WHITE PAPER

Integrated risk and compliance use case guide

servicenow

Table of Contents

An integrated risk program

Imagine managing risk—be it digital, IT, compliance, or third-party—across every department and function without slowing down processes or overburdening your team. Picture a scenario where previously siloed processes become part of an integrated risk program that extends across the enterprise. With ServiceNow, you can make this vision a reality.

Everyone knows the risks of regulatory noncompliance and ignoring vulnerabilities. But the threats continue, and they're constantly evolving. Inefficient processes, human error, new initiatives like digital transformation, and unforeseen delays all increase risk. The reality is that, despite best intentions, critical items keep falling through the cracks—and most companies can't even identify what fell through, let alone the potential impact if left unaddressed.

At the same time, complexity keeps growing with each new regulation, process, application, and piece of hardware. It's no surprise that legacy governance, risk, and compliance (GRC) products can't keep up with this growing list of challenges.

To manage risk and compliance in this ever-changing landscape, you need a modern, cloud-based platform that can continuously monitor activities, improve decision-making, and increase performance through automation and AI-powered user experiences. You can work the way you want, with the ability to easily collaborate with other departments and effectively communicate with business users, the CEO, and the board. And user-friendly portals with mobile interfaces make it easy to work anytime and anywhere.

45%

of security and IT execs expect a further rise in ransomware attacks.

- PwC 2023 Global Digital Trust Insights

19%

of breaches occurred because of a compromise at a business partner.

- IBM/Ponemon 2022

9%

of annual revenue, what exploitable network misconfigurations cost organizations.

- Titania 2022

Designed for cloud scale, the Now Platform® lets you share data and automate cross-functional workflows by consolidating enterprise and third-party data using open APIs. ServiceNow Integrated Risk Management (IRM) builds on these platform capabilities, seamlessly embedding risk and compliance activities into everyday business processes so you can automatically collect evidence, quickly assign tasks, and streamline audits. Identify business risks fast through continuous monitoring and risk events, and then easily roll these risks up to an enterprise-wide view. And reduce compliance complexity and turbocharge efficiency with a common control framework that lets you "test once and comply many."

With risk and compliance embedded in cross-functional workflows, you can easily manage risk across the enterprise. For instance, an HR compliance violation can trigger a legal issue. Or when a vendor's security performance degrades, that risk can trigger restrictions on their access to your network. You handle risk with confidence and take the right action—and take it sooner—so your business stays protected.

Let's take a closer look at some common risk and compliance management challenges:

1. Monitoring for critical vulnerabilities and understanding the business impact
2. Identifying and addressing misconfigurations before they become business risks
3. Embedding risk and compliance management into the application release and change process
4. Monitoring HR policy requirements and identifying onboarding risks
5. Ensuring privacy standards are met
6. Proactively addressing third-party issues, including ESG

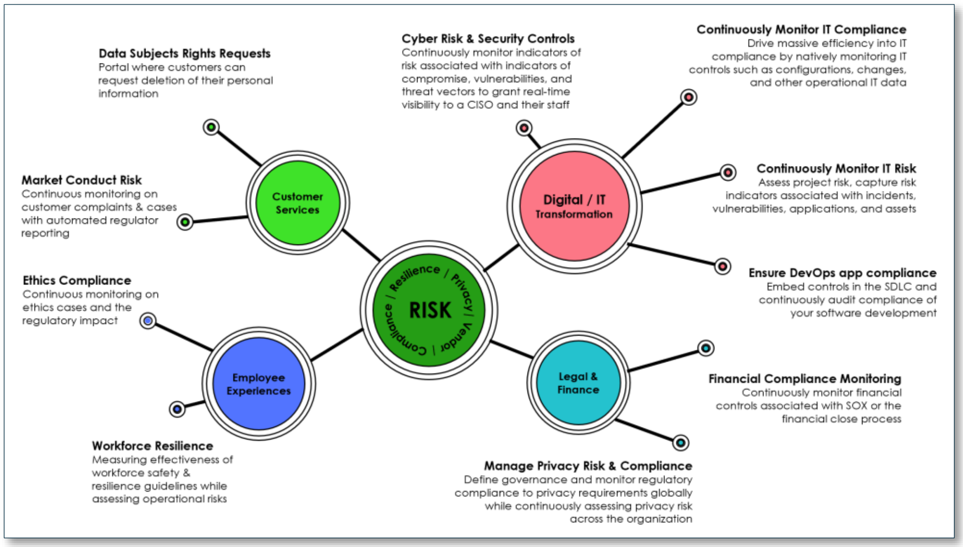

Data Subjects Rights Requests
Portal where customers can request deletion of their personal information
Cyber Risk & Security Controls
Continuously monitor indicators of risk associated with indicators of compromise, vulnerabilities, and threat vectors to grant real-time visibility to a CISO and their staff
Continuously Monitor IT Compliance
Drive massive efficiency into IT compliance by natively monitoring IT controls such as configurations, changes, and other operational IT data
Market Conduct Risk
Continuous monitoring on customer complaints & cases with automated regulator reporting
Customer Services
Digital / IT Transformation
Continuously Monitor IT Risk
Assess project risk, capture risk indicators associated with incidents, vulnerabilities, applications, and assets
Ethics Compliance
Continuous monitoring on ethics cases and the regulatory impact
Resilience / Privacy / Vendor / Compliance /
RISK
Ensure DevOps app compliance
Embed controls in the SDLC and continuously audit compliance of your software development
Employee Experiences
Legal & Finance
Financial Compliance Monitoring
Continuously monitor financial controls associated with SOX or the financial close process
Workforce Resilience
Measuring effectiveness of workforce safety & resilience guidelines while assessing operational risks
Manage Privacy Risk & Compliance
Define governance and monitor regulatory compliance to privacy requirements globally while continuously assessing privacy risk across the organization

Figure 1: Risk and compliance is used to address needs across the enterprise.

90%

of organizations believe digital transformation is driving new risks.

- Gartner 2020

45%

of breaches occurred in the cloud.

- IBM/Ponemon 2022

2.29 billion

records were exposed worldwide in 2022.

– Tenable 2022 Threat Landscape Report

Use case: Monitor for critical vulnerabilities and understand the business impact

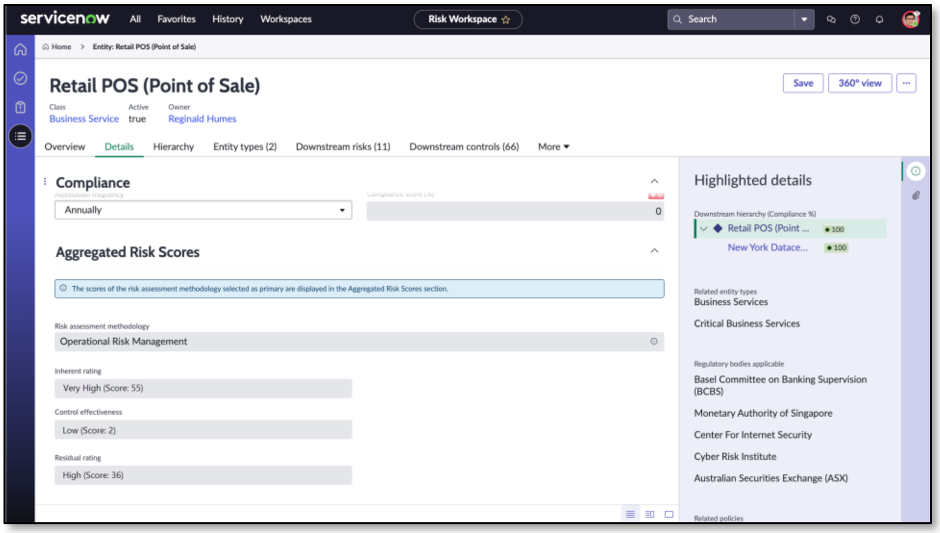
With legacy solutions, it's an ongoing challenge to manage security vulnerabilities and risk across multiple departments and functions. Someone on the security team may be able to spot a vulnerability due to a missing application patch—but it takes an integrated risk platform to tell you that the vulnerability affects your point-of-sale (POS) system and has the potential to cost millions in lost revenue. An integrated risk management program can help you gauge the associated risk, understand how it compares to all other risks, and track it through to resolution. You can also easily communicate the risk status and potential business impact to upper management.

Imagine a security manager tracking 50 identified vulnerabilities. They might not notice that one patch isn't installed correctly. Maybe a machine is offline when the patch is pushed out, or perhaps the patch depends on other updates to fully address the vulnerability. Whatever the reason, vulnerabilities like these linger unless you have an integrated risk program to identify and enforce the needed security.

Working through ServiceNow Vulnerability Response, ServiceNow IRM collects data from a variety of vulnerability scanners. It identifies outstanding vulnerabilities and prioritizes each one based on severity, the availability of exploits, relative risk (based on a customizable score), and the potential impact on services (based on asset and business insights). Issues are automatically routed to the correct vulnerability manager for immediate resolution, who can choose a prescribed remediation path for a given vulnerability using Vulnerability Solutions Management. Dashboards provide real-time updates to the risk manager and business stakeholders. And decision-makers can easily quantify and manage the overall risk posture of the enterprise.

A risk manager at work

As a risk manager, I'm responsible for monitoring threats on a minute-by-minute basis. I can see on my ServiceNow Risk dashboard that a new critical risk has appeared. Drilling into the alert reveals that the POS system has an unpatched vulnerability and reveals insights into its exploitability. The issue can affect overall system availability and make us vulnerable to fraud or data theft. Without ServiceNow, I would waste time figuring out who should address the issue.



Retail POS (Point of Sale)

Class: Business Service
Active: true
Owner: Reginald Humes

Compliance

Attestation frequency: Annually
Compliance score (%): 0

Aggregated Risk Scores

The scores of the risk assessment methodology selected as primary are displayed in the Aggregated Risk Scores section.

Risk assessment methodology: Operational Risk Management
Inherent rating: Very High (Score: 55)
Control effectiveness: Low (Score: 2)
Residual rating: High (Score: 36)

Highlighted details

Downstream hierarchy (Compliance %)

Retail POS (Point ...	● 100
New York Datace...	● 100

Related entity types
Business Services
Critical Business Services

Regulatory bodies applicable
Basel Committee on Banking Supervision (BCBS)
Monetary Authority of Singapore
Center For Internet Security
Cyber Risk Institute
Australian Securities Exchange (ASX)

Related policies

Figure 2: Risk is calculated based on the business impact.

Instead, I can immediately see the correct people responsible for taking action on the security and IT teams. The ServiceNow IRM risk management application also automatically calculates the risk score, taking into consideration the threat and the potential loss if we leave it unaddressed.

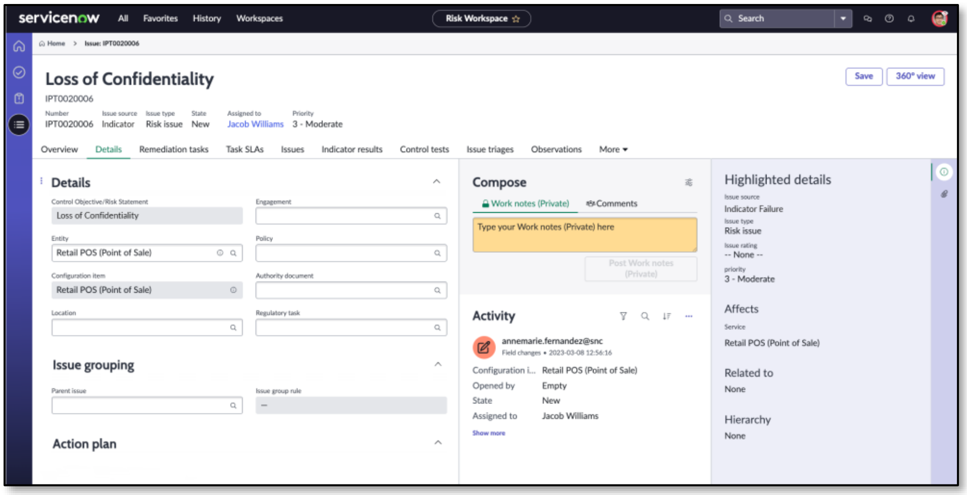
For this particular threat, the risk score is high, and the calculated average loss expectancy (ALE) is almost $14M. If the calculations were within our predefined risk threshold of $8M, I could accept it. In this case, the level of risk is unacceptable, and I need to act.

I can see this vulnerability has been active for two weeks. By clicking on the indicator's related list, I can also identify which device has the unpatched vulnerability. A combination of continuous risk monitoring capabilities for essential business services and out-of-the-box risk indicators from ServiceNow helped us spot the risk.

Looking at my controls list, I can see that "Manage change requests," "Manage changes," and "Establish and maintain a patch management program" are missing. I can immediately add these controls from this form.

When the system first identified this risk, it automatically created an issue and sent it to the appropriate team.

I can drill down into the created issue using the issues list. I know some organizations might engage the vulnerability manager at this point, but because this was a Windows machine, we have a special Windows patch team I want to alert. From within the issue, I can track progress and, if necessary, work with other parts of the organization to resolve the issue quickly without endless email exchanges.



Loss of Confidentiality

IPT0020006

Number	Issue source	Issue type	State	Assigned to	Priority
IPT0020006	Indicator	Risk issue	New	Jacob Williams	3 - Moderate

Details

Control Objective/Risk Statement: Loss of Confidentiality

Engagement:

Entity: Retail POS (Point of Sale)

Policy:

Configuration item: Retail POS (Point of Sale)

Authority document:

Location:

Regulatory task:

Issue grouping

Parent issue:

Issue group rule: --

Action plan

Compose

Activity

annemarie.fernandez@snc
Field changes • 2023-03-08 12:56:16

Configuration i...	Retail POS (Point of Sale)
Opened by	Empty
State	New
Assigned to	Jacob Williams

Highlighted details

Issue source: Indicator Failure

Issue type: Risk issue

Issue rating: -- None --

priority: 3 - Moderate

Affects

Service: Retail POS (Point of Sale)

Related to: None

Hierarchy: None

Figure 3: The issue is automatically created with the appropriate priority and assigned to the owner of the affected asset.

When the Windows patch team has completed the patch, the security team can rescan our systems. If the vulnerability is resolved, the critical risk will disappear from my Risk Dashboard, and the issue will close automatically. The system tracks all status updates within the issue—providing an audit trail for future reference.

With an integrated platform, all teams (security, risk, and IT) have access to the same underlying information, presented on dashboards designed specifically for each team. We can use this information to prioritize security vulnerabilities in relation to all other business risks for holistic risk management.

Tech Tip:

Check out the new risk indicator templates within ServiceNow IRM. Go to Risk Management > Risk Statement > Risk Framework.

Use case: Identify and address misconfigurations before they become business risks

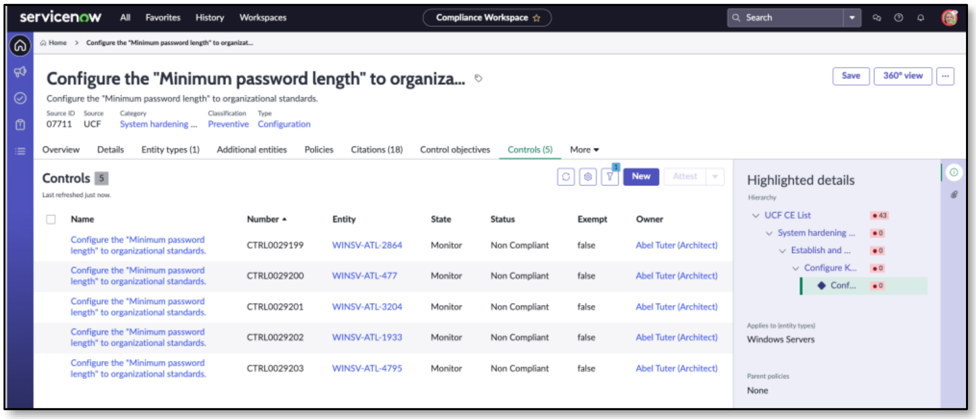
It's not unusual for IT teams to maintain thousands of different software packages, systems, and devices. While most teams have processes in place to verify configurations, mistakes still happen. A newly installed router might have a password entered in clear text, which leaves it visible. Maybe an access control for a new firewall isn't set up properly, leaving an opening for intruders. Perhaps security isn't configured correctly for an S3 storage bucket in the AWS cloud, leaving sensitive data publicly exposed. Or the user of a device might have admin privileges that allow them to install unauthorized software or change important security settings, leaving an opening for an attacker to gain unrestricted network access.

Standards and external regulatory compliance obligations (for example, SOX, PCI, and ISO) often include elements that attempt to address the business risk of misconfigured software, older protocols, and weak passwords. Enterprises translate these requirements into configuration hardening policies. Too often, however, organizations only identify misconfigurations after an attack. A better approach is to identify misconfigurations before they put your business at risk.

Working through ServiceNow Security Operations Configuration Compliance, you can monitor data from security configuration assessment tools. But you now want to extend ServiceNow IRM continuous monitoring to your configuration hardening policies so that you can identify a failed configuration test result, assess the potential business impact, automatically create an issue, and proactively engage the responsible party to address the weakness before it is exploited.

A compliance manager at work

Several failed controls have popped up on my Policy and Compliance dashboard. Drilling into them, I see that the latest scan by our security configuration assessment tool has spotted misconfigured software. The data shows multiple Windows servers that don't have the appropriate setting for maximum software password age, meaning there may never be a prompt to change the password—which creates an opportunity for a clever attacker. This could be the result of a software update or new installation.



Configure the "Minimum password length" to organiza...

Configure the "Minimum password length" to organizational standards.

Source ID	Source	Category	Classification	Type
07711	UCF	System hardening ...	Preventive	Configuration

Controls 5

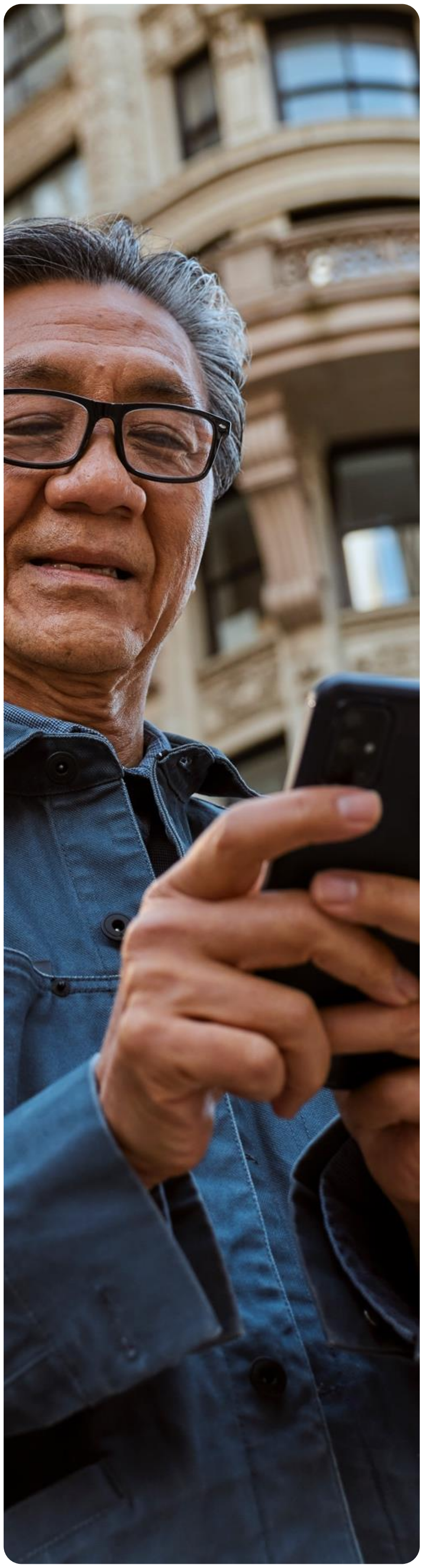
Last refreshed just now.

Name	Number	Entity	State	Status	Exempt	Owner
Configure the "Minimum password length" to organizational standards.	CTRL0029199	WINSV-ATL-2864	Monitor	Non Compliant	false	Abel Tuter (Architect)
Configure the "Minimum password length" to organizational standards.	CTRL0029200	WINSV-ATL-477	Monitor	Non Compliant	false	Abel Tuter (Architect)
Configure the "Minimum password length" to organizational standards.	CTRL0029201	WINSV-ATL-3204	Monitor	Non Compliant	false	Abel Tuter (Architect)
Configure the "Minimum password length" to organizational standards.	CTRL0029202	WINSV-ATL-1933	Monitor	Non Compliant	false	Abel Tuter (Architect)
Configure the "Minimum password length" to organizational standards.	CTRL0029203	WINSV-ATL-4795	Monitor	Non Compliant	false	Abel Tuter (Architect)

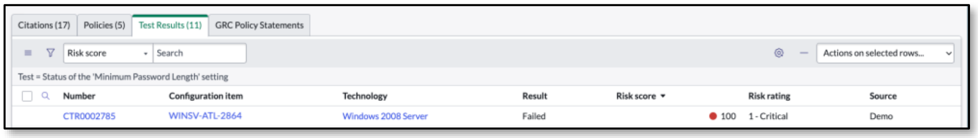
Applies to (entity types)
Windows Servers

Parent policies
None

Figure 4: Continuous monitoring of controls shows the entities affected and identifies any policy exceptions.



ServiceNow Security Operations collects scan data and makes it available to IRM Continuous Monitoring. The IRM Configuration Compliance application then matches failed configuration test results to assets in the ServiceNow Configuration Management Database (CMDB). The CMDB shows the business importance of each asset, providing a criticality assessment that is combined with other factors to automatically calculate a risk score used to prioritize failed results.



Test = Status of the 'Minimum Password Length' setting

Number	Configuration item	Technology	Result	Risk score ▾	Risk rating	Source
CTR0002785	WINSV-ATL-2864	Windows 2008 Server	Failed	● 100	1 - Critical	Demo

Figure 5: The Configuration Tests tab shows the source used to collect configuration data.

Just like my Policy and Compliance dashboard displayed the failed controls, my IRM Risk dashboard displays the risks associated with these misconfigurations alongside other identified enterprise risks. And the IT manager can see the criticality level of the failed test results on the Configuration Compliance dashboard.

Although I could have had each noncompliant control automatically generate an issue and send it to the IT manager, I would rather review configuration test failures before routing issues to the appropriate person. Because the same control is failing across multiple assets, I've elected to group the issues under a single parent issue with a single remediation task before assigning the group to the IT manager.

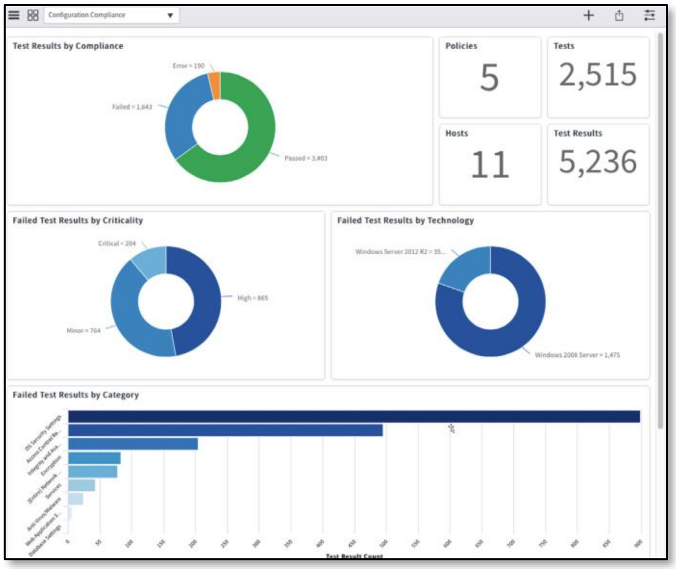


Figure 6: The Configuration Compliance dashboard is dynamically updated based on new test results.

If this type of issue becomes a common occurrence, I may create a rule to automatically group similar issues under a predefined parent issue to automate the process. I can then track the parent issue to completion.

IT will update the issue, so I will know whether the configuration change will happen during the next update cycle, when the security team or IT will review and approve the change. Each team has visibility into the current status of the change, the next steps, and who is responsible.

When a subsequent scan shows the configuration issue has been remediated (in other words, there is no longer a configuration test failure), the control will again be compliant. When the IT manager closes the parent issue, providing proof that the remediation process was successful, all child issues will also close.

Tech Tip:

When you identify several similar issues, use grouping to make tracking easier.

Embed risk and compliance management into the application release and change process

Your organization has hundreds—even thousands—of applications. Managing risk, compliance, and audit for each application is a massive undertaking if risk isn't embedded into the application lifecycle. Applications need to be continuously monitored to identify vulnerabilities quickly. Those that access, store, or process personally identifiable information have to be closely tracked to ensure regulatory compliance and avoid massive penalties. DevOps policies must be followed for in-house applications and audited for compliance. The list goes on.

To successfully manage risk and application sprawl, aligning on a common risk library embedded into your application release and change processes is critical. Together, ServiceNow APM and IRM let you create this alignment, providing an integrated solution that helps risk managers, application owners, development teams, and compliance teams work seamlessly together using a Risk Identification Questionnaire that's completed before the application is released into production. This allows these traditionally siloed teams to collaborate frictionlessly throughout the application's lifespan.

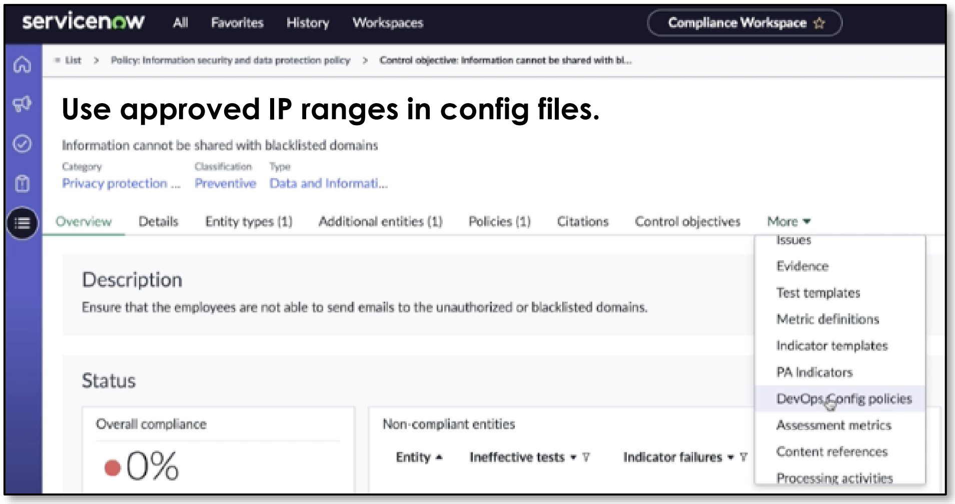
A risk manager at work

It's not a bad start to my day. We're going live today with a major application that many people are eager to learn about. When we first started planning for this new application, the application manager used ServiceNow APM to add the business application to the ServiceNow platform. APM helps manage licensing and maintenance and lets application managers and owners stay on top of the application lifecycle. Now I've got a notification that the application manager has changed the application state from design to inventory. I always get these types of notifications because IRM and APM work seamlessly together.

As part of the process, I work with the application owner to fill out the ServiceNow risk identification questionnaire. We determine the type of data the application will access, store, or process. IRM uses this information to calculate inherent risk and automatically assign the appropriate controls. Once the application owner attests the controls are in place and working, the system calculates the residual risk. If any risks remain, no matter how low, I'll work with the application owner to create tasks to identify the proper courses of action should any of these risks ever materialize. I can track the risk to this application and other applications at the same time using the Heatmap workbench.

I've implemented a risk assessment for the application. This assessment helps me continuously gather data from the application and IT owner. The assessment uses automated factors, which pull data from tables on the ServiceNow platform, but I could have also included manual factors, which require a manually entered response. Automated factors are continuously updated, so the assessment reflects the current risk to the business.

The leadership team wants to track reputational risk, so I've set up automated factors to monitor CSAT scores. A bad customer experience can affect business. There's one application that consistently stays high risk for reputational scores (bad CSAT scores), even though the other controls are compliant and there are no audit issues. Upon investigation, it looks like this application has had several outages. I'm going to need to bring together the development team and customer service manager to discuss a remediation plan.



Use approved IP ranges in config files.

Information cannot be shared with blacklisted domains

Category: Privacy protection ...
Classification: Preventive
Type: Data and Informati...

Description

Ensure that the employees are not able to send emails to the unauthorized or blacklisted domains.

Status

Overall compliance: ● 0%

Non-compliant entities

Figure 7: Complying with DevOps policies doesn't need to slow down development.

The DevOps team has been working hard and releasing code quickly. The outages are often a result of small data fixes and a few bad coding practices. We need to add policies and controls for the DevOps team alongside the other policies and controls for the application. The DevOps team can do this using the ServiceNow DevOps Accelerator and DevOps Config with Policy as a Code Engine (PACE). They create a process that tracks configuration policy compliance and exceptions via IRM. That way, if this application needs updating, the development team isn't slowed down, but I ensure we're maintaining compliance.

The application happens to be updated during the next dev cycle. We can see that the policy we put in place to ensure that developers have access to and are using the right IP ranges in the config files identified a violation. Because of DevOps Config policies and IRM integration, this was caught before the code was released into production. Addressing these issues before customers are affected helps improve customer satisfaction scores.

A single platform that allows application managers, development teams, and risk teams to share data and work together can help reduce the impact of business application development issues and application sprawl.

Tech Tip:

Many organizations house their policies on a SharePoint site or other application. Consider moving your policies into ServiceNow so that you can easily associate policies with controls and risks and report on compliance. You can also request policy exceptions and evolve into using DevOps config policies to clean up code and reduce vulnerabilities in real time. Integration with O365 and Word makes easy to collaborate to keep policies current and track versions.

Use case: Monitor HR policy requirements and identify onboarding risks

Your organization. For instance, you might use one system for onboarding and another to manage policies, but the policies don't map back to appropriate controls. And beyond internal policies and best practices, there's a wide range of regulations across the employee journey that can vary greatly from state to state and country to country.

- Is your company subject to local laws regarding pay for unused personal time off?
- Have all appropriate steps been followed during onboarding and termination?
- When was the last time employees confirmed the review of anti-harassment and insider-trading policies?
- Have the appropriate pre-employment background checks been completed?
- How do leave policies vary depending on where an employee resides?
- Have the appropriate policies been followed for whistleblowers, non-discrimination, sexual harassment complaints, and investigations?
- Have you implemented and approved the appropriate policies regarding separation of duty?

Fortunately, there's a relatively simple way to mitigate these risks. With a robust solution like ServiceNow HR Service Delivery working seamlessly in tandem with ServiceNow IRM, you have an integrated risk platform and an additional line of defense. IRM can monitor activity across solutions, automatically alert the appropriate teams when there is a compliance concern, track the concern through resolution, and prove that your organization has adhered to all requirements.

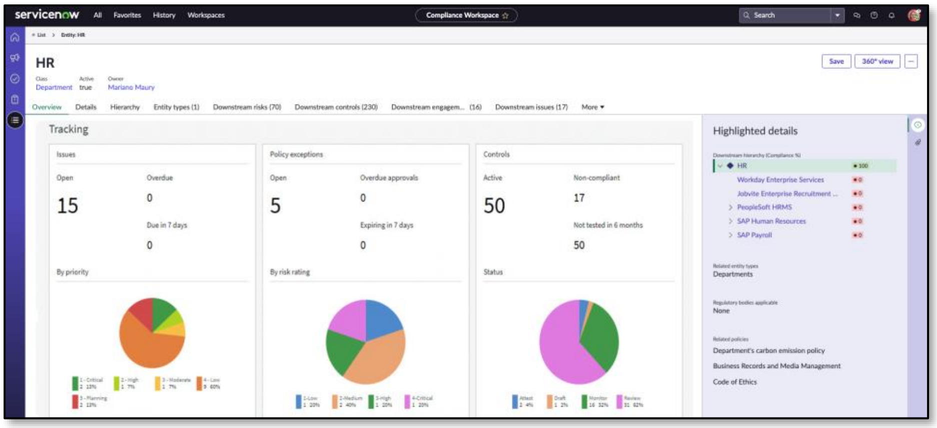
The bottom line: our integrated risk platform lets you spend time on people, not processes.

An HR manager at work

As a talent manager, I need to work with my team to ensure that our organization is following all the local regulations and our internal policies. These can vary greatly depending on employee location. In my ServiceNow dashboard, I can view reports specifically configured to help me track our compliance efforts. In one case, I can see an onboarding risk resulting from an HR task that was closed but never completed. The HR compliance manager is identified, as is the new employee.

When I drill into the closed but incomplete task, I see that a new employee (a much-needed account executive) hasn't signed a required NDA as part of the onboarding process—but the hiring manager has signed off on the case. Looking

at the risk, I see it could have a significant impact on the business. The account executive is scheduled to start tomorrow. This is in direct violation of our process.



HR

Class: Department | Active: true | Owner: Mariano Maury

Issues		Policy exceptions		Controls	
Open	Overdue	Open	Overdue approvals	Active	Non-compliant
15	0	5	0	50	17
	Due in 7 days		Expiring in 7 days		Not tested in 6 months
	0		0		50

Downstream hierarchy (Compliance %)
- HR ● 100
  - Workday Enterprise Services ● 0
  - Jobvite Enterprise Recruitment ... ● 0
  - PeopleSoft HRMS ● 0
  - SAP Human Resources ● 0
  - SAP Payroll ● 0

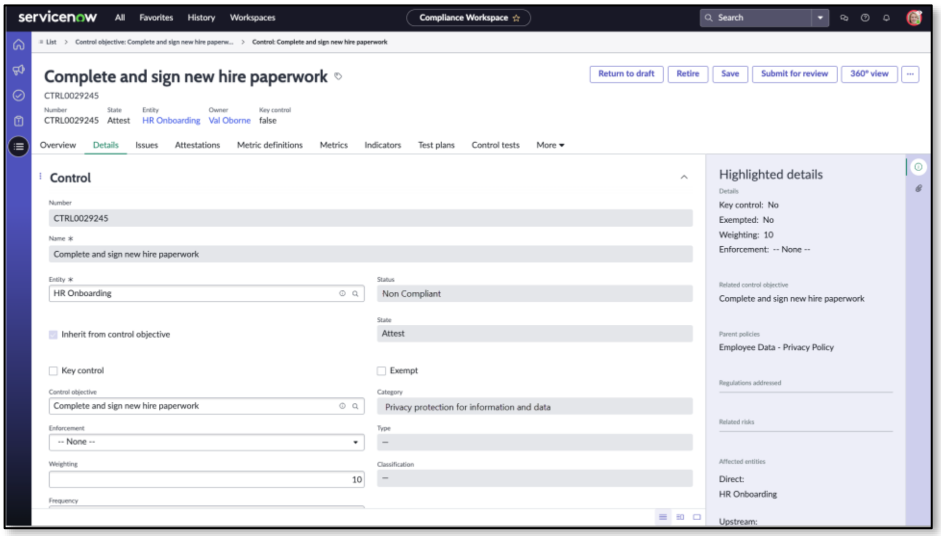
Related entity types: Departments

Regulatory bodies applicable: None

Related policies: Department's carbon emission policy; Business Records and Media Management; Code of Ethics

Figure 8: Drag and drop reports into your dashboard so it meets your unique needs.

IRM automatically identified the risk, but I can also see that the HR compliance manager noticed the error. When I look at the compliance manager's attestations, I see they indicated that the new-hire paperwork was not complete.



Complete and sign new hire paperwork

CTRL0029245

Number: CTRL0029245 | State: Attest | Entity: HR Onboarding | Owner: Val Oborne | Key control: false

Number: CTRL0029245

Name *: Complete and sign new hire paperwork

Entity *: HR Onboarding

Status: Non Compliant

☑ Inherit from control objective

State: Attest

□ Key control

□ Exempt

Control objective: Complete and sign new hire paperwork

Category: Privacy protection for information and data

Enforcement: -- None --

Type: --

Weighting: 10

Classification: --

Frequency

Details: Key control: No; Exempted: No; Weighting: 10; Enforcement: -- None --

Related control objective: Complete and sign new hire paperwork

Parent policies: Employee Data - Privacy Policy

Regulations addressed

Related risks

Affected entities: Direct: HR Onboarding; Upstream:

Figure 9: Attestations allow you to ensure policies are being followed.

When the system identified the risk, it automatically generated an issue and sent it to the HR compliance manager. That person will work with the hiring manager to resolve this before tomorrow. The new employee will see the NDA in their to-do list on the employee portal.

This situation also highlights the fact that we need to do more training for our hiring managers. I'll create a task for the HR compliance manager to schedule a meeting so we can discuss how this happened and modify our process if necessary. The HR compliance manager will create a task for the hiring manager to repeat online training for the hiring process. If I don't see it before our meeting, I'll have the compliance manager create it directly afterward.

I'm also going to monitor that the related issue and tasks are closed. When the signed document is uploaded, that will clear the violation on my dashboard.

Tech Tip:

We follow a similar process to ensure that new employees acknowledge anti-harassment, insider trading, and other policies during the onboarding process. ServiceNow IRM continuously monitors for compliance across all policies and regulations and helps us build a consistent response process that includes an audit trail.

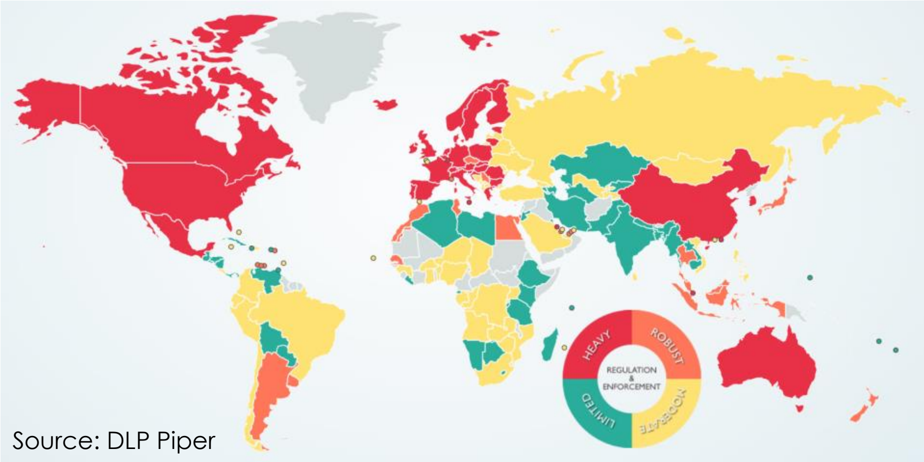
The CHRO also has a real-time view of the organization's global risk posture through dynamic dashboards tailored to their needs. And the CHRO can easily share information with other executives and board members, making it simpler for the team to prove compliance.

Use case: Ensure privacy standards are met

The General Data Protection Regulation (GDPR) has had an impact on virtually every company in the world with an online presence. Given the GDPR's hefty fines of up to 4% of global annual revenue, companies are taking precautions to ensure compliance. One added benefit is that, by complying, they protect their reputation with customers.

However, GDPR isn't the only data protection regulation that organizations must follow. Countries such as Japan, Australia, Brazil, Canada, and the United States have approved similar legislation—adding to the compliance burden.

Data Protection Laws of the World



Source: DLP Piper

Figure 10: The growing number of data protection regulations is adding complexity.

At ServiceNow, we take a different approach to compliance that allows you to easily meet all of these different privacy regulations. We identify the applications that touch personal data, gathering supporting evidence while tracking application compliance across functional groups. And we streamline access to critical risk, control, vendor, and security data. The result? You rapidly identify threats, improve efficiency, and protect your customers' sensitive data.

Key ServiceNow privacy protection capabilities include:

- Importing data privacy requirements and descriptions through Policy Management
- Distributing and tracking Data Protection Impact Assessments (DPIAs)
- Executing risk evaluations and managing issues
- Managing audit engagements
- Addressing data subject requirements and requests
- Facilitating Personally Identifiable Information (PII) mapping
- Addressing 72-hour breach notifications
- Managing third-party data privacy compliance
- Addressing Data Protection Officer (DPO) requirements and providing visibility

A data protection officer (DPO) at work

As the data protection officer (DPO), I need to make sure the policy and risk posture of my organization is strong. To do that, I need real-time visibility into security privacy events, risks, and compliance violations that could affect the business. I've built my dashboard with those things in mind.

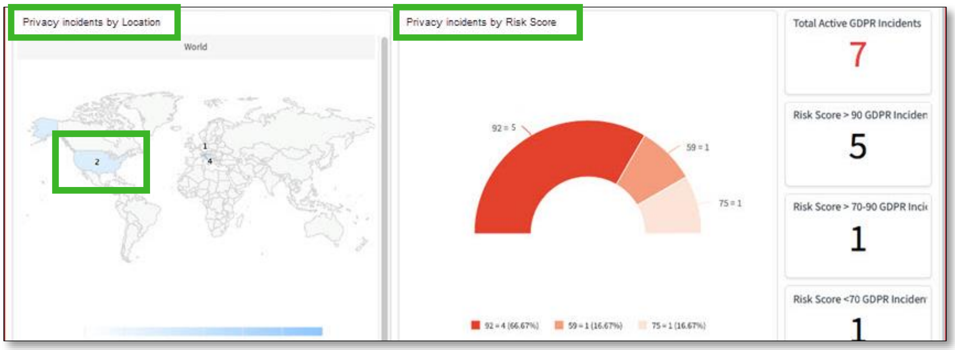

Privacy incidents by Location
World
2
1
4
Privacy incidents by Risk Score
92 = 5
59 = 1
75 = 1
🟥 92 = 4 (66.67%)
🟧 59 = 1 (16.67%)
▫ 75 = 1 (16.67%)
Total Active GDPR Incidents
7
Risk Score > 90 GDPR Inciden
5
Risk Score > 70-90 GDPR Inci
1
Risk Score <70 GDPR Inciden
1

Figure 11: The data protection officer needs real-time visibility into the security and risk posture of their organization.

One of my dashboard reports shows me data breaches by level of risk, and it indicates there's something I should be acting on. I have five major incidents with high risks. By clicking on the report, I can see there are two major security incidents in the United States. Drilling into the incidents in New York, I see that one of the incidents is linked to a possible attack on a server. Drilling in further, I see that my team has already analyzed it and tagged it as a privacy concern using the GDPR tag. As part of the workflow, the system automatically emails me and creates a task when the risk is escalated so that it appears on my dashboard.

When an incident is tagged as GDPR, the system automatically generates a new task for security and IT, informing them of the new risk. I can now drill into more details to find out how this incident occurred and how to prevent it from happening again. I acknowledge that a breach occurred, and once I close my task, the system automatically alerts legal, PR, and other critical response teams. The workflow also includes tasks to execute the data privacy response plan.

A link to the security incident is now part of the record and identifies which business service or entity is affected. In this case, the incident impacts SAP Financial Accounting and involves a third party. I select the vendor and see there is a risk that the vendor may have disclosed confidential information. The risk is calculated as moderate, which is higher than I'd like because my risk appetite is very low. I can also see the mitigating controls. Some are non-compliant, resulting in a moderate risk rating. The controls are common across the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

This incident causes the system to automatically trigger privacy and security assessments, which are sent through the Vendor Risk Management vendor portal. I'll watch for these assessments to come back and keep an eye on the security incident's progress as the responsible security analyst begins triage.

An integrated risk platform can share information quickly between departments, including a complete audit trail to comply with stringent requirements such as the GDPR 72-hour breach notification. Built-in workflows accelerate risk response by automatically generating risks and issues and routing them to the right individuals.

Tech Tip:

Different privacy regulations can share many common requirements. Be sure to define a common controls framework so you can test a control once and apply the results to multiple regulations. You either can do this manually or through integration with the Unified Compliance Framework or other content providers from the ServiceNow store.

Use Case: Proactively address third-party issues, including ESG

It's widely accepted that third parties are essential for business success, accelerating time to market, enabling innovation, and reducing costs. But these third-party relationships also represent a major business risk due to the massive business disruptions and reputational damage that can result from exposures.

As vendor risk management programs have grown, they have typically focused on a limited range of governance issues such as financial viability and cybersecurity, and even with these risks, many organizations struggle to scale vendor risk management due to lack of visibility and time-consuming manual processes.

Now, organizations are being asked to expand this scope to environmental, social, and governance (ESG) concerns due to both public pressure and recent regulations such as the EU Corporate Sustainability Reporting Directive (CSRD). For example, enterprises are increasingly expected to have a Net Zero strategy, and yet a significant part of a company's carbon footprint often comes in the form of Scope 3 emissions from its third-party suppliers. Similarly, organizations are held accountable for the labor and human rights records of their vendors. With vendor risk management programs already under strain, ESG threatens to push these programs past the breaking point.

ServiceNow transforms the way you manage third-party risks, including ESG. We provide consistent assessment and remediation processes, create transparency and accountability with an integrated view of risks across all your third parties, and reduces effort by automating key supplier risk management processes. And because these capabilities run on the Now Platform®, they work seamlessly with our broader set of integrated risk management capabilities, letting you holistically manage enterprise risk across your entire internal and external value chain.

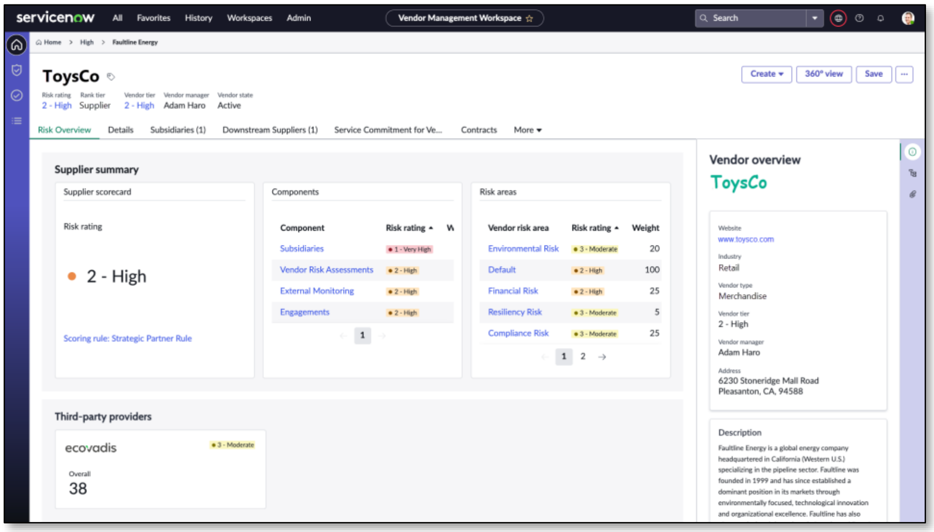
A third-party risk manager at work

I start every morning in my tailored ServiceNow Third-Party Risk Management third-party workspace, where I can get a status overview of all of my suppliers. The retailer I work for has many suppliers, so this makes it easy for me to see how we're doing and identify any issues I need to focus on.

I could look at the performance of my third parties in the performance tab, but I'm really here to look at the risk they pose to our business.

I notice that one of our primary merchandise suppliers, ToysCo, has a high risk score. The score was calculated based on the vendor risk assessment and engagement assessment I just sent out. Both of these came back high, even though the combined rating the system has calculated based on my risk intelligence feeds from EcoVadis and Interos shows a moderate risk.

I could look at ToysCo's subsidiaries, but I'm here to look at the issues. I see a high-priority issue was generated from the Human Rights vendor risk assessment that indicates ToysCo's SA8000 certification is no longer current. To get a better understanding of the issue, I click on the details tab.



ToysCo

Risk rating	Rank tier	Vendor tier	Vendor manager	Vendor state
2 - High	Supplier	2 - High	Adam Haro	Active

Supplier summary

Supplier scorecard

Risk rating

● 2 - High

Scoring rule: Strategic Partner Rule

Components

Component	Risk rating	W
Subsidiaries	● 1 - Very High	
Vendor Risk Assessments	● 2 - High	
External Monitoring	● 2 - High	
Engagements	● 2 - High	

Risk areas

Vendor risk area	Risk rating	Weight
Environmental Risk	● 3 - Moderate	20
Default	● 2 - High	100
Financial Risk	● 2 - High	25
Resiliency Risk	● 3 - Moderate	5
Compliance Risk	● 3 - Moderate	25

Third-party providers

ecovadis ● 3 - Moderate

Overall
38

Vendor overview

ToysCo

Website
www.toysco.com

Industry
Retail

Vendor type
Merchandise

Vendor tier
2 - High

Vendor manager
Adam Haro

Address
6230 Stoneridge Mall Road
Pleasanton, CA, 94588

Description

Faultline Energy is a global energy company headquartered in California (Western U.S.) specializing in the pipeline sector. Faultline was founded in 1999 and has since established a dominant position in its markets through environmentally focused, technological innovation and organizational excellence. Faultline has also

Figure 12: The dashboard shows the calculated risk score and each risk area.

If this were a less important issue, I might just create a task for someone to investigate or take a specific action. But this is more important. Since I've got the IRM Risk Management application, I'm going to create a risk event. I can do this easily using the button in the upper right-hand corner of the screen.

When the dialog box opens, it's already prepopulated with some information. This issue is a critical risk with a financial impact, so I'll make sure that's selected and enter the expected loss, which is $100k. The risk event gets created and assigned to the risk manager at the company as soon as I hit submit. The risk event will also show up automatically in the ESG Management workspace, so our ESG team will know about it.

Grace, the risk manager, sees the new risk event for ToysCo when she navigates to Show Risk Events in her workspace, along with all the information she entered. She checks out the impacted entity and decides to perform a root cause analysis.

After assigning the risk to herself, she lists the consequences and any actions already taken. She enriches the risk event by attaching the risk event to a specific "Potential reputational damage due to social issues" risk for the entity ToysCo. There are no other similar risk issues, so Grace simply submits the risk for approval. Now there is organization-wide visibility into this risk, and it can be monitored throughout the resolution process.

While Grace has been analyzing the risk, I've contacted ToysCo to try to address the issue. It appears they're in the process of recertifying for SA8000. I've added this information to the issue record, so we have an audit trail. I will also be returning the assessment to ToysCo because the responses were unsatisfactory.

Once they have obtained their certification, they can resubmit the assessment. Until that time, we will need to pause work with them. Luckily, we have an alternative supplier we can use. Once we receive the updated assessment, I will close the issue and mark the risk as being resolved. Since we're all working off the same source of data, everyone's dashboard will be automatically updated.

Being able to proactively address this issue may have saved my company thousands of dollars in fines and, more importantly, avoided reputational damage or lost customers.

Tech Tip:

If you have IRM and Third-Party Risk Management, you can create controls based on a specific response to a question on a questionnaire. An incorrect answer will result in a control failure and automatically generate an issue, speeding time to resolution.

Use case: Ensure your compliance program effectively supports your business services

Behind the curtain that separates the front and back office lies a battalion of systems, processes, and hardware. You'll also find a variety of monitoring tools—tools that create a mountain of data about compliance and security violations. These violations include faulty employee termination processes, unauthorized to mission-critical or sensitive data, security incidents, unpatched systems, unapproved hardware and software changes, emergency changes, and many others.

Combing through this data manually to uncover and prioritize the most critical business risks is a formidable effort. Without automated processes to ensure compliance, system, process, and hardware owners spend huge amounts of time analyzing data so they can attest that they follow the proper policies. And manual processes create a high risk of errors and issues slipping through the cracks.

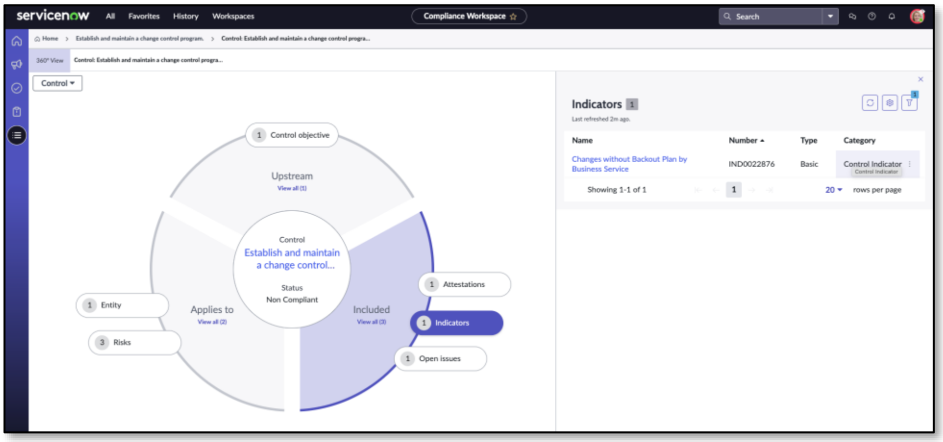
By using the same integrated, automated ServiceNow risk platform you rely on every day, you can be confident you're capturing the most critical issues while reclaiming thousands of work hours for high-value projects. You're able to easily and confidently prove compliance, and you make providing supporting evidence for audits virtually painless.

An audit manager at work

As an internal auditor, I know from experience that planning is important. Recently, I've been working on my audit plan for the year. The business control owners have completed the risk assessments I sent them, and I've defined the scope of my audit for this year, including PCI and SOX, our SAP Financial Accounting business service, our Linux servers, and server hardening. These are all defined in my Configuration Management Database (CMDB), so scoping them was easy. I don't have a very mature CMDB, but I've made sure the 20 most critical assets, processes, and systems are represented correctly.

Based on the results of my risk assessments, I've decided to begin my audit with the SAP Financial Accounting business service.

I can see from my dashboard that I have a compliance violation. Continuous



Indicators 1

Last refreshed 2m ago.

Name	Number	Type	Category
Changes without Backout Plan by Business Service	IND0022876	Basic	Control Indicator

Showing 1-1 of 1 · 1 · 20 rows per page

Figure 13: Regular monitoring ensures best practices are being followed.

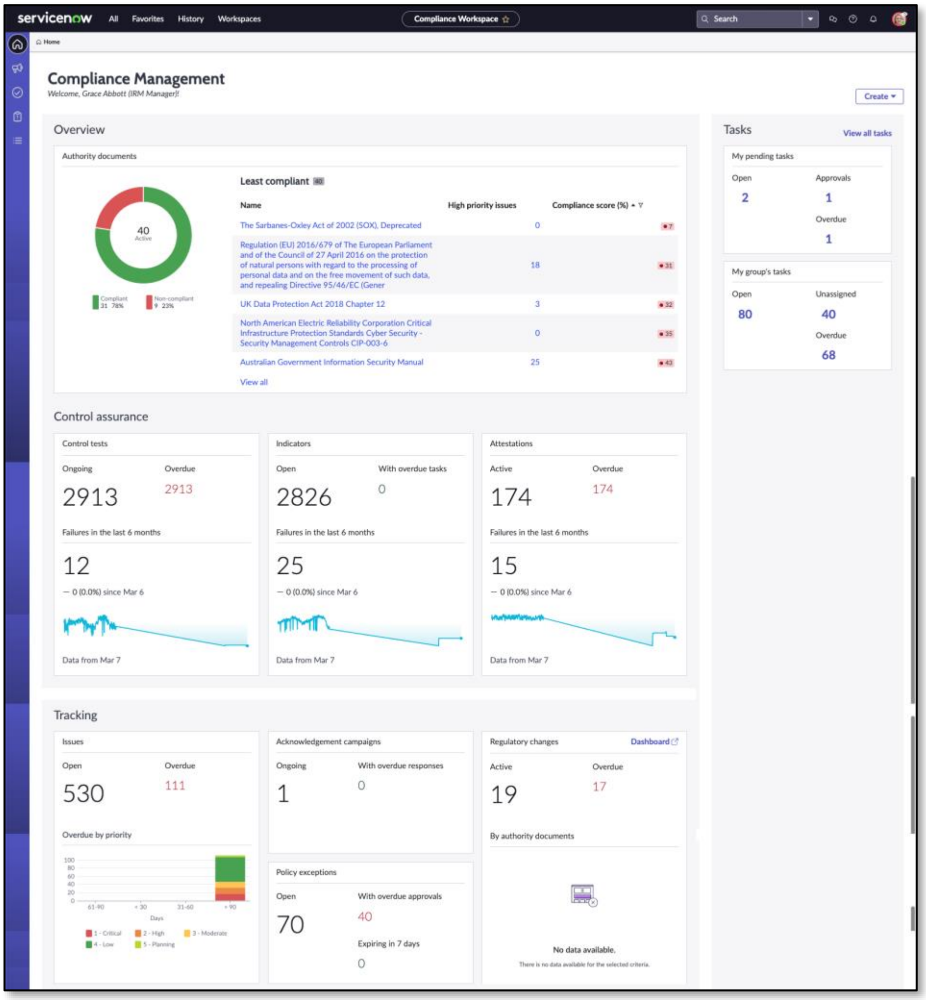
monitoring shows that someone implemented a change without a backout plan. As a result, the system automatically created an issue for the SAP Financial Accounting service owner.

The service owner decides to delegate the issue using the Assignment group field so a teammate can investigate why this happened. For instance, is there a history with this type of issue, and Is there a training opportunity?

After a discussion with the manager of the team responsible for the violation, it turns out the history of the issue goes back just a few weeks. New team members recently joined the company, and there's a clear need for training. The team manager promises to send the new members an attestation with a link to the change management policy, so they can read the policy and confirm that they understand it.

The issue is closed with a note stating that the "Manager will ensure proper training." I can see that the issue is closed, along with the notes from the investigation. We'll keep a close watch to ensure resolution.

When the external audit team arrives, they can check the current status of our controls. If they want, they can look at past results, the failures we spotted, our responses, and the complete audit trail of our actions. This data gives them a high level of confidence and helps to streamline our audit process.



Compliance Management
Welcome, Grace Abbott (IRM Manager)!

Overview

Authority documents

Least compliant 40

Name	High priority issues	Compliance score (%)
The Sarbanes-Oxley Act of 2002 (SOX), Deprecated	0	● 7
Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Gener	18	● 31
UK Data Protection Act 2018 Chapter 12	3	● 32
North American Electric Reliability Corporation Critical Infrastructure Protection Standards Cyber Security - Security Management Controls CIP-003-6	0	● 35
Australian Government Information Security Manual	25	● 43

Tasks

My pending tasks: Open 2; Approvals 1; Overdue 1

My group's tasks: Open 80; Unassigned 40; Overdue 68

Control assurance

Control tests: Ongoing 2913; Overdue 2913; Failures in the last 6 months 12; — 0 (0.0%) since Mar 6; Data from Mar 7

Indicators: Open 2826; With overdue tasks 0; Failures in the last 6 months 25; — 0 (0.0%) since Mar 6; Data from Mar 7

Attestations: Active 174; Overdue 174; Failures in the last 6 months 15; — 0 (0.0%) since Mar 6; Data from Mar 7

Tracking

Issues: Open 530; Overdue 111; Overdue by priority

Acknowledgement campaigns: Ongoing 1; With overdue responses 0

Policy exceptions: Open 70; With overdue approvals 40; Expiring in 7 days 0

Regulatory changes: Active 19; Overdue 17; By authority documents

No data available.
There is no data available for the selected criteria.

Figure 14: Interactive dashboards let you drill down into reports for greater detail.

Tech Tip:

As a starting point for populating your CMDB, define a minimum desired state. For example, a common criterion is "A server exists in the CMDB only if it has a relationship to at least one application." Otherwise, it's difficult to tell what the server is used for. ServiceNow allows you to create this type of requirement, so in the event of a violation, a notification is automatically sent to the appropriate person in IT, or a task is created to define the application for the offending server.

You can also use data certification to maintain clean information in your CMDB. Prompt application owners to attest whether their application is internet-facing or whether it accesses Personally Identifiable Information (PII) or credit card data (protected by PCI) by scheduling tasks at a specified frequency. The responses are saved directly to the CMDB.

An integrated risk program for 21st century risk and compliance challenges

It’s a relatively safe bet that the scope and potential impact of security threats will continue to increase—and that the compliance burden will continue to grow with them. On top of that, organizations undergoing a digital transformation face new challenges. To counter greater risks and increased pressures, you must embed risk management and compliance activities into new digital workflows and ensure various departments and functional areas think and act as one. They must share information more effectively, identify breaches and disruptions before they wreak significant damage, and utilize cross-functional workflows to enforce the required escalation, review, and response activities. Only an integrated risk program on a common platform can solve this challenge:

- Continuously monitor for risk and compliance across the extended enterprise
- Holistically prioritize risk based on business impact to improve decision making
- Automate repetitive and redundant manual tasks to increase performance

ServiceNow IRM helps make sure you not only comply with new regulations, but also thrive in this new era.

Find out more about how with ServiceNow you can:

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

Use Asset management and IRM – the more you know the lower the risk

Manage business continuity risk

Use the risk product portfolio to power your resilience business

Learn more at www.servicenow.com/risk.

servicenow