Top 5 Myths About Implementing ServiceNow GRC

Governance, Risk and Compliance (GRC) is an important area of focus for several organizations. Companies want a robust GRC program in place to help manage compliance with regulations and internal policies; enhance information security practices and streamline audits and remediation activities.

Organizations that are considering ServiceNow® as a potential tool for scaling and evolving their GRC capabilities generally have a few concerns about the tool. This article aims to dispel the Top 5 Myths our clients have expressed.

For most GRC teams, the biggest drains on their time are evidence collection and remediation tracking activities. Another major source of frustration is creating reports and dashboards from multiple data sources, compiled into various spreadsheets. ServiceNow GRC leverages the workflow and task management capabilities of the core platform to enable the collection of real-time data and to track and manage cross-functional activities.

If you are looking to automate your control testing and to build an integrated Service Management – GRC platform, ServiceNow offers several advantages:

- Embed your IT controls and compliance requirements into your organization's Service Management
- Leverage the Configuration Management Database (CMDB) to automate control testing
- Take advantage of a test-once, comply-many approach. Since control test instances store the results of the tests, you can re-use them across multiple regulations, and provide consistent results to auditors and regulators
- Leverage the Service Management processes to streamline remediation activities, by generating tasks for corrective actions and implement SLAs, notification and alerts.

Myth #1:

ServiceNow is an IT Service Management tool; not a GRC tool

Myth #2:

I need a robust CMDB before I can implement ServiceNow GRC

Myth #3:

I need a robust Risk Register before I can implement ServiceNow GRC

Myth #4:

Our organization already owns one (or several) GRC tools. I don't need ServiceNow GRC

Myth #5:

It will take too long and cost too much to implement ServiceNow GRC

It's true that a well-built CMDB is the center of information on services, systems, applications delivered to the business. However, a lot of organizations tend to boil the ocean in their quest for a robust CMDB.

You do not need a robust CMDB **before** implementing GRC. What you need is an ability to track the data that supports control testing.

+1 (612) 708 1500 | info@inry.com | www.inry.com/insights

Top 5 Myths About Implementing ServiceNow GRC

In the foundational stages of implementing ServiceNow GRC, you need CMDB to contain certain information –the basics like server names, locations, ownership, applications installed, relationship to other assets in the infrastructure – that are relevant to the scope of the applications or platforms for ITGCs. For example, if SOX is important to you, and your organization has 5-8 SOX applications, your CMDB needs to have reliable data related only to those applications. It is not required for the CMDB to be "robust" for the entire enterprise before implementing ServiceNow GRC.

As the GRC program becomes more mature and moves towards automation and brings in additional authority documents, GRC teams can work with the Configuration Management team to drive requirements for the CMDB, and the two capabilities can grow in tandem.

We all tend to say "Governance, risk and compliance" in a single breath, but in both theory and practice, Risk Management is a very different function from Compliance.

Organizations are subject to a variety of laws and regulations; and in addition, there may be certain internal professional policies, standards, best practices and procedures for which you drive compliance. Testing the level of adherence to these laws, regulations and policies is a good business practice. A strategy for measuring and monitoring this adherence is good Compliance Management; but not necessarily Risk Management.

Is there risk involved if there is non-compliance to certain regulations? Absolutely. But Risk Management is so much more.

ServiceNow GRC recognizes this distinction. While Compliance Management, Risk Management and Audit Management are all part of the GRC license, ServiceNow treats each component very modularly. Risk Management is a separate plugin within the GRC license and can be deployed at will. This can happen in parallel with, before, or after Compliance Management is implemented. Mapping relationships between Risks and Policies / Standards / Procedures / Controls is relatively easy and does not require a development effort in most normal implementations.

Most traditional GRC tools act as a centralized repository for Audit and Compliance Information. Using the tool, you can maintain the overall compliance and control hierarchy, including scope of audit / compliance, risks, controls to address the risks and mechanism to assess the controls. You can store related policies and procedures, reports and filing templates and schedules for various regulations. And traditional GRC tools stop there.

The reason ServiceNow GRC is so powerful is that it can do all that; and in addition; it provides the integrated Service Management – GRC platform. Most commonly used frameworks and regulations are modeled on ITIL principles. Generic examples are NIST,COBIT, and ISO standards, which is why the integration between Service Management and GRC makes sense. See Myth #1 for more details on how an Integrated Service Management and GRC application can benefit you.

It is possible for ServiceNow to co-exist with your other tools – where you continue to leverage your existing tools as a repository for your control framework and use ServiceNow GRC specifically for the automation of evidence collection and remediation tracking. Should you continue to pay for multiple tools? You decide.

You may have previously participated in traditional GRC tool implementations that required long development cycles with a "black box" approach – where you had to adapt your processes to the tool or circumvent the tool's limitations by spending time, effort and dollars to customize these solutions.

ServiceNow GRC's key differentiator is that it can be configured, not customized, to fit your specific needs and processes. You may think this requires a lot of time. This is a common myth. It's core workflow and task management capabilities are easily and rapidly configurable.

In addition, INRY has developed a highly efficient (Process Area Specific Sprints) PASS methodology, which has been honed over multiple engagements that makes it easy and fast to implement ServiceNow GRC. The foundational capabilities can be implemented in as little as 6-8 weeks. This gives you a viable product that you can start using immediately and refine over time. The implementation approach can be accelerated even further if you already have a control framework.

It can be a daunting task to choose the right GRC tools to support your Compliance, Risk Management and Audit Management needs. As you are gathering information to support your decisions, it is important to separate the myths from facts. If you require more information, or have specific questions regarding ServiceNow GRC capabilities or the INRY approach, please contact us at info@inry.com

2022 GLOBAL PARTNER Award Winner servicenow

Fastest Growing Company

FT FINANCIAL TIMES Inc. 5000

Certified & Secure

AICPA SOC 2 SOC 2 TYPE II CERTIFIED