

High level of uncertainty and reduced tolerance to systemic impacts is leading several organizations to achieve a more formal and effective Risk Management approach

For many organizations risk management is rapidly developing into a more forward looking, enterprise-wide approach. The high level of uncertainty and the reduced tolerance to systemic impacts is leading several organizations to achieve a more formal and effective risk management approach.

As organizations increase their focus on being proactive and desire a more aggressive risk mitigation discipline, the burden of identifying, cataloging, mitigating and managing risk is becoming cumbersome.

If your organization is starting to look for a technology that can support a Risk Management framework, focused on workflows to assess, manage and mitigate risks, you might have arrived at ServiceNow as a viable solution.

This article discusses a simplified approach for organizations looking to formalize their risk management program for the first time using ServiceNow. Please note, this article does not intend to cover the entire depth, breadth and complexity of Enterprise Risk Management. Also, INRY does not claim to have Enterprise Risk Management expertise, this is merely a guide to implementing Risk Management using ServiceNow.

Every organization has its own framework and process, whether documented or not; depending on the scope of the Risk Management efforts, the complexity and Industry. They may have a framework designed internally for their unique needs; or perhaps adopt an authoritative Risk Management framework, such as the NIST Cyber Security framework, COSO Enterprise Risk Management – Integrated Framework or the RIMS Risk Maturity Model (RMM) etc.

INRY Risk Management Lifecycle

INRY has attempted to create a simplified and generic Risk Management Lifecycle, intending to address common tasks performed. This is used to assist our clients with their ServiceNow implementation for Risk Management.

1. IDENTIFY

Consolidating information from multiple sources to generate a risk register

5. MANAGE

Ongoing evaluation and re-assessment of risks

2. ANALYSE

Review risks, assign categories, and understand impact

4. MITIGATE

Define, assign, and manage risk mitigation / reduction activities

3. MEASURE

Apply scoring mechanisms to quantify and prioritize inherent and residual risk, establish KRIs

Creating a risk register is a crucial first step in ensuring the success of your ServiceNow Risk Management implementation

1. IDENTIFY

Risk Identification is an arduous process requiring organizations to consolidate and organize information from several sources. According to IMA's "Enterprise Risk Management: Tools and Techniques for Effective Implementation, Institute of Management Accountants, 2007.", organizations may use any or all of the following methods to collect information related to existing as well as emerging risks within their organization:

- Brainstorming
- Event inventories and loss event data
- Interviews and self-assessment
- Facilitated workshops
- SWOT analysis
- Risk questionnaires and risk surveys
- Scenario analysis
- Using technology
- Other techniques

Creating a risk register is a crucial first step in ensuring the success of your ServiceNow Risk Management implementation. These risk registers, maintained in ServiceNow as frameworks and associated risk statements, play an important part in helping you with tracking risk scores, priorities and categories and mitigation and remediation activities. Risk statements can be imported into ServiceNow from an excel sheet or created manually.

2. ANALYZE

Different authorities describe Risk Analysis activities differently. For the purposes of our approach, INRY describes Risk Analysis as the "Characterization and Categorization of Risks" – this implies classifying risks according to risk drivers, impact or any other collection of "buckets" that are the most relevant in the context of your Organizations Risk philosophy.

- Legal
- Financial
- Operational
- Reputational
- Legal/Regulatory
- Credit
- Market
- IT

In addition, organizations also like to categorize Risks as High / Medium / Low. Sometimes this is done iteratively with the next step, "Measure"

3. MEASURE

According to Information Systems Audit and Control Association (ISACA), Risk Analysis can be performed by one of two methods: Quantitative Analysis or Qualitative Analysis.

Quantitative Risk Assessment involves quantification of all elements of the risk, including the asset value, determining an exposure factor (EF) for each threat, calculating a Single Loss Expectancy (SLE), calculating the potential Annual Rate of Occurrence (ARO) and deriving an Annual Loss Expectancy (ALE) by multiplying ARO with SLE. The advantage of this approach is that it is based on assigning an actual financial value to the risk. The downside, obviously, is that you cannot always quantify the impact of the risk in terms of dollars.

Most organizations use a Qualitative Analysis or a non-financial analysis for Risk measurement. This is based on intuition and experience. The most common qualitative analysis used for Risk measurement is the simple Likelihood x Impact formula. The Risk is scored based on the probability that it might occur in a year (Likelihood) multiplied by the damage it can cause if unmitigated (impact). Scoring is typically performed on a scale of 1 to 5 or 1 to 10.

ServiceNow supports both methodologies and does not restrict you in any way if you cannot perform Quantitative scoring. You can still use the Qualitative method to effectively manage and track risk.

It is easy to configure business rules to assign a priority to the risk, as described in the Analysis section, based on the Risk Score.

4. MITIGATE

ServiceNow has a fantastic underlying workflow engine and native ITSM capabilities which makes it a truly unique risk management platform.

According to The Forrester Wave: Governance, Risk and Compliance Platforms, Q1 2018, "ServiceNow's GRC module leverages the information that the ITSM tool collects (including data for asset management, change management, incident management, and problem management), which makes a compelling driver for IT GRC use cases.

Key takeaway: Customers of ServiceNow ITSM are finding ServiceNow GRC to be an easy transition that helps them take a risk-based approach to information security and IT operations."

This means that the ability to manage and mitigate Risk is supported well by ServiceNow. If you have the ITSM product on ServiceNow; then the people that are most likely to use the platform for Risk Management are probably already using it for ITSM. ServiceNow's workflow engine makes it easy to track the "states" of a risk – from "draft", to "review" to "retire" and generate workflows for exception management and risk acceptance.

5. MANAGE

According to the Institute Of Internal Auditors (IIA), Risk Management is not a once-and-done thing. Truly effective risk management requires continuous monitoring, risk assessments, internal audit assessments, and an ongoing evaluation of an ever-changing and dynamic global business environment. In fact, this is the most daunting aspect of Risk Management.

ServiceNow makes this easier by providing an ability to create indicators for continuous monitoring; ticklers or notifications for key dates or action triggers; and setting automatic alerts/ notifications when Assessments or Risk Acceptances have been assigned to various individuals within an organization.

You can also monitor risks by mapping them to internal policies or controls, essentially flagging off a risk when a control is observed to be compromised or fails.

Out of the box reports and dashboards make it easy to create an Inherent Risk Heatmap.

Effective Risk management requires continuous monitoring, risk assessments, internal audit, and an ongoing evaluation of an ever-changing global business environment

Summary

In conclusion, if you are evaluating ServiceNow for Risk Management, you are probably on to a viable solution.

The ServiceNow platform is very feature-rich and can be an overwhelming experience initially if you are new to Risk Management within the platform. INRY has a very simple and straightforward approach to implementing Risk Management, which can be enhanced over time as the maturity of your organization grows and evolves.

For more information, feel free to contact us at info@inry.com



Fastest Growing Company



Certified & Secure



SOC 2 TYPE II CERTIFIED