Now on Now:
How we’ve automated compliance monitoring to support regulated market customers
Contents

Introduction ........................................................................................... 3
Where our story begins ........................................................................ 3
Our strategic objectives....................................................................... 4
Implementing the best solution .......................................................... 5
  Research ....................................................................................................................5
  Build vs. buy assessment .....................................................................................5
  Design ........................................................................................................................5
  Development, testing, and deployment .......................................................5
Continuously compliant and ready to scale ...................................... 7
About ServiceNow ................................................................................ 7
Introduction

Managing risk is difficult for every business today. Technology environments are complex, data ecosystems are sprawling, and threats are pervasive.

The pressure only heightens when doing business within regulated markets. Managing regulated environments is tedious. Audits are frequent and comprehensive and there are serious repercussions for falling out of compliance, from lost certifications to lost customers.

In this case study, we’ll share the challenges that ServiceNow’s regulated markets team faced in maintaining compliance with some of the world’s most stringent regulations. And, more importantly, you’ll learn how we adopted ServiceNow integrated risk management (IRM) to help achieve continuous compliance.

Where our story begins

At ServiceNow, our regulated markets team works closely with our security, compliance, legal, and risk teams to track compliance rules and controls. Controls encompass basic rules like frequency of password resets and character minimums, all the way up to complex rules like the need to physically separate virtual machines or the requirement for data processing to only occur within a private cloud.

Prior to implementing our solution, we struggled with issue detection. As an example, we experienced 21 control failures within the environment of one regulated market over a period of roughly 18 months. Each failure was discovered manually by an internal auditor, administrator, or user. In many cases, failures were identified weeks or even months after they occurred. Much of the time, we simply didn’t know when we were out of compliance—we couldn’t see it.
When a failure occurred, we had to manually review lists of hundreds of controls to determine who or what team owned the control and should manage remediation. This labor-intensive process often took days to complete, driving up operational costs and leaving our risk levels elevated. We didn’t have the right tools or systems for proactive and continuous monitoring, so the best we could do was respond to problems reactively, which was taking far longer than what was expected from our compliance teams.

The legacy process we used is outlined in the chart below. We had technology to help us investigate and resolve control failures, but our activities were largely manual and reactive.

**Legacy process**

When a failure occurred, we had to manually review lists of hundreds of controls to determine who or what team owned the control and should manage remediation. This labor-intensive process often took days to complete, driving up operational costs and leaving our risk levels elevated. We didn’t have the right tools or systems for proactive and continuous monitoring, so the best we could do was respond to problems reactively, which was taking far longer than what was expected from our compliance teams.

The legacy process we used is outlined in the chart below. We had technology to help us investigate and resolve control failures, but our activities were largely manual and reactive.

**Our strategic objectives**

We knew there had to be a better way to work. We wanted to have greater control over our digital properties and deliver the business outcomes—across cost, risk, and other measures—that we set out to achieve.

Specifically, we aimed to:

1. Reduce manual issue detection and management
2. Significantly improve time-to-resolution
3. Gain better visibility into our environments
4. Achieve smooth audits with no surprises
Implementing the best solution

We took a methodical and phased approach to identify, build, and implement our solution.

Research (~2 months)
We began by engaging our IT risk management team to validate the scope of controls for which the regulated market team is responsible. We also engaged our compliance engineering team to align on control monitoring efforts and rule out potential redundancies.

Build vs. buy assessment (~1 month)
We evaluated several viable solutions on the market using specific criteria and a build-versus-buy framework. Because ServiceNow® IRM was one of our options, we scoped its capabilities to assess feasibility. Not only is IRM recognized by analysts as a leading risk management platform, but it offers us the benefits of being on the Now Platform®, which leverages a single data model and architecture to enable automated cross-enterprise workflows and unified experiences.

The final decision to move forward with IRM was made after extensive research documentation and presentations to internal executives and stakeholders. We took the time to address concerns, get buy-in, and elicit critical feedback.

Timeline

<table>
<thead>
<tr>
<th>Research</th>
<th>Build vs. buy</th>
<th>Design</th>
<th>Development</th>
<th>Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>~2 months</td>
<td>~1 month</td>
<td>~1 month</td>
<td>~6 weeks</td>
<td>~2 weeks</td>
</tr>
</tbody>
</table>

Design (~1 month)
Once we homed in on IRM as our anchor solution, we closely studied its features, capabilities, and limitations. We collaborated with our internal stakeholders to create a simple design that would help us be more proactive and effective in our management of regulated market environments.

Development, testing, and deployment (~2 months)
This was the simplest part of our journey—we had the benefit of implementing a solution that required little to no code. We kept the scope manageable by selecting ten controls that are easy to monitor. Testing was relatively swift, with only a handful of minor configuration defects identified and fixed.
IRM provides great out-of-the-box features, like an existing control library that aligns with FedRAMP guidelines. It was also a cinch to add our own in-scope controls library. Within IRM, we set up nine indicators to automatically monitor and detect control failures using a no-code method. A simple workflow auto-creates and auto-assigns an issue record to the proper remediation team when one of our indicators detect a failure.

Using the dashboarding capabilities of the Now Platform and ServiceNow Performance Analytics, we created a compliance health dashboard that helps our control owners gauge system compliance and risk levels at a moment in time and year to date. Issues are auto-populated into the dashboard in real time. Control owners can click into each area of the dashboard to explore specific issues and review historical data.

Supporting data
We can configure parameters on any Now Platform table to match the requirements of a given technical control.

Schedule
We can set the cadence for how often each control should be validated.

Results
We can view this always-on dashboard for a pulse check of all controls being monitored.

Compliance health dashboard
We can view this always-on dashboard for a pulse check of all controls being monitored.
Continuously compliant and ready to scale

We are responsible to many groups—customers, partners, auditors, governing bodies, and regulatory agencies. It’s paramount for us to manage risk and maintain the trust we’ve earned within the regulated markets ecosystem.

Today, we can do much more than we could before, and we didn’t add headcount or expend a lot of resources. By simply adopting IRM and taking advantage of the Now Platform, we’ve redefined how we maintain compliance and keep risk levels low.

Since implementing IRM, we’ve reduced compliance failure risk by 20% in our regulated market environments. The downstream impacts are huge, from cost savings to customer retention. Because we now have continuous monitoring, testing is simpler and less stressful for our operations team.

Looking ahead, we plan to expand coverage to monitor the complete list of technical controls in our regulated environments. We’re exploring innovation opportunities with IRM, such as building a plug-and-play microservice that gives any IT system owner visibility into their system’s compliance health. And our ongoing, hands-on experience with IRM will continue to inform future product enhancements to best meet the needs of customers like you.

Since implementing IRM, we’ve reduced compliance failure risk by 20% in our regulated market environments.