Now on Now: How ServiceNow has transformed its own GRC processes

Increasing scalability, lowering risk, and slashing costs by $500,000
Introduction

When your business is growing at 40% a year, it’s difficult to keep up. Processes that worked before are now breaking under the strain. Running a business with more than 7,000 employees—and doing it well—is very different from being a start-up. Spreadsheets and emails don’t cut it any more, not if you want to automate and accelerate every corner of the enterprise.

That’s what Andrew Wheatley discovered when he first looked at ServiceNow’s own governance, risk, and compliance (GRC) processes. Andrew heads up our internal audit team. He found himself at the sharp end of manual processes that just wouldn’t scale.

This ebook delves into ServiceNow’s GRC journey and how we’ve moved from time-consuming, siloed manual work to connected, automated processes that support our growth. Along the way, Andrew shares his experience and insights, including our challenges, how we approached them, our solutions, and the benefits we’ve seen.
Inefficient manual processes and lack of visibility

Andrew starts by recalling the pain: “We had people spending 90% of their time on SOX. Everything was driven by emails and spreadsheets—requests, tests, reviews, status—everything. Yes, we stored some information such as quarterly attestations, in databases, but there was no way to track progress. We ended up downloading data and running massive pivot tables just to get basic reports. We struggled with visibility and transparency, and that was blocking our way forward.” And, because no one else could access this documentation, Andrew’s team had to update all the controls.

“Governance, risk, and compliance touches nearly every area of our business. To manage risk effectively, you need real-time visibility. That’s what ServiceNow GRC gives us—24/7 automated assurance that we’re operating our business to the highest standards.”

— Chris Bedi, CIO, ServiceNow
Drowning in documentation

“We had to get out of the documentation business. The only way we were going to support growth was to spend 30% to 40% of our time on SOX—not 90%. Compliance is everyone’s responsibility, but unless we could drive automated workflows and give our business process owners self-service access, nothing was going to change,” said Andrew.

Police, not business partners

There was also another problem: business perception. Process owners saw the audit team as cops—policing processes rather than adding value. “We wanted to push ownership and accountability to the people who actually ran these processes. But to do that, we knew we had to give back. First, we had to make it easy by integrating compliance seamlessly into their everyday work. Second, we needed to actually help them run their business and manage risk, and that meant delivering real-time visibility of what their teams were doing, not just historical audits.”
Our approach to a successful GRC transformation

So, how did we go about transforming GRC at ServiceNow? What were the steps we took? How did we approach them? How did we use the ServiceNow GRC app and the Now Platform® to scale cost effectively and create a better control environment?

Clear goals, laser focus

First, we established clear goals—the outcomes that defined success. “GRC implementations fail when you don’t have a clear vision up front. You waste time heading off in the wrong direction, and it’s impossible to get organizational buy-in,” said Andrew.

Second, we decided to focus on SOX rather than taking on other areas such as ISO 27001, SANS, or GDPR at the same time. “You need to pick one area with low-hanging fruit and high business visibility. Otherwise, the business is going to run out of patience before you deliver,” stated Andrew.

Our GRC Goals

- Visibility and transparency
- End-to-end workflows
- Self-service portal
- Integration into everyday work
- Continuous control monitoring
- Automated evidence collection
- Real-time reports and dashboards
Unified solution, iterative approach

By choosing SOX, we were also able to cover all the core GRC capabilities, including policy and compliance, risk, and audit. That’s important because all of these processes need to work together. For example, by automatically collecting compliance evidence, we could dramatically simplify auditing. Similarly, risk management builds on compliance by continuously monitoring critical controls.

At the same time, we took an iterative approach, delivering a minimum viable product as the first step. “That allowed us to go live in just four months with a useful solution—even if it didn’t have indicators and dashboards. And it meant that we could get feedback earlier rather than rolling out a fully-featured offering that didn’t meet business needs,” said Andrew.

Enterprise-wide transformation

Another key reason why GRC initiatives fail is because they are treated as backroom projects. To succeed, GRC needs to be treated like any other transformation initiative. In our case, our CFO was the executive sponsor and approved the implementation budget.

“It’s important to understand and communicate the full business value. You may save $500,000 within your GRC team—and we did—but the total business impact can be millions of dollars,” said Andrew.
A comprehensive plan to drive adoption

This enterprise-wide approach didn’t stop at ROI. Our team engaged up front with business process owners to get them on board—and followed this up with a comprehensive plan to drive adoption. For example, there was mandatory training that covered everything from ownership and accountability to hands-on training on controls, attestations, and so on. And, the team also created further awareness through webinars all-hands sessions, and other regular communications.

Planning for the future

Finally, we understood that this was only the first part of our GRC journey. That meant we needed to plan for the future. For instance, we implemented SOX first, but wanted to use it more broadly. “We kept the design generic so we could reuse it. Where we did make SOX-specific enhancements, we made sure we could disable them easily. For example, we’ve been able to reuse policy management flowcharts and narratives as is, just reconfiguring the backend workflows,” said Andrew.
The benefits we have reaped

Since we started our GRC transformation, we’ve achieved significant results. We now have a full GRC implementation for SOX financial controls, including policy and compliance, risk, and audit. We’ve also successfully tackled other areas such as ISO 27001, SSAE 16, and FedRAMP.

Empowered business process owners

Now, our business process owners are full partners in the compliance process, using our ServiceNow service portal to manage their own policies and controls. With ServiceNow® Performance Analytics dashboards, they can also track audit activities, monitor compliance, and get real-time insights into the status of their control and risk landscape.

And this is done on the same Now Platform® that business owners use for their day-to-day work. “There’s no need to open up a separate GRC system. It’s right there along with their other business tools. That makes GRC a part of their DNA. We’ve also integrated GRC directly into their business processes. For example, our finance team uses ServiceNow to manage their monthly reconciliation. We’ve built controls around that, and as the reconciliation progresses, it automatically generates indicators linked back to these controls. It’s basically zero touch,” said Andrew.
Real-time visibility of compliance and risk

Monthly accounting reconciliation is just one example of how we’re using ServiceNow® GRC to give us near real-time visibility of our control and risk status. Currently, we’re automatically monitoring more than 100 indicators tied to controls. We’re also monitoring a complete set of SOX financial risks, as well as 50 other key risks across our business.

Combined with event-based alerts, that gives us 24/7 assurance. Andrew cites our SAP system as an example. “ServiceNow GRC automatically monitors our SAP configuration tables. When there’s a significant change, it alerts the business owner and asks the owner to confirm that the change was approved. If it wasn’t, we know right away and can roll back the change. Without ServiceNow GRC, we might never discover the issue.”
Dramatically increased efficiency

Back to our original problem: slow manual processes that just wouldn’t scale. How has GRC helped to transform the landscape, giving us the bandwidth we need to support our business growth?

Here are some examples:

• 66% reduction in quarterly control certification due to continuous control monitoring, as well as automated surveys, which are built into the Now Platform

• 85% reduction in the time needed to track status, due to real-time reporting and dashboards

• 90% reduction in coordination efforts with external auditors now using ServiceNow GRC to gain direct, transparent access to all our GRC data
Where are we going next?

Since our initial SOX launch, we’ve already successfully tackled areas such as ISO 27001, SSAE 16, and FedRAMP. Now, we’re working on GDPR and SANS and expect to go live with these shortly. By freeing up our GRC resources, we’ve been able to take on more and more critical areas. The more we automate, the more capacity we have to automate, creating a positive snowball effect.

Yet, it’s not just about taking on new compliance areas. Andrew says, “We’re also driving further fundamental improvements in our GRC processes—for example, expanding our automated monitoring capabilities. And there are a huge number of other opportunities. For example, ServiceNow GRC lets us rationalize controls across multiple overlapping authority documents, streamlining compliance even further.”
The bottom line

With ServiceNow GRC, we’ve saved $500,000 a year through process automation, and that’s just for SOX. That’s freed up resources to broaden our GRC coverage and keep pace with business growth.

And we’ve made GRC far stronger by turning it into a living, breathing discipline. Before, GRC was a slow, historical process that didn’t add value for our business owners. Now, business owners have real-time visibility of their controls and risks, so they can take action right away to address issues, before they become major problems. That empowers them, giving them ownership and accountability. And repositions our GRC team as a trusted business partner.
ServiceNow was founded on a very simple idea: that work should be easier.

That getting simple stuff done shouldn’t be so hard and complex stuff should be manageable. Today, the entire enterprise—IT, HR, customer service, security, and beyond—can tap into the power of the Now Platform® to create a better experience for employees, users, and customers, and transform the way work is done.