Six Steps To Implement Risk Management Using ServiceNow GRC

ServiceNow® GRC has a Risk Management application which provides ways to:

- Organize categories of risks to normalize risk scores across the organization
- Consistently assess risks using a best practice workflow
- Understand and report on financial and statistical impact of risk to the organization

Our clients who are considering ServiceNow GRC ask us about the best way to get started with the Risk Management application.

We realize that managing and measuring risk to the enterprise can be an overwhelming exercise. Integrhythm has developed a methodology called "Process Area Specific Sprints" or "PASS" by combining best practices from Agile and Prince2. PASS is designed to rapidly deploy and introduce ServiceNow functionality into the organization's departments with a targeted focus, accomplished over a number of iterations, each spanning between 4-6 weeks.

This Perspectives paper describes a six-step process that Organizations can adopt to deploy Risk Management in ServiceNow using Integrhythm's PASS methodology. The approach enables clients to grow their risk management capability in tandem with their Compliance and Audit Management applications. A key benefit to the approach is that the Compliance and Audit Management applications are not dependent on Risk Management being completely deployed.

Step 1:

The Beginning – Identify

Before you do anything else, the first step is to identify and document your risk management process and the relationships between the risks in your risk register and map them to your compliance objectives and activities.

At this stage, you should also identify a process for Risk Assessments, and Risk Measurement. ServiceNow provides two ways to measure risks – the Qualitative approach used by many of our clients (Likelihood × Impact) and the Quantitative approach (Inherent and Residual Annual Loss Exposures). The Quantitative approach requires you to define values for Single Loss Expectancy (SLE), Annual Rate of Occurrence (ARO) for both inherent and residual risk. Annual loss exposure is the product of SLE and ARO. Most organizations do not have the process to calculate these values with accuracy so they tend to rely on the Qualitative approach.

Step 2:

No Looking Back – Consolidate

The second step is to enable the Risk Management application in ServiceNow. The Risk Management plugin is typically included in your ServiceNow GRC licenses. The main focus in this step is to consolidate your risk register and KRIs and combine them into a central repository within ServiceNow. All the information developed in Step 1, including your assessment process and the measurement approach are consolidated and migrated into ServiceNow. From here on, you have a minimal viable product where you can start using the tool to manage and maintain your Risks.

Step 3:

The Only Way Is Up – Integrate

The key differentiation between ServiceNow GRC and the other tools out there is ServiceNow's ability to automate risk management. If your risks have been mapped to your controls, you can now leverage ServiceNow's Indicators.

Indicators are used to collect data to monitor and measure compliance and risks; and are also used to collect audit evidence. This enables consistency and real time vs. point in time measurement. By adding Indicators to Risk (think of them as Key Risk Indicators) they collect the metrics and allow you to aggregate and integrate results from various assessments. You can also leverage other data available in ServiceNow (Service Management or Asset Management or Vendor data) to measure and monitor risks.

Step 4:

Teamwork – Automate

Once all three of the above steps are complete, Risk Management can team up with Compliance; and configure Issues to continuously monitor risks and automate risk management activities.

In ServiceNow, Issues can be automatically created when:

- An indicator result is Failed or Not Passed.
- An attestation result is Not Implemented.
- Control test effectiveness is marked "Ineffective" and the state of the test is Closed Complete.

Step 5:

Become a leader – Influence

While risk management is a strategic function, most of our clients note that it quickly devolves into an operational role. So much of a Risk Manager's time is spent on collecting data; analyzing it; collating, aggregating and slicing and dicing it for senior leadership reports, that there really isn't much room for generating insights or thinking strategically.

With ServiceNow, most of the routine data collection activities become automated. Alerts, SLAs and notifications can be used to track various activities and perform automatic escalations. This enables Risk Managers to more proactively and consistently assess risks and measure them; understand and provide real-time reports on financial and statistical impacts of risks to the organization; and assist in both qualitative and quantitative risk-based decision making.

Step 6:

Success – Sustain

So what does a successful implementation look like? It's the point at which a high functioning Risk Management organization can

- Continuously improve risk management practices
- Use KRIs to drive organizational behaviors
- Help the enterprise rapidly adapt to changing conditions by having visibility not just into the risks themselves; but the inter-relationships between the risks which are fully embedded into your compliance framework

Further Information

For more information about our Risk Management approach or methodology, please visit **www.integrhythm.com/grc/** or contact us at **info@integrhythm.com**

Integrhythm Inc.

© Integrhythm Inc. All rights reserved. All other brands, service names, trademarks and/or registered trademarks are used to identify their respective owners.

www.integrhythm.com
linked.in/integrhythm
info@integrhythm.com