WHITE PAPER

# 8 Simple Steps for Automating Governance, Risk and Compliance (GRC)

Slash audit costs, improve efficiency, and minimize risk

servicenow sysintegra

We've helped hundreds of businesses spanning all major vertical industry sectors automate GRC processes. Along the way, we learned a lot about what makes for a highly effective implementation—and what doesn't. Now we want to share our learnings with you. This checklist highlights eight simple steps for automating GRC based on conversations with our most successful clients.

**Why automate GRC?**

While your mileage may vary depending on the solution you ultimately choose, on average, ServiceNow customers who automate GRC reduce audit costs by 80%. Other benefits of automating GRC include:

- Improving visibility into GRC initiatives
- Saving time by automating highly administrative, repetitive, or complex GRC processes, like evidence collection
- Reducing risks and preventing problems with continuous monitoring
- Responding quickly to business and regulatory changes

**Let's get started**

Check out these eight simple steps for automating your GRC processes in a way that maximizes value and minimizes cost.

1. **Define your business rules.** Your GRC application is only as good as your business rules. Define them upfront and include them in your implementation plan. Typical rules you'll need to define are:
   - Controls and control owners
   - Control tests and expected results
   - Test and control frequencies
   - Risks, impact, and likelihood
   - Critical vendors
   - Attestation surveys, questions, and required evidence
   - Who needs to interact with or view the contents of the GRC system and why
   - How your organization wants to map authoritative sources, policies, procedures, controls, and risks to one another
2. **Rationalize your controls.** As your business and your risk profile evolves, you'll need to periodically review and rationalize your controls. As part of this process, ask these questions about each of your controls:
   - How does this control support my business objectives?
   - Is this control actually preventing or detecting risk?
   - Is there a different control I can put in place that better protects my business?
   - Is there a control I can put in place that reduces process overhead and improves IT performance while also mitigating risk?
   - Can a complicated control be replaced with a simpler, more effective control?

> "On average, ServiceNow customers who automate GRC reduce audit costs by 80%.

3. **Consolidate your controls.** If you're required to operate controls across multiple regulatory authorities or frameworks (e.g., SOX, HIPAA, GDPR, and PCI), then you've probably already noticed that there are common, repeated controls. Yet most companies still treat each regulation or framework as an independent set of controls, performing multiple audits, redundant tests, and repetitive evidence-gathering activities. These separate activity streams cost your company thousands of work hours and excessive auditing fees each year.

   A better and less costly approach is to establish a single consolidated set of controls. By cross-mapping controls, you can test a shared control and demonstrate that it meets the requirements across multiple regulatory and best practice frameworks. We call this concept, "Test once, comply many." You can manually cross-map the controls or use tools such as the Unified Compliance Framework® to do the work for you.

4. **Define what's important.** Controls are meant to protect the things we value. When companies haven't defined what matters (or what's in and out of scope), then controls get applied to everything, regardless of importance. This results in massive amounts of unnecessary work and creates deficiency noise that can distract your organization from the real risks at hand.

5. **Identity your risks.** Identifying your risks — and the impact and likelihood of those risks occurring — will help your organization focus on the right things. It can also help you understand the true business impact of a failed control. When faced with finite resources, risk identification can help you prioritize your control testing and remediation activities.

6. **Start small.** Large-scale, complex implementations, which take months to implement, rarely meet expectations. This is true of not only GRC deployments, but also technology deployments in general. They are often taxed by resource fatigue, competing business demands, and the challenge of maintaining daily business operations during a complex project.

   Build a GRC roadmap with your implementation partner, which will let you add GRC functionality in between audit cycles to minimize business disruption. This approach has the added benefit of incremental technology adoption, which typically results in higher adoption rates.

7. **Build toward continuous monitoring.** Continuous monitoring means you can identify control deficiencies when they happen and immediately begin remediation. In other words, you can catch problems when they're small, and stop them from getting any bigger. This significantly reduces your overall risk, as well as the level of effort required to maintain compliance.

8. **Pick the low-hanging fruit.** When creating your GRC roadmap, look for early opportunities to eliminate administrative overhead, reduce your risk, or both. Start by automating GRC processes that are heavily administrative, or tackling those processes related to current audit findings or control deficiencies.

By following these eight simple steps, you will have a GRC system that scales with your business, greatly reduces compliance costs and resource requirements, improves operational efficiency, controls risk, and provides real-time insight into your entire GRC program.

**Want to learn more?** Visit **servicenow.com/grc**

"When companies haven't defined what matters (or what's in and out of scope), then controls get applied to everything, regardless of importance.

servicenow sysintegra