ServiceNow Vendor Risk Management

As your vendors become privy to more of your sensitive systems and data, their risk and compliance posture becomes even more important to your security. Best practice is to assess your vendors on a regular basis, but until now, it has been a time-consuming and error-prone exercise comprised of spreadsheets, email, and rudimentary legacy risk management tools.

ServiceNow Vendor Risk Management transforms the way you manage vendor risk through vital reporting of vendor risk and issues, a consistent assessment and remediation process, and automated assessment procedures. It provides a means to facilitate stakeholder interactions, drive transparency and accountability, and effectively monitor vendor-related risks. By aligning vendor risk management with overall enterprise risk management priorities, you can create an essential integrated view of risk and a stronger extended enterprise risk posture.

Dashboards and reporting

Dashboards and reporting provide visibility into your vendor tiering, risk and tier assessment plans, open issues, and risk across your vendor ecosystem. Dashboards are customizable, while reports can be scheduled or run on-demand. Both are a standard part of the platform.
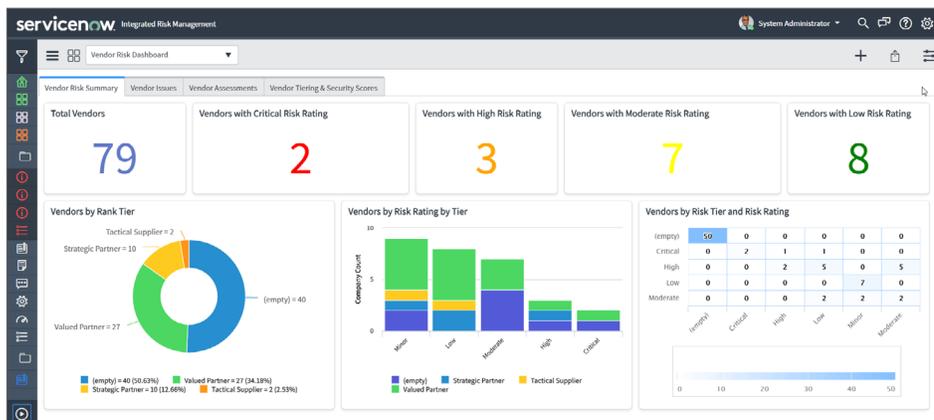

Figure 1: Vendor risk overview dashboard with tiering reports

Vendor portfolio

The vendor portfolio is your database of vendors and vendor information. This includes the vendor contacts you interact with, the business services and products that the vendors fulfill, vendor assessment records and documentation, along with other general vendor information.

The existing company table within ServiceNow is the default for compiling vendor data. If you already have vendor information in ServiceNow ingested through Vendor Performance or an asset discovery service it is immediately available to Vendor Risk Management. Vendor information can be updated manually or be integrated with an existing supplier management system, using the Now platform integration capabilities. Also, a self-service portal is available so vendors can maintain and update their own information.

Gain Efficiencies Through Automation

Deliver a system of engagement to manage stakeholder relationships, automate routine processes and risk scoring, and manage risk throughout the vendor assessment life cycle.

Reduce Your Risk Exposure

Monitor risks and issues in your vendor environment, and assess the impact to the organization's risk posture.

Respond to High-Risk Vendors

Accelerate decision-making across stakeholders and facilitate cross-functional remediation and risk mitigation processes.

Increase Communication and Collaboration

The Now platform collaboration engine, issues management capabilities, and the Vendor Portal bring together your extended enterprise

Leverage a Unified Platform

Speed assessment, scoring, and risk prioritization of vendors by using GRC indicators and vendor risk scores.

Assessment management

Assessment management allows you to create assessment templates, which are a combination of questionnaires and document requests. Assessments can be designed for internal purposes to assess a vendor's tier or delivered to vendors to track risk. Vendor assessments are based on the assigned tier or classification schema.

The assessment designer allows you to standardize your key document requests and convert your internal Excel-based questionnaires. Alternatively you can leverage the built-in Shared Assessments Standardized Information Gathering (SIG) questionnaire to streamline the process of collecting, parsing, and scoring a risk assessment. Automated scoring of vendor risk assessment responses is based on a robust hierarchical weighted scoring framework. Tier scores are also automatically generated based on responses to the tiering assessments. Both scoring frameworks are fully configurable.

Vendor tiering and automating risk assessments

Integration with security score providers allow you to get a third-party view of the security performance of your vendors. This knowledge can be used to manually adjust calculated vendor tier scores.

Vendor risk assessments can be sent to vendors on a defined schedule, an ad-hoc basis, or automated based on an initial tier assignment, manual tier change, or security score change.

Vendor portal

All vendor interaction and communication is centralized in a user-friendly vendor portal to eliminate inefficient email communications and status tracking via spreadsheets.

The vendor can manage their response team inviting members from their various functional groups to collaborate and assigning tasks within the vendor portal. The vendor portal provides you and your vendor stakeholders visibility and transparency on the status of assessments, issues, and tasks.

Issues and remediation

The Now platform enables cross-functional cooperation for issue management based on assessments. When an issue is identified, it is easy to collaborate with the vendor and subject matter experts to design remediation plans; this also makes it easier for the vendor to define and respond to issue remediation. You can associate issues to risks, controls, and risk ratings at a questionnaire and assessment level. A status column identifies the critical issues that could have the greatest impact on the vendor's risk posture and warrant immediate attention with the vendor.

Notifications

Notifications keep you informed of events that concern you; options include email, SMS text message, or push notification.

A unified GRC program

The Vendor Risk Management application can be used in conjunction with the core GRC applications. For example, when a vendor is linked to a GRC "profile type," any controls applied are assigned to that vendor's profile. This control requirement would then be visible in the Vendor Risk Management application.

Also, Vendor Risk Management issues can be associated with an internal risk in GRC when a vendor is assigned as a profile; providing linkage and monitoring capabilities.

Using the Policy and Compliance Management application, individual questions can be mapped to a vendor's
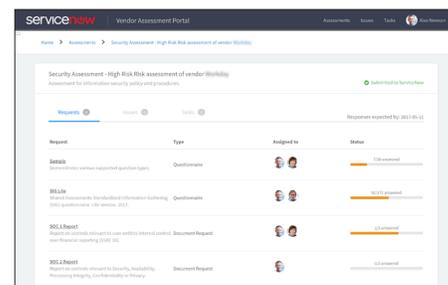

Figure 2: The vendor portal keeps all communications in one place.

control and the response can impact that control—marking it as "compliant" or "non-compliant" during the review. This can be used to provide top-down traceability from an authority document or compliance requirement to the question in a questionnaire for a specific vendor. Through the Risk Management application, non-compliant controls can automatically adjust the risk score associated with that vendor.

The Vendor Risk Management application on the Now platform eliminates the need for multiple applications used to communicate with and assess vendors, ensures consistent process executions, workload management, and various avenues of reporting. The Configuration Management Database (CMDB) integration can be used to accelerate dependencies mapping and fine-grained impact analysis. The service management platform can facilitate testing and evidence data collection of the vendors' process and IT controls, at scale. Using the GRC and security applications on the Now platform, you can provide your organization with a more comprehensive definition and proactive approach to managing risk, compliance, and security.

For more information

Visit our website at
www.servicenow.com/grc

servicenow.