprehensive strategy helps to protect critical assets, minimize downtime, avoid reputational harm, and maintain regulatory compliance.
- There are six major components to risk management, including defining risk appetite, identifying and measuring risks, prioritizing risks, collecting risk management data, creating a plan, and monitoring continuously.
- Organizations face numerous risks across categories like cybersecurity, operations, finance, legal, and compliance.
- Traditional risk management strategies and ERM have numerous shortcomings that make them ineffective.

The digital landscape is becoming increasingly complex and unpredictable. As threats continue to multiply each year, organizations have little choice but to evolve and modernize their risk management strategy. Modern risk management is critical for reducing the impacts of cyberattacks, minimizing other disruptions, and avoiding compliance issues.

In the next chapter, we'll take a closer look at compliance management, including major types of compliance risks to know about and the potential impact of noncompliance.



# Understanding compliance management



## What is compliance management?

The compliance landscape has expanded significantly in recent years. Organizations today must comply with an ever-growing range of local, federal, and global regulations and industry standards designed to protect consumer data and prevent abuse.

As a subset of risk management, compliance management requires creating systematic processes for maintaining integrity and security and ensuring organizations act under shifting laws, regulations, standards, and guidelines. A robust compliance management policy should include policies and controls and involve regular audits to identify and address noncompliance across specific areas.

That said, compliance—and risk management in general— isn't just about identifying and avoiding violations and penalties. A robust policy should never aim to restrict the organization from achieving its goals. Rather, a compliance management strategy should provide a working framework to help organizations operate safely and efficiently in today's fast-moving regulatory environment, with fewer operational disruptions and stronger outcomes. In short, compliance management provides a strong foundation for secure and risk-free growth.

**85% feel that compliance requirements have become more complex in the last three years.<sup>8</sup>**

# IT compliance vs. IT security compliance

IT compliance is often confused with security compliance. However, there are some key differences:

- **IT compliance** refers to laws, regulations, and security guidelines impacting an organization's IT environment. It involves managing systems and user data to comply with regulatory and legal needs, such as GDPR and HIPAA.
- **IT security compliance** focuses on the specific requirements for keeping assets and data safe from threats, such as MITRE ATT&CK and Zero Trust.

The secret to success is building a policy that encompasses IT and security compliance while considering all regulatory requirements that apply to the organization.

## Common types of compliance risks

Compliance is similar to risk management because it's now a shared responsibility between IT and other departments. Now that most processes are highly digital and interconnected, organizations must have a unified compliance strategy that spans all interconnected processes. In other words, processes like data handling and quality control can no longer be left alone to individual teams or individuals. Here are some of the common compliance risks facing organizations today:

### Data handling

Organizations collect vast amounts of data to power AI and machine learning and gain a competitive advantage. This also makes data a significant liability. Organizations must ensure they are properly storing, processing, transmitting, and using data in a way that aligns with a variety of data privacy and security rules. Mishandling data can lead to data exposure and significant penalties from governing bodies.

### Quality

Organizations must ensure that the products and services they release are operationally sound and compliant with customer and regulatory standards. This is particularly important in highly regulated industries like healthcare and finance, which have specific quality and safety standards.

### Processes

Certain organizations must adhere to strict process controls governing how users access systems and information. For example, this may involve setting up strong access controls on software and hardware and encrypting data.

### Fraud and abuse

Illegal activity, such as corruption and fraud, can lead to significant penalties for organizations and individuals. As such, organizations must take active measures to detect, respond to, and report fraud and abuse.

### Environment, health, and safety (EHS)

All organizations must comply with workplace health and safety regulations and act in accordance with local environmental and community guidelines. Compliance requires close collaboration between HR, legal, relevant departments, executives, and local governing agencies.

# Potential impacts of noncompliance

Compliance, like all forms of risk management, is highly resource-intensive. Organizations must allocate time, labor, and capital to align with various frameworks and policies, with little to no ROI for their efforts.

As such, it's common for leaders to simply avoid potential risks to conserve resources and focus on other priorities. Organizations often choose to forego critical services like data loss prevention (DLP), disaster recovery (DR), and business continuity (BC) or Continuity of Operations (COOP), in hopes they will avoid disaster scenarios.

But when it comes to compliance, avoidance can be exceedingly risky and open the door to a variety of negative consequences.

## Financial and legal penalties

Data breaches can lead to costly lawsuits and financial penalties that directly impact the bottom line.

For example, the New York attorney general's office recently filed a lawsuit against a major insurance company, alleging they failed to adequately protect consumer data and report breaches, with the lawsuit seeking penalties of up to \$5,000 per violation.<sup>9</sup>

## Reputational harm

It takes years to build trust with customers and a single violation to break it. Compliance violations can negatively impact public confidence and create long-term damage.

Unfortunately, data breaches and security violations don't simply go away when the problem ends. It can take years to fully regain consumer trust.

## Supply chain disruptions

Security and safety violations can have a ripple effect, impacting both downstream and upstream partners in a supply chain. For example, failing to adopt proper security mechanisms in an app or database can enable threat actors to exploit connected third-party systems. This can lead to a loss of trust, lawsuits, and financial repercussions.

Unfortunately, supply chain attacks are becoming increasingly common, with the global annual cost of software supply chain attacks on pace to reach \$138 billion by 2031—up from \$60 billion in 2025.<sup>10</sup>

**Failing grade:** Of the 43% of enterprises that failed a compliance audit in the last 12 months, 31% experienced a breach that same year, compared to just 3% of those that had passed compliance audits.<sup>11</sup>





## Key takeaways from chapter 2

In this chapter, you learned:

- Compliance management is a process for maintaining integrity and security and acting in accordance with shifting laws, regulations, standards, and guidelines.
- IT compliance and IT security compliance are closely related. IT compliance focuses on regulatory standards, while IT security compliance involves safeguarding assets and data from threats.
- Compliance spans data handling, quality, processes, fraud and abuse, and EHS.
- Noncompliance carries significant financial and reputational risks. It can also lead to costly supply chain disruptions.

The regulatory landscape is constantly changing, which requires organizations to be up to date with the latest policies and guidelines. Falling behind with compliance management puts organizations at risk of financial, legal, and reputational harm.

Next, we'll explore compliance management in specific industries and some common challenges that organizations encounter when navigating compliance.

# Challenges of navigating compliance today

Organizations today must track an ever-growing list of regulations and frameworks. There is often an overlap, with certain regulations applying to multiple industries, adding to the complexity.

Regulations often change, forcing organizations to continuously adapt. For example, organizations need to stay up to date with the latest PCI DSS standards to ensure payment security. Additionally, continuous HIPAA updates are expected to significantly impact both privacy and security measures.

As organizations navigate the complexities of regulatory requirements, it's crucial to understand the specific compliance frameworks that apply to their industry. Each sector has unique standards and guidelines designed to protect sensitive information and ensure operational integrity. Let's explore a mapping of industry-specific compliance frameworks to provide a clearer picture of the requirements and best practices for various fields.

## Industry-specific compliance frameworks

### Public Sector (Federal, State & Local)

#### Key Frameworks

- Federal Information Security Management Act (FISMA)
- Federal Risk and Authorization Management Program (FedRAMP)
- Cybersecurity Maturity Model Certification (CMMC)

#### Compliance Challenges

- Ensuring compliance despite budget and resource constraints
- Relying on outdated and inefficient legacy systems that lack modern security requirements
- Detecting supply chain risks

### Education

#### Key Frameworks

- Family Educational Rights and Privacy Act (FERPA)
- Children's Online Privacy Protection Act (COPPA)
- Title IX
- Protection of Pupil Rights Amendment (PPRA)

#### Compliance Challenges

- Safeguarding against evolving attacks, with threat actors increasingly targeting education institutions
- Gaining visibility into unmanaged and managed assets
- Streamlining threat remediation

---

## Energy, Oil & Gas

### Key Frameworks

- ISO 27001
- NIST SP 800-82
- ISO 14001
- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)

### Compliance Challenges

- Managing complex supply chain risks
- Responding to persistent and evolving threats against critical infrastructure
- Protecting legacy systems
- Maintaining compliance for smart grids, IoT devices, and digital platforms

---

## Healthcare

### Key Frameworks

- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH Act)
- ISO 27799 (Information security management)
- ISO 13485 (Quality management for medical devices)

### Compliance Challenges

- Managing and protecting electronic health records (EHR)
- Ensuring patient consent for data sharing
- Governing and securing endpoints and communications

---

## Manufacturing

### Key Frameworks

- ISO 27001
- ISO 9001 (for QMS)
- NIST Cybersecurity Framework
- IEC 62443 (Industrial Automation and Control Systems Security)

### Compliance Challenges

- Balancing quality assurance and security with productivity
- Adapting to digital transformation (AI, IoT, and smart facilities)
- Managing supply chain risks
- Overcoming resource constraints and staffing shortages

---

## Retail

### Key Frameworks

- Payment Card Industry Data Security Standard (PCI DSS)
- General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA)

### Compliance Challenges

- Protecting customer payment data
- Achieving marketing and sales goals while avoiding compliance breaches
- Ensuring supply chain partners comply with data security standards

---

## Technology

### Key Frameworks

- ISO 27001
- ISO/IEC 27018 (for cloud privacy)
- Service Organization Control 2 (SOC 2)
- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Information Technology Infrastructure Library (ITIL)

### Compliance Challenges

- Ensuring compliance with different industries and regulatory environments
- Safeguarding cloud services and infrastructure
- Safely deploying, managing, and tracking AI



# Noteworthy regional policies

In addition to industry-specific regulations, organizations must stay on top of changing geographic-specific regulations. These policies often apply to organizations that serve citizens in particular countries and regions, regardless of where the organization is based.

Here are some noteworthy geographic-specific regulatory frameworks to know about:



## EUROPE

**European Union:** GDPR, AI Act, Digital Operational Resilience Act (DORA)

**Germany:** Federal Data Protection Act

**France:** French Data Protection Act

**England:** U.K. Data Protection Act 2018



## NORTH AMERICA

**United States:** California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), Colorado Privacy Act (CPA)

**Canada:** Personal Information Protection and Electronic Documents Act (PIPEDA)

**Mexico:** Federal Law on the Protection of Personal Data Held by Private Parties (LFPDPPP)



## SOUTH AMERICA

**Brazil:** Brazilian General Data Protection Law (LGPD)

**Argentina:** Personal Data Protection Act (PDPA)

**Colombia:** Statutory Law 1266 of 2008, Statutory Law 1581 of 2012



## CENTRAL AMERICA

**Costa Rica:** Protection of Personal Data Law (Law 8968)

**Panama:** Data Protection Law

**Honduras:** Law for the Protection of Confidential Personal Data



## AFRICA

**South Africa:** Protection of Personal Information Act (POPIA)

**Egypt:** Personal Data Protection Law (PDPL)

**Kenya:** Kenya Data Protection Act (DPA)



## ASIA

**China:** Personal Information Protection Law (PIPL)

**Japan:** Act on the Protection of Personal Information (APPI)

**Vietnam:** Law on Cybersecurity



## OCEANIA

**Australia:** Privacy Act of 1988, Essential Eight

**New Zealand:** Privacy Act 2020

### A deeper look at Australia's Essential Eight compliance

The Australian Cyber Security Centre (ACSC) put together a framework called the Essential Eight—a baseline set of mitigation strategies that make it harder for threat actors to compromise computer systems.

While Essential Eight compliance isn't mandatory, organizations are strongly encouraged to use it to reduce their attack surface. It's comprised of eight pillars, including:

1. Application control
2. Application patching
3. Configuring Microsoft Office macro settings
4. User application hardening
5. Restricting admin privileges
6. Patching operating systems
7. Multifactor authentication
8. Daily backups

## Does regulatory compliance apply to international waters and airspace?

Both international waters and airspace fall outside the jurisdiction of any single country. As a result, ensuring compliance can be complex.

In general, ships and aircraft are governed by the country where they are registered. For example, a cruise ship registered in the U.S. must comply with U.S. regulations, even when sailing in international waters. Similarly, various global conventions and treaties govern maritime and aviation activities. Some examples include the United Nations Convention on the Law of the Sea (UNCLOS) and the International Civil Aviation Organization (ICAO).

## Evolving beyond conventional GRC

Traditionally, organizations have relied on Governance, Risk, and Compliance (GRC) strategies to ensure regulatory adherence and manage threats. However, as risks and regulations continue to evolve, organizations must also adjust their GRC policies to maintain operational resilience and ensure compliance.

However, many organizations still rely on outdated GRC frameworks that no longer align with today's dynamic risk and regulatory landscape, which can lead to a number of disadvantages:

- Traditional GRC is heavily siloed, with compliance areas existing in isolation.
- Organizations tend to be highly reactive instead of proactive with GRC, typically responding to risks and requirements after they occur.
- GRC is often manual, with organizations using spreadsheets and legacy systems to track compliance and risk management. The process tends to be time-consuming and inefficient.

The modern approach to GRC focuses on aligning internal policies with external regulatory requirements through continuous monitoring, regular auditing, ongoing employee training, and proactive compliance updates. What's more, effective GRC should extend all areas of the organization, involving key internal and external stakeholders and industry partners.



## Key takeaways from chapter 3

In this chapter, you learned:

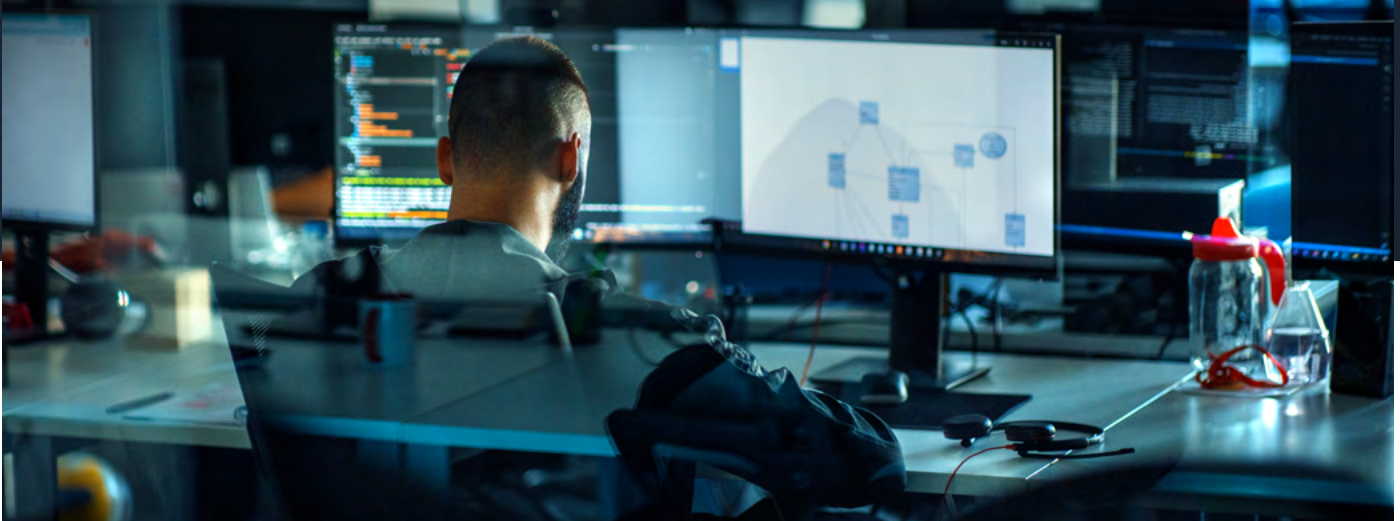
- The compliance landscape is more complex than ever, encompassing all industries and geographical regions.
- Compliance frameworks are constantly evolving as governments and regulatory agencies respond to threats and consumer expectations.
- Traditional GRC strategies are no longer sufficient. Organizations must modernize by adopting continuous monitoring, regulator audits, training, proactive compliance updates, and cross-functional collaboration.

As you can see, modern compliance management is a complex and ongoing process. Keeping up with dynamic frameworks requires significant time and access to industry experts. As a result, organizations often fall behind and become non-compliant with frameworks like GDPR, HIPAA, and others.

Now that we have covered both risk and compliance management, it's time to see what's possible by bringing them together into one unified solution. Read ahead to learn why modern compliance needs a risk-based approach and some examples of risk and compliance management in action.



# Compliance and risk management: Key differences and benefits



## Compliance management vs. risk management

As previously mentioned, compliance management is a subset of risk management. While both disciplines aim to protect organizations from threats, they ultimately serve different purposes and follow distinct procedures.

Let's compare the differences between compliance management and risk management side-by-side to better understand their unique roles:

	Compliance management	Risk management
<b>Objectives</b>	<ul style="list-style-type: none"><li>• Ensure compliance with industry and government regulations</li><li>• Avoid penalties or fines</li></ul>	<ul style="list-style-type: none"><li>• Manage and reduce risks and vulnerabilities across the entire organization</li><li>• Eliminate visibility gaps</li></ul>
<b>Approach</b>	<ul style="list-style-type: none"><li>• Prescriptive in nature</li><li>• Focuses on adhering to internal and external policies and frameworks</li></ul>	<ul style="list-style-type: none"><li>• Predictive in nature</li><li>• Focuses on identifying, assessing, and mitigating potential risks that could impact objectives</li></ul>
<b>Scope</b>	<ul style="list-style-type: none"><li>• Can include both internal and external policies</li></ul>	<ul style="list-style-type: none"><li>• Encompasses a wide range of potential risks from internal and external sources</li></ul>
<b>Outcomes</b>	<ul style="list-style-type: none"><li>• Audit readiness</li><li>• Reduced legal exposure</li><li>• Regulatory approval</li></ul>	<ul style="list-style-type: none"><li>• Reduced operational and reputational risk</li><li>• Improved organizational resilience</li><li>• Informed decision-making</li></ul>

# Why modern compliance management needs a risk-based approach

Up until about a decade ago, organizations could afford to treat risk and compliance management as separate tracks, often with minimal overlap. But today, that separation no longer works. Digital transformation, coupled with complex and evolving risks and mounting regulatory pressure, is forcing organizations to take a unified approach to the two disciplines.

**71% of organizations plan to undertake digital transformation initiatives that will require compliance support over the next three years.<sup>8</sup>**

To remain competitive, organizations need to operate smarter and faster. By consolidating risk and compliance management and leveraging automation, they can accomplish more with less while significantly reducing risks and vulnerabilities.

Integrating risk and compliance management into a single, unified strategy—powered by AI and machine learning—will lead to the following benefits:

- **End-to-end integration** with full visibility into internal and external risks and regulatory requirements
- **Proactive management** combines predictive risk assessment with compliance controls to prevent incidents and ensure accountability
- **Greater efficiency and visibility** between risk and compliance teams and other organizational units
- **Improved audit readiness** with fewer visibility gaps and compliance issues
- **Competitive advantage** through enhanced trust, transparency, and resilience

## Examples of risk and compliance management in action

There are many ways that organizations can use risk and compliance management to enhance operations and reduce exposure, including:

- **Boosting cyber hygiene:** Maintaining cyber hygiene is critical for global organizations, especially during events like mergers and acquisitions. A robust risk and compliance framework can enable rapid detection, analysis, and protection for all endpoints and reduce security gaps.
- **Improving endpoint patching and compliance:** It is essential to keep endpoints updated with the latest security patches. However, manual patching can be slow and error-prone. A modern risk and compliance strategy can help streamline patching and maintain compliance more efficiently.
- **Protecting sensitive data:** You might think that only specific organizations, such as those in healthcare, are vulnerable to cyberattacks targeting sensitive data. However, the reality is that every industry handles information that could be detrimental if exposed. Whether it's financial records, customer details, or proprietary business information, all sectors face the risk of cyber threats and must take proactive measures to protect their data.

To truly secure sensitive data, organizations must move beyond basic patching and need to leverage real-time visibility and automation to keep their systems continuously updated and protected.

- **Streamlining cyber insurance:** Cyber coverage provides a safety net that helps organizations recover by covering the costs associated with data breaches, extortion, and other cyber-related incidents. By investing in cyber coverage, organizations demonstrate their commitment to safeguarding sensitive information and maintaining the trust of their customers and stakeholders.

However, the underwriting process can be time- and resource-intensive. Oftentimes, organizations lack adequate coverage due to poor visibility across their environment. By having comprehensive risk and compliance management, organizations can improve their policy terms and potentially even access discounts on their premiums.

**90% of organizations now have some form of cyber insurance coverage.<sup>12</sup>**

## Key takeaways from chapter 4

In this chapter, you learned:

- Compliance management is a subset of risk management.
- Traditionally, compliance management and risk management serve different purposes.
- Organizations must combine risk and compliance management to take a risk-based approach to compliance.
- Having a modern, unified risk and compliance management strategy can help with many different needs, from boosting cyber hygiene to streamlining cyber insurance coverage.

While risk and compliance management traditionally have different functions and outcomes, together they form the foundation of modern risk and compliance management. Organizations must leverage both as one unified strategy to stay ahead of costly cyberattacks and compliance violations.

Read on to learn some best practices for implementing risk and compliance and how to build a strategy that aligns with your organization's specific needs.



# Best practices for risk and compliance



There's no one-size-fits-all formula for streamlining risk and compliance management. Every organization has a unique digital environment with distinct risks and regulatory requirements. To be effective, risk and compliance strategies must be tailored to each organization's specific needs.

With this in mind, there are several best practices that organizations can adopt to manage risk and stay aligned with evolving regulatory frameworks:

## Consolidate tools

Most organizations today are using disparate tools for risk and compliance management. This leads to visibility gaps and information silos while driving up operating costs.

Ideally, IT, operations, and security teams should work from a single unified platform that offers deep interoperability and end-to-end visibility across the organization. This approach saves time while strengthening coordination and compliance efforts.

## Determine your cyber risk score

A cyber risk score measures an organization's overall exposure to cyber threats and their potential impact. This includes financial, legal, operational, and reputational liabilities.

By calculating a cyber risk score, all stakeholders—from rank-and-file workers to C-level executives—can better visualize the risks they are up against and better understand their security posture. Cyber risk scores are also valuable when assessing merger and acquisition opportunities, shopping for insurance premiums, and evaluating vendors and partners.

There are several methods to calculate risk, one of which is the Monte Carlo strategy. This technique simulates thousands of potential cyberattack scenarios by randomly varying inputs like attack frequency and breach size to estimate a range of outcomes.

## Make reporting actionable

Cyber risk scores and risk reports can be useful for identifying weaknesses and shaping security strategies. However, they tend to be much more effective and valuable when they drive concrete action.

One way organizations can make reporting insights more actionable is to leverage AI and automation to streamline risk management and compliance workflows to prioritize risks, assign ownership, set deadlines, and track progress. This can ensure that reporting doesn't just highlight problems but actively leads to resolutions.

## Continuously measure risk

Organizations today are highly dynamic, with risk profiles that change with new technologies, users, and threats. The only way to stay ahead is to continuously measure and track exposure.

This is particularly important when it comes to closing vulnerabilities. Exploits often become publicly available within a few days and sometimes even a few hours of disclosure. Without continuous monitoring in place, vulnerabilities can go unnoticed—giving threat actors easy access to the network. But with real-time reporting and remediation, organizations can better protect endpoints and reduce threats.

## Prioritize risks with goals and objectives

Not all risks and vulnerabilities will require the same level of urgency. For example, a vulnerability in a critical system that's actively being exploited will require immediate remediation, while a misconfiguration in a non-sensitive server might be scheduled for later correction.

Effective risk prioritization involves assessing both the likelihood of a risk occurring and its potential impact on the organization. By focusing on these factors, organizations can allocate resources to address the most significant threats first.

A key part of this process involves integrating IT and security teams with other crucial departments. Clear communication will ensure risk management efforts support overarching organizational objectives and shifting strategies.

## Maintain cyber hygiene

The number of devices has exploded in recent years, with organizations today using a variety of connected devices both onsite and across remote environments. To accurately track and secure these devices, organizations must have a comprehensive inventory of all IT assets, including laptops, desktops, IoT devices, servers, and more.

In addition to creating an inventory, it's also important to keep it updated and accurate. Inventory changes continually as new technologies and users enter the organization and network.

## Accelerate automation

IT and security teams should be relying heavily on automation to collect endpoint data and remediate risks without human intervention.

By leveraging automation, organizations can reduce manual work and close vulnerabilities at a much faster pace. This results in a more secure and compliant environment and frees teams to focus on more strategic tasks.



## Key takeaways from chapter 5

In this chapter, you learned:

- There is no one-size-fits-all approach to streamlining risk and compliance management. Every organization is unique.
- When building a risk and compliance management strategy, organizations can adopt several best practices like continuously measuring and automating tasks.

Risk and compliance management can be highly resource-intensive, requiring significant time and energy along with deep visibility into IT assets. However, many organizations today lack the means to ensure end-to-end security and compliance. By following best practices, teams can work faster and more efficiently, while improving security and addressing compliance gaps.

Next, we'll provide an overview of how to choose the right compliance and risk solution, including key features to look for in a platform. The next section will also explore the future of compliance and risk management.



# How to choose the right compliance and risk solution: Today and tomorrow



Making the decision to move forward with a modern risk and compliance strategy is the first step toward building a secure, compliant, and resilient organization. The next—and often more challenging—part is choosing the right platform to support your ability to achieve these goals by empowering your organization to manage risks more effectively, ensure compliance with ease, and realize the benefits of your investment sooner.

## Features to look for in an effective compliance and risk management solution

When choosing a compliance and risk management solution, look for the following features to ensure it quickly delivers real value to the organization:

- **Usability:** Many tools offer sleek, user-friendly interfaces, but lack the depth and support that organizations need to detect and remediate threats. On the flip side, some platforms provide robust capabilities but are challenging to use and come with a steep learning curve. Organizations need a platform that's intuitive enough for broad adoption yet powerful enough to be trusted.
- **Integration:** To be effective, the platform must integrate seamlessly with your existing tech stack. Platforms that don't integrate easily can lead to excessive manual oversight, as well as visibility gaps and data silos.



- **Compliance:** It's critical to ensure the platform aligns with the specific regulatory requirements the organization must adhere to, such as GDPR or HIPAA. Most tools won't cover all frameworks out of the box, so it's important to evaluate how well the platform maps to the organization's compliance needs.

- **Continuous data monitoring:** The platform should provide continuous monitoring along with deep visibility into all the locations where sensitive data lives, such as logs or Windows registry paths.

Deep reporting with software bill of materials (SBOM) insights: It's necessary to have a platform that can report on all aspects of cybersecurity and technology compliance, including SBOMs, digital certificates, and container security.

- **CISA KEV integration:** The Cybersecurity Infrastructure Security Agency (CISA) maintains a database called the Known Exploited Vulnerabilities (KEV). An effective compliance and risk management solution should integrate seamlessly with CISA KEV to quickly detect vulnerabilities.
- **Risk prioritization and remediation:** While identifying vulnerabilities is important, remediating them presents an entirely different set of obstacles, especially for understaffed IT teams in distributed environments. A platform that can automatically prioritize and resolve vulnerabilities can help security, IT, and operations teams, including SecOps and ITOps, save time and reduce manual work.
- **Quick endpoint scans:** Organizations now manage an average of 135,000 device endpoints.<sup>13</sup> As the number of endpoints continues to grow and the attack surface expands, organizations must leverage a solution that can quickly detect and manage them in real time.
- **Enhance Role-based Access Control (RBAC):** RBAC allows administrators to define granular permissions and control which endpoints users can access and manage. By choosing a risk and compliance solution that seamlessly incorporates RBAC, roles can be more easily assigned to individual users, groups, or predefined personas, improving security and oversight.

## The future of risk and compliance management with AI

AI is transforming almost every aspect of operations—including risk and compliance management. Up until recently, risk and compliance professionals could afford to conduct lengthy and thorough assessments. However, with threats rapidly evolving in sophistication and becoming AI-driven, manual assessments are quickly being rendered obsolete and inefficient.

To keep pace with the threat landscape, organizations must modernize and accelerate their risk and compliance processes, leveraging real-time threat intelligence and AI to proactively identify and address vulnerabilities.

The future of AI-driven risk and compliance management will center heavily around:

### Automated risk assessments

AI can rapidly analyze large datasets to identify potential threats. Automated risk assessments reduce reliance on manual processes and improve overall decision-making.

### Real-time monitoring and alerts

AI enables teams to instantly detect anomalies and breaches. By leveraging AI, organizations can automate the quick remediation of issues and improve their security posture.

### Predictive analytics

Today's machine learning algorithms can accurately detect patterns in vast amounts of data. By harnessing these predictive capabilities, organizations can proactively address risks before they escalate into serious problems.

### Continuous compliance tracking

AI insights can help ensure ongoing alignment with today's dynamic and complex regulations, minimizing the risk of costly violations while improving audit readiness.

### Improved documentation and reporting

AI-powered analytics delivers accurate, real-time insights that simplify compliance reporting and help organizations clearly demonstrate adherence during audits.

## Success story: Honeywell exceeds 90% patch compliance

One company that once struggled with documentation and reporting is Honeywell, a leading global industrial supplier with roughly 15,000 server endpoints spread across more than 80 countries.

The company was generating poor patching compliance benchmarks due to a lack of visibility into their endpoints—leaving them highly vulnerable to attacks. On top of this, it had accumulated an abundance of disparate security tools, many of which were unable to share critical data and resulted in limited reporting.

At the recommendation of a team member, Honeywell decided to try Tanium for its proven ability to integrate IT, compliance, security, and risk reporting into a single, user-friendly platform. The decision quickly paid off. With the help of Tanium, **Honeywell was able to establish a single pane of glass for patch compliance and reporting.** The company drastically improved endpoint security, reduced unnecessary tools, and surpassed 90% patch compliance for three months in a row—a feat that was previously unattainable.

**“Prior to using Tanium, our patch compliance was low. Now, with Tanium, we've crossed the 90% patch-compliance mark for three months in a row. That's significant.”**

**Manish Chopra**

IT director, Honeywell



## Key takeaways from chapter 6

In this chapter, you learned:

- Not all risk and compliance management solutions deliver the same level of usability, support, and protection. It's important to be selective when picking a platform.
- When exploring different services, make sure to find a platform that offers advanced features like continuous data monitoring, deep reporting capabilities, and CISA KEV integration.
- The future of risk and compliance management is AI-driven, and heavily centered around automation and real-time intelligence.

Choosing the right compliance and risk solution is essential for safeguarding against emerging threats and meeting evolving regulatory requirements. Before selecting a platform, it's necessary to evaluate all aspects, including the insights it provides and its ability to remediate threats and compliance violations across a broad range of categories.

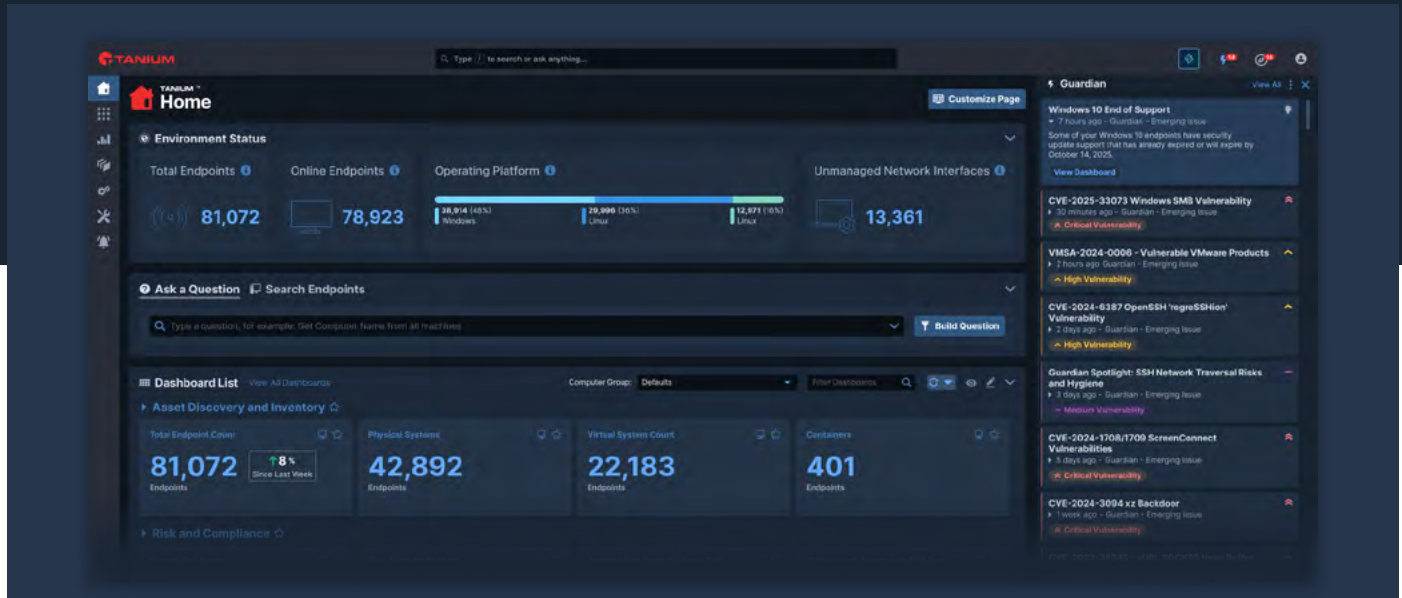
Equally important is the provider's ability to evolve and adapt to changing conditions. A forward-looking platform should not only meet today's needs but also help future-proof the organization against tomorrow's risks.

In the final chapter ahead, we'll explore how Tanium is ushering in the next era of compliance and risk management.

ties.



# How Tanium improves compliance and risk management



## Why Tanium?

The risk and compliance solutions market continues to lag behind evolving organizational and security demands. Most of the available tools are siloed point solutions, with fragmented data sets and limited automation—making them unsuitable for detecting and responding to emerging, AI-driven threats. They also tend to be highly resource-intensive, as they are both complex and expensive.

As such, organizations across the board are struggling with:

- **Rampant risks** stemming from exposed vulnerabilities lead to breaches and data loss
- **Poor visibility**, with leaders often unaware of which risks they face—or which issues to address first
- **Noncompliance** with new and existing regulatory demands, resulting in fines, penalties, and reputational damage

Tanium Risk & Compliance was purpose-built to address these challenges through a single, intuitive platform. It delivers complete, real-time visibility into endpoint risks and compliance gaps, along with contextual insights that drive smarter and faster remediation.

Organizations across all industries now use Tanium Risk & Compliance to:

- **Monitor:** Continuously scan for vulnerability and compliance gaps across every managed and unmanaged endpoint, providing real-time visibility into the IT environment



- **Prioritize:** Take a proactive, collaborative, and risk-based approach to deciding which vulnerability and compliance gaps to close first, leveraging real-time risk scores and endpoint criticality assessments
- **Automate:** Streamline compliance processes and reduce manual tasks through automation, ensuring continuous compliance and audit readiness
- **Act:** Deploy a wide range of controls to close vulnerability and compliance gaps, including automated remediation actions and validation of their impact on risk scores in real time
- **Report:** Generate detailed compliance reports and audit trails automatically, simplifying the process of demonstrating adherence to regulatory standards

## Tanium's AI policies

The use of artificial intelligence has emerged as an area of great concern among risk and compliance professionals. That's why Tanium maintains organizational AI policies and processes to ensure AI technologies are used in a safe, ethical, and legally compliant manner. Tanium incorporates and follows AI industry standards, regulations and guidelines in its policies and processes, including the NIST AI Risk Management Framework (AI RMF), the OWASP Top 10 for Large Language Model Applications, and the European Union (EU) Artificial Intelligence (AI) Act. Tanium regularly reviews its policies and processes to align with its continued proactive monitoring of emerging AI regulations, best practices and industry standards. You can read more about Tanium's AI policies and principles at the Tanium Resource Center.

## Success story: VF Corporation automates critical system updates

VF Corporation, also known as VFC, needed to evolve and automate its end-to-end patching and security orchestration strategy to boost productivity and protect its network.

VFC is now using Tanium Automate, which simplifies IT and security task orchestration using real-time endpoint visibility and data, while also using other Tanium modules like Patch, Deploy, and Discover. As a result, **VFC enjoys tighter security with real-time visibility and a faster, more efficient patching process.** Tanium Automate also frees VFC's patching lead to focus on deep work instead of repetitive, labor-intensive security tasks.

"My overall experience using Automate has been outstanding so far, the tool is delivering exactly what we expected," said David Anderson, VFC's patch automation and vulnerability remediation lead. "We are now able to quickly patch using runbooks and focus on other priorities, knowing that these critical updates are taking place in the background. Plus, runbooks only take about five minutes or so to create. The entire process gives us back countless hours in our schedule."

**"I highly recommend using Tanium Automate, especially for busy security teams that are trying to save time on manual, repetitive tasks like patching."**

**David Anderson**

Patch automation and vulnerability remediation lead, VF Corporation

## Tanium's partnerships and joint solutions

Tanium has established strong partnerships and joint solutions with key technology alliances, which enable organizations to leverage integrated solutions that enhance their IT operations, reduce operational risk, and manage compliance, including:

### **Cyber insurance providers**

Tanium partners with leading cyber insurers such as Chubb and Beazley to help organizations streamline the underwriting process.

Organizations can leverage Tanium's free risk assessment service to gain a clearer understanding of their security posture, expedite underwriting, and secure more favorable policy terms.

### **Microsoft Sentinel**

Microsoft Sentinel is a leading cloud-native Security Information and Event Management (SIEM) service that provides intelligent security analytics and threat detection.

Tanium's integration with Microsoft Sentinel enables organizations to reduce the complexity of their environments and achieve higher levels of incident response efficacy.

### **ServiceNow Integrated Risk Management (IRM)**

ServiceNow is a cloud-based platform that offers digital workflow solutions for managing and automating organizational processes in security, IT, customer service, and other areas.

Organizations can accelerate incident response and enhance operational resilience by combining Tanium's real-time endpoint visibility and control with ServiceNow's workflow automation capabilities.

Discover the power of seamless integration with the Tanium Integrations Gallery, which enables you to effortlessly connect Tanium's platform with key technology partners like Microsoft and ServiceNow. With a simple, centralized interface, you can discover, deploy, and manage joint solutions and integrations without requiring deep technical expertise.

## Tanium AEM: Bringing next-gen AI capabilities to risk and compliance management

Today's IT and security teams face mounting challenges in tracking and managing dynamic endpoints at scale. With a growing mix of operating systems, user profiles, and security compliance demands, traditional endpoint management is no longer enough.

This complexity is driving demand for autonomous endpoint management (AEM)—an emerging discipline that combines unified endpoint management and digital employee experience with AI and ML to accelerate risk identification and remediation.

“Largely driven by increased AI and machine learning (ML) capabilities, technology vendors have accelerated development and release cadence, and IT cannot keep pace... the accelerated pace of software updates and increased level of vulnerabilities continue to overwhelm IT, undermine technology stability, increase cybersecurity risk and degrade digital employee experience.”<sup>14</sup>

Gartner

Tanium AEM, built on Tanium's award-winning platform, is at the forefront of this development. Tanium AEM leverages real-time data and insights to automate routine tasks and drive smarter, faster decisions. IT and security teams can use Tanium AEM to minimize manual effort, reduce risk exposure, and close compliance gaps at scale.

Solutions like Tanium Risk & Compliance are an integral part of Tanium AEM, which provides the tools and capabilities organizations need to holistically manage risks and ensure compliance effectively across their entire IT infrastructure. Integrating solutions within Tanium AEM enhances their functionality, allowing organizations to benefit from real-time visibility, automated processes, and comprehensive endpoint data by using one centralized platform, making it easier to maintain overall security and compliance.

With Tanium AEM, organizations can:

- **Prevent** disruptions when deploying endpoint changes
- **Scale** IT and security operations with greater precision
- **Accelerate** remediation times
- **Identify** and eliminate zero-day risks before exploitation
- **Gain** instant answers about any global endpoint

## Key takeaways from chapter 7

In this chapter, you learned:

- Tanium Risk & Compliance was specially designed to help organizations discover, prioritize, and remediate critical threats.
- Tanium offers deep interoperability with popular services and applications like Microsoft Sentinel and ServiceNow.
- Organizations can use Tanium to expedite and improve the insurance underwriting process.
- Tanium AEM delivers next-generation risk and compliance management by combining real-time endpoint visibility, autonomous operations, and AI-driven insights into a single platform.

The days of manual, reactive risk and compliance management are coming to an end. Increasing regulatory demands, rising cybersecurity threats, and growing operational complexity are forcing organizations to rethink their strategies and invest in modern, AI-driven solutions.

Success now demands real-time visibility, along with intelligent, autonomous decision-making. Organizations must also break down silos and treat risk and compliance as a unified discipline.

Tanium delivers the real-time visibility and control needed to transform risk and compliance management from a liability into a strength. As the only provider of converged endpoint management, Tanium is leading the shift from legacy practices to next-generation risk governance.



NEXT

## Take a free risk assessment

Improving your risk and compliance posture starts with first understanding how each endpoint compares across key vectors, including vulnerabilities, patch status, sensitive data exposure, and more.

Tanium offers free risk assessments to help organizations gain a clearer view of their environments and build actionable improvement plans.

**GET YOUR ANALYSIS TODAY** →

### PRODUCTS FEATURED

- [Tanium Risk & Compliance](#)
- [Tanium AEM](#)
- [Tanium + Microsoft](#)
- [Tanium + ServiceNow](#)
- [Tanium Integrations Gallery](#)

### ENDNOTES

- 1 <https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html>
- 2 <https://www.bluevoyant.com/resources/managing-cyber-risk-across-the-extended-vendor-ecosystem>
- 3 <https://www.cyberhaven.com/blog/4-2-of-workers-have-pasted-company-data-into-chatgpt>
- 4 <https://tech.co/news/cybersecurity-statistics>
- 5 <https://www.ibm.com/think/insights/whats-new-2024-cost-of-a-data-breach-report>
- 6 <https://gdpr-info.eu/issues/fines-penalties/>
- 7 <https://poole.ncsu.edu/thought-leadership/article/new-report-enterprise-risk-management-processes-remain-undervalued-by-global-boards-and-executives-amid-heightening-risk-environment/>
- 8 <https://www.pwc.com/gx/en/issues/risk-regulation/global-compliance-survey.html>
- 9 <https://www.infosecurity-magazine.com/news/new-york-sues-allstate-data-breach/>
- 10 <https://cybersecurityventures.com/software-supply-chain-attacks-to-cost-the-world-60-billion-by-2025/>
- 11 [https://www.thalesgroup.com/en/worldwide/defence-and-security/press\\_release/2024-thales-data-threat-report-reveals-rise-ransomware](https://www.thalesgroup.com/en/worldwide/defence-and-security/press_release/2024-thales-data-threat-report-reveals-rise-ransomware)
- 12 <https://news.sophos.com/en-us/2024/06/26/cyber-insurance-and-cyber-defenses-2024-lessons-from-it-and-cybersecurity-leaders/>
- 13 <https://adaptiva.com/resources/report/managing-risks-and-costs-at-the-edge>
- 14 <https://www.tanium.com/press-releases/tanium-named-among-vendors-for-autonomous-endpoint-management-in-2024-gartner-hype-cycle-for-it-management-intelligence/>



The Power of Certainty.™

Visit us at [www.tanium.com](https://www.tanium.com) and follow us on [LinkedIn](#) and [X](#).

© Tanium 2025