SAI360

Risk | Learning | EHS | Sustainability

SAI360 Vendor Risk Managment

Solution Description

CONFIDENTIALITY STATEMENT

TABLE OF CONTENTS

OVERVIEW

In order to provide quality of service as well as maximize profit margins, organizations are lowering their operational costs by partnering with third-party vendors who mostly manage critical business operations. But the catch-22 is that adding third and fourth-party vendor technologies to improve business agility means creating more vulnerabilities for hackers to exploit.

Organizations are realizing that cybersecurity is now made up of more than just the standard IT security infrastructure. Vendor risk managers also play a huge role in building a strong and resilient security posture. In today's highly regulated and competitive business environment, automation is essential for effectively managing extended digital risk. An organizations' ability to track and automate activities is critical to reducing non-compliance risk and improving their overall digital risk and security posture.

This document describes the Vendor Risk Management (VRM) solution. It specifies how the software supports the vendor risk management process and outlines the solution design.

SAI360 Vendor Risk Management helps organizations to quickly and effectively implement a Vendor Risk Management program. The solution enables organizations to streamline and manage risk and compliance across the enterprise and extended vendor network, achieving a more consistent and efficient Vendor Risk Management process to support a complete view of digital risk.

SAI360 is a multilingual platform that offers by default English, German, French, Spanish, Dutch, and Portuguese. The solution is easily translatable to include additional languages and supports the documentation of one or multiple content languages.

BENEFITS

Once implemented and delivered, your organization will receive the following benefits:

- Expand your extended network of third-party vendors and save time in the process with streamlined onboarding and risk rating scores for security, financial posture, and exclusions that prioritize vendors and allocate resources based on their criticality and relevance to your business.
- Efficiently and effectively perform multiple levels of vendor risk assessments and understand your vendors' gaps without the traditional use of unreliable tools such as email and spreadsheets.
- Prioritize remediation of high-priority risks.
- Never miss an update with ongoing third-party screening for financial, cyber, credit, and other vendor risks via integration partnerships.
- Gain insights and act with out-of-the-box reports, with slice-and-dice and visualization capabilities of your vendor risk management results.
- Best-practice based implementation of vendor risk management, rapidly and with the adjustments needed to meet your organization's specific needs as defined in the Statement of Work.

SAI Global's vendor risk solution automates the VRM process end to end, scales to manage hundreds to thousands of vendors, monitors workflow and progress, consolidates risk data, and enables organizations to adapt the reporting to get a true picture of the vendors risk profile.

KEY CAPABILITIES

FastStart for Vendor Risk Management includes the following key capabilities:

- Personalized notifications that can be triggered automatically for the vendor to complete a vendor Risk Assessment survey at the appropriate level of detail based on the responses to the Profiling questionnaire.
- User-friendly interface to increase user participation in questionnaires.
- Pre-configured questionnaires that are mapped to control frameworks such as NIST CSF, CIS, and SIG.
- One-page vendor risk summarization, based on risk assessment and automated scoring and grading, including industry name, provided by partners.
- Vendor management tools to categorize and rank vendors based on their criticality and relevance to the business.
- Out-of-the-box vendor risk reporting with slice-and-dice and visualization capabilities to communicate VRM efforts at a high level or with detailed granularity.
- Digital audit trail of VRM activities.
- Full integration with other Integrated Risk Management use cases, such as Business Continuity Management, Incident Management, and Policy Management, among others.

VENDOR RISK MANAGEMENT SUMMARY

The SAI360 Vendor Risk Management helps organizations to manage risks on their entire third-party vendor portfolio in an efficient manner, not only by allowing a consistent and easy-to-manage way to identify and proactively mitigate exposure to risks, but also by providing a central repository and intelligence for collecting and correlating data, revealing trends, and harvesting actionable insights.

This section describes briefly the Vendor Risk Management solution delivered as part of the GRC/IRM platform. The figure below shows an overview of the key steps within the VRM process and the core functionality supported by the solution.

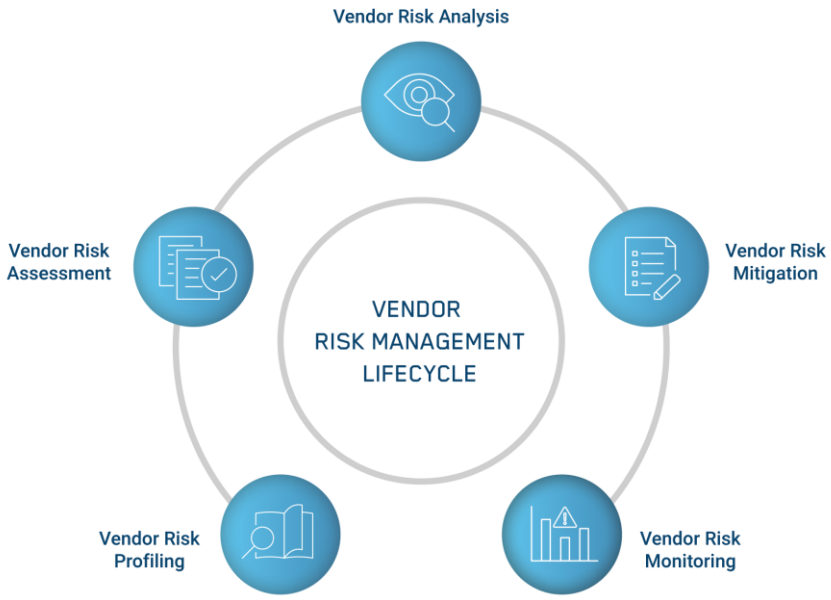


Figure 1: Vendor Risk Management cycle

VENDOR PROFILING

Instead of trying to achieve the impossible by trying to understand all risks a business may face, a saner approach would be to look at the criticality of known, identifiable risks. Risk criticality involves looking "around" the vendor. That is, assess the vendor's necessity in the first place by asking questions around their purported need instead of more direct questions. For example:

- What would the vendor's data access frequency be like? Would it be the same or change over time?
- What levels of data sensitivity does the vendor need? What kinds of data sensitivity can they clearly articulate and why? Can they state what they will not need access to?
- Which country or countries does the vendor operate in, from a labor perspective? What about from an electronic data storage perspective?

This list isn't exhaustive, but rather illustrative to explain a different way to size up a vendor or third party. Responses to these questions should not only yield answers, but also a visceral reaction on how important or critical a misstep in that area could be to your business.

Users can instantly onboard and prioritize vendors by following an easy-to-use wizard. This onboarding process categorizes vendors according to their access to information, to the services they provide, and to their importance to the business. The onboarding helps to establish the criticality level of vendors, which triggers risk assessments and alert messages.

RISK ASSESSMENT

After the initial vendor risk baseline, performance is measured with ongoing assessments that show patterns and changes. Analytics databases and applied BI are leveraged to graphically present real-time findings, making them easily understandable across the organization.

The automated and ongoing questionnaires keep the information fresh and never static. They address cybersecurity risks, policies, and regulations to show the gaps between regulatory requirements and a vendor's actual performance. They provide flexibility to use industry-accepted frameworks to tailor the solution to individual needs.

RISK ANALYSIS

Organizations need a system that offers an algorithmic calculation of the likelihood of a breach and its potential severity, vendor by vendor, as each gets scored in real time. This replaces assumptions with actionable insight and tells the company who to do business with and who to avoid.

The solution offers an automatic calculation of the risk index of vendors according to the answers provided to the assessment and to risk factors associated with the questions.

RISK MITIGATION

Understanding the impact of the vendor risk landscape is the key to effectively defend against it. Once risks and their criticality are assessed, businesses can put into play a mitigation plan for unacceptable issues that pose a large risk to the organization.

Vendor risk mitigation can take many forms:

- Require the vendor to change their process or business to meet the organization's needs. Depending on the severity of the risk and the willingness of the vendor, this is often the best approach, but not often the easiest.
- Ensure a level of trust through documentation. Vendor validation through certifications, reviews, and audits can instill a level of confidence in the business that the vendor is operating to a satisfactory level.
- Protect against missteps with legal language. Defining and agreeing to specific (minimum, average, etc.) levels of performance can be achieved with service-level agreements (SLAs). In addition, these can limit liability or define recourse if something in the partnership runs afoul.
- Periodically check on the vendor's performance. Whether remote or on-site, checking that the vendor is indeed honoring their terms of the contract through actual

observations demonstrates the business's level of concern with potential risk issues. In addition, these observations can be regular or irregular; announced or unannounced.

- Terminate the vendor/business relationship completely. This may not address missteps from the past, but severing the working relationships can prevent many further risks from occurring.

With the SAI360 Vendor Risk Management, once an unacceptable issue is identified during the risk assessment, the risk analyst prioritizes, evaluates, and implements the appropriate risk-reducing controls/countermeasures by creating mitigation plans to follow up on the progress, review, approvals or rejections of countermeasures.

RISK MONITORING

With ongoing risk monitoring and alerting, organizations can supplement manual risk assessments and stay informed when important events related to a vendor occur. Vendors can be understood more thoroughly with ongoing screening for financial, cyber, credit, and other supplier risks through integrations and continuous monitoring solutions.

The dashboards and analytics provide a true picture of the vendor risk profile to organizations so that clear next steps can be determined using out-of-the-box risk intelligence reports with slice-and-dice and visualization capabilities of the findings of the vendor risk management process.

ROLES INVOLVED IN THE PROCESS

PERSONA	ACRONYM	DESCRIPTION
Vendor Contact	1. VC	The Vendor Contact role is responsible for contracts with clients. This profile: • Completes the risk assessment questionnaire and provides evidence of answers; 2. Keeps the risk at an acceptable level required by the client by mitigating risks related to identified issues.
Relationship Owner	3. RO	The Relationship Owner role is responsible for contracts with vendors. This profile: • Follows up activities of vendors under their responsibility on the vendor risk management process; • Tracks and reviews activities and tasks to mitigate issues; 4. Requests exceptions (authorization) to do business with vendors at an unacceptable risk level.
Risk Analyst	5. RA	The Risk Analyst role is responsible for the identification of vendor risks. This profile: • Follows up answers and evaluates questionnaires on risk assessments, reports issues, and provides recommendations on vendors; • Communicates vendor risks to the business area; 6. Track risk evolution on vendors.
Vendor Risk Manager	7. VRM	The Vendor Risk Manager role is responsible for the overall vendor risk management process. This profile: • Monitors the team's activities on risk assessments, mitigation, and other tasks; • Reports changes on the risk posture of vendors to stakeholders; • Follows up activities of the VRM team; 8. Manages the team's workload.

Vendor Exception Committee	9. VEC	The Vendor Risk Committee role is responsible for the vendor risk management. This profile: 10. Evaluates and approves vendor exception requests.
Solution Administrator	11. SA	The Solution Administrator role is responsible for the solution configuration. This profile: 12. Configures rules, alerts, and global parameters.

SOLUTION COMPONENTS

Organizations today look more and more for business partners to support part of their processes, to provide specialized knowledge, to reduce costs, or to expand the business. This results in an increasing dependency on third parties to manage organizations' data, including employees' data and customers' data. Exposing sensitive data to other organizations adds risks to the business and requires additional controls to guarantee compliance with regulations.

FastStart for Vendor Risk Management provides customers with a solution that includes:

- Vendor profiling for easy onboarding and prioritization of vendors, leveraging an easy-to-use wizard that triggers assessments and alert messages.
- Vendor risk assessment with pre-configured questionnaires mapped to industry standard control frameworks.
- Continuous vendor monitoring with risk mitigation, exception workflow, and automated due diligence.
- Management reporting for real-time reporting and analytics to showcase the impact of the vendor risk management program at a high level or with detailed granularity.

VENDOR PROFILING

When relationship owners need to request a risk assessment of a vendor under consideration, a vendor onboarding process can be initiated. Right after the vendor is registered on the platform, a profile questionnaire is sent to the relationship owner, which obtains basic demographic information about the vendor and contact persons, as well as personal data privacy and corporate relationship information to define the vendor criticality. Based on the answers provided, a pre-configured rule will categorize the vendor according to their criticality. The criticality of vendors will define the questionnaire that will be used during the risk assessment to identify issues and categorize the risk level of vendors.

The risk posture of the vendor for the organization can be defined by a combination of:

a) Automated Due Diligence - During the profiling process, an automated due diligence is carried out through the integrations to provide a thorough scanning of vendor risk data for a complete understanding of the different types of vendor risk. Supported by integrations with external tools such as SecurityScorecard (cyber risk) and others, the vendor risk management team will have additional information to make decisions and prioritize actions on vendors.

b) Associations - Vendors can be associated with assets and risks. These associations will produce a deeper view of vendors and the impact of their risk on other processes and sub-processes.

c) Products and Services - Another additional information that may be relevant to help the vendor risk management team make decisions on vendors comes from the related products or services. Relationship owners can register products and services provided by vendors, and during this process, some important questions are answered.

Results from risk assessments and continuous monitoring are integrated into a single vendor workspace, enabling the organization to easily visualize risks and take immediate action.

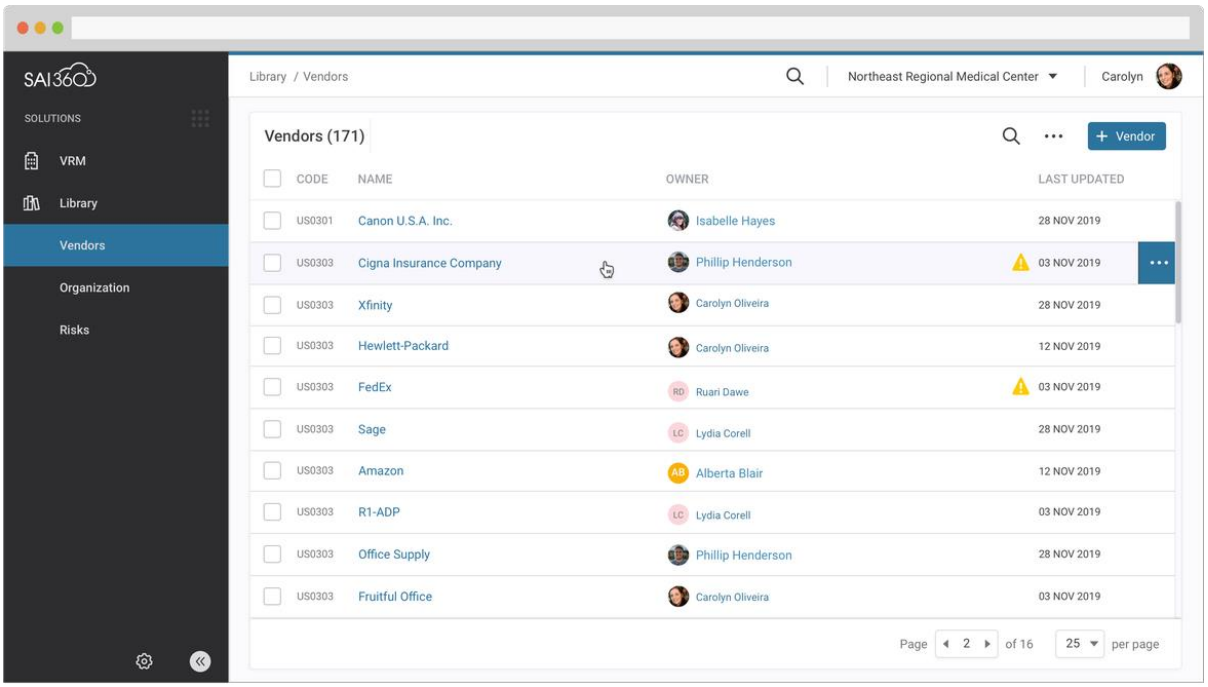


Figure 2: Vendors Workspace

The vendor profile management compiles all the vendor profiles in a single place. Profiles provide a comprehensive view of vendors, concentrating all the information about them and also associated products, risks, assets, contacts, risk assessment, and profile questionnaire. Here you can also track the risk posture, open issues, and open mitigation tasks.

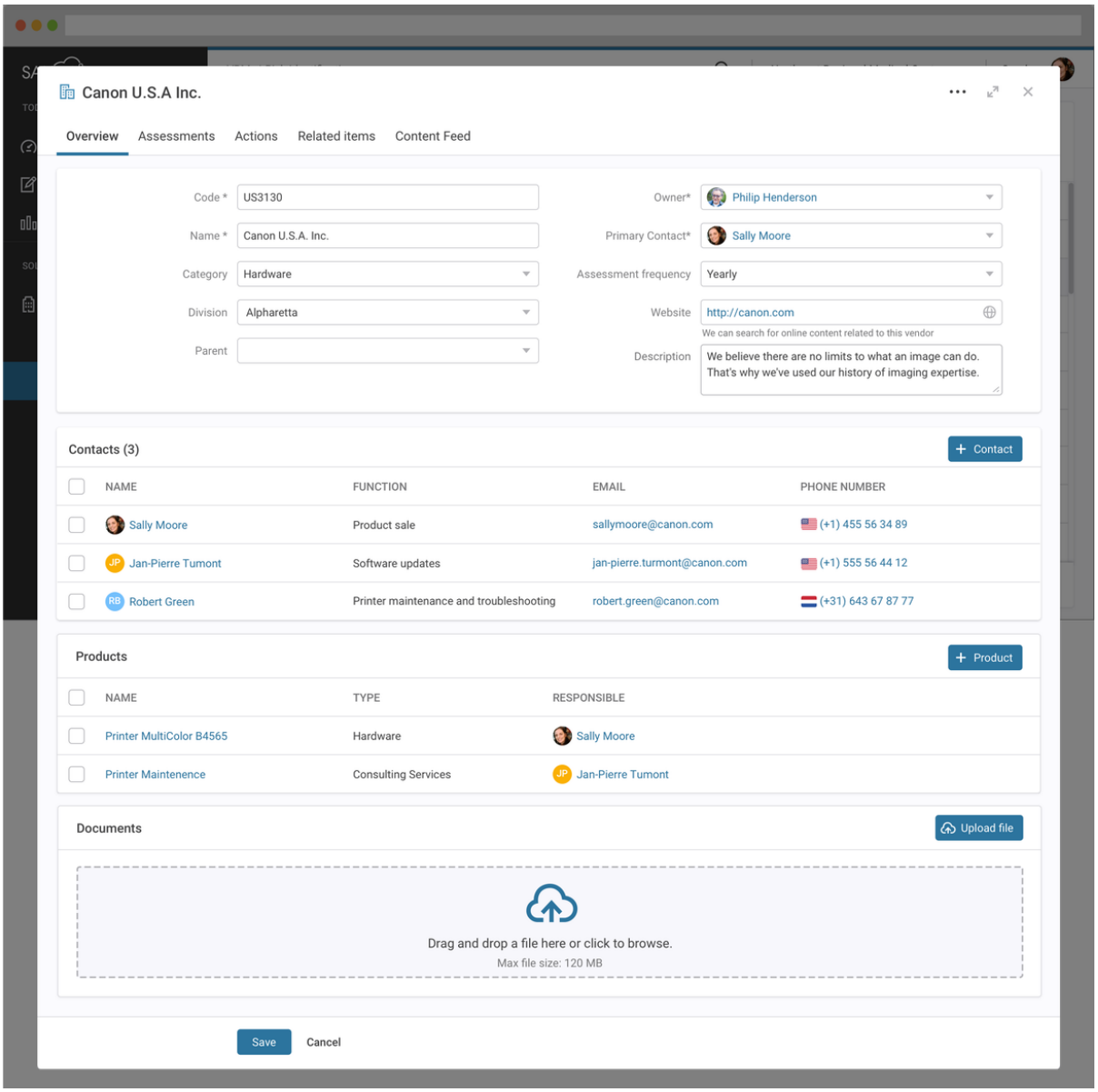


Figure 3: Vendor Profile

VENDOR RISK ASSESSMENT

The Vendor Risk Assessment phase starts with an email sent by SAI360 to the vendor contact person, when a new vendor is getting onboard or when an established vendor is being reassessed. The risk assessment can be scheduled to occur on a regular basis or it can be sent on-demand as needed. The e-mail sent by SAI360 contains a link to the risk assessment questionnaire, according to the vendor profile classification. The link takes the vendor representative directly to the vendor risk assessment questionnaire.

The FastStart for Vendor Risk Management utilizes pre-configured questionnaires (out of the box or customized) to automatically calculate the risk index of vendors according to the answers provided to the questionnaire and to risk factors associated with the questions. For example, privacy risk if an encryption control is not in place for a vendor that has access to personal information. The system implements intelligent capabilities as part of the interview, such as: questions that expand or collapse based on previous responses; the ability to add comments to each question; the ability to upload evidence to support each response; the ability to save partially completed questionnaires for later completion; the ability to export questionnaires to XLS files and later import them; and the ability to have support text and links to external sources for additional explanation.

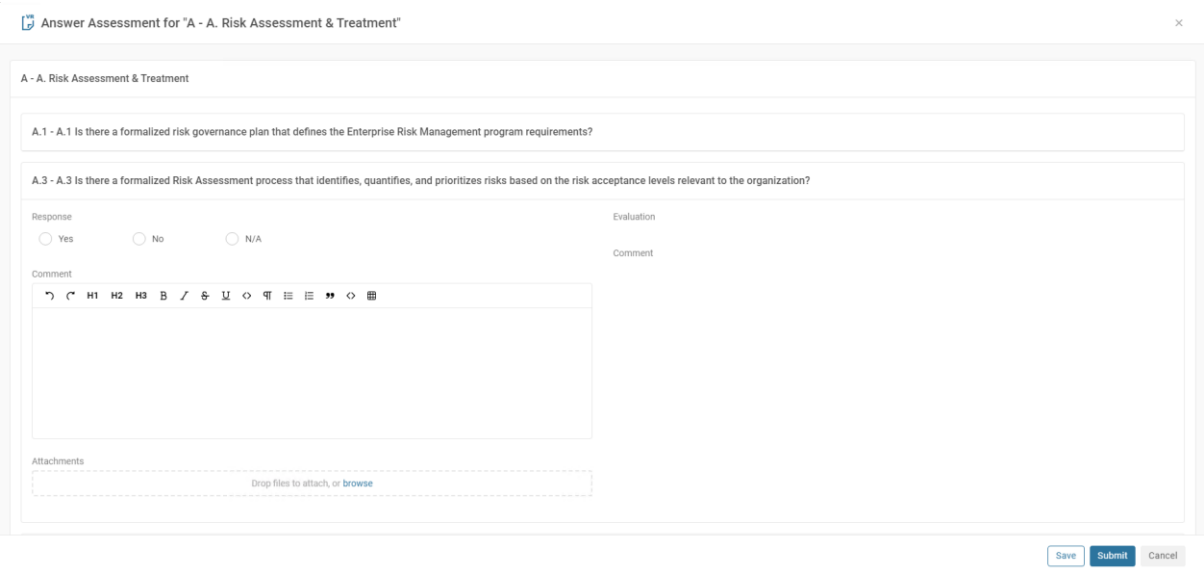


Figure 4: SIG Questionnaire

Once the vendor completes the questionnaire, SAI360 sends a notification to the assigned reviewer to evaluate the responses, comments, and evidence files provided by the vendor.

With the risk assessment workflow, risk analysts can view the assessment status that indicates if the vendor has started the risk assessment survey, whether it is completed, and the percentage of questions completed for surveys that are in progress. SAI360 also sends interview notifications to both the vendor contact and the reviewer. This process helps to manage timelines and offers a more realistic estimate of delivery dates.

Reviewers can change responses provided by vendors and add their own comments. After reviewing the interview, reviewers can either submit the responses, completing this step, or return the survey back to the vendor representative for further clarification. At this point, SAI360 allows a back and forth communication between the vendor representative and the

reviewer through comments in the survey until the reviewer deems the interview completed.

While evaluating the responses, the risk analyst can accept individual or multiple risks that do not pose a large impact on the organization, as well as create issues so that unacceptable risks can be mitigated through the implementation of a mitigation plan.

As a result of the analysis, the vendor will be categorized according to its risk level and score, which are calculated considering the answers provided to the questions and their weight.

CONTINUOUS VENDOR MONITORING

In a dynamic and demanding risk environment, continuous monitoring can provide valuable communication tools and insights that reveal a more comprehensive, real-time or close to real-time picture of the vendor and the organizational security posture of that vendor. Monitoring strategies should be evaluated whenever changes occur to business elements (both internal and external), such as core mission, risk tolerance or business processes, to ensure that controls function appropriately, and any new gaps are identified.

AUTOMATED DUE DILIGENCE

As organizations need to integrate with cybersecurity and social media monitoring tools to monitor vendors in real-time as much as possible and react to changes, an automated due diligence process is carried out to enhance the risk posture understanding of each vendor's profile.

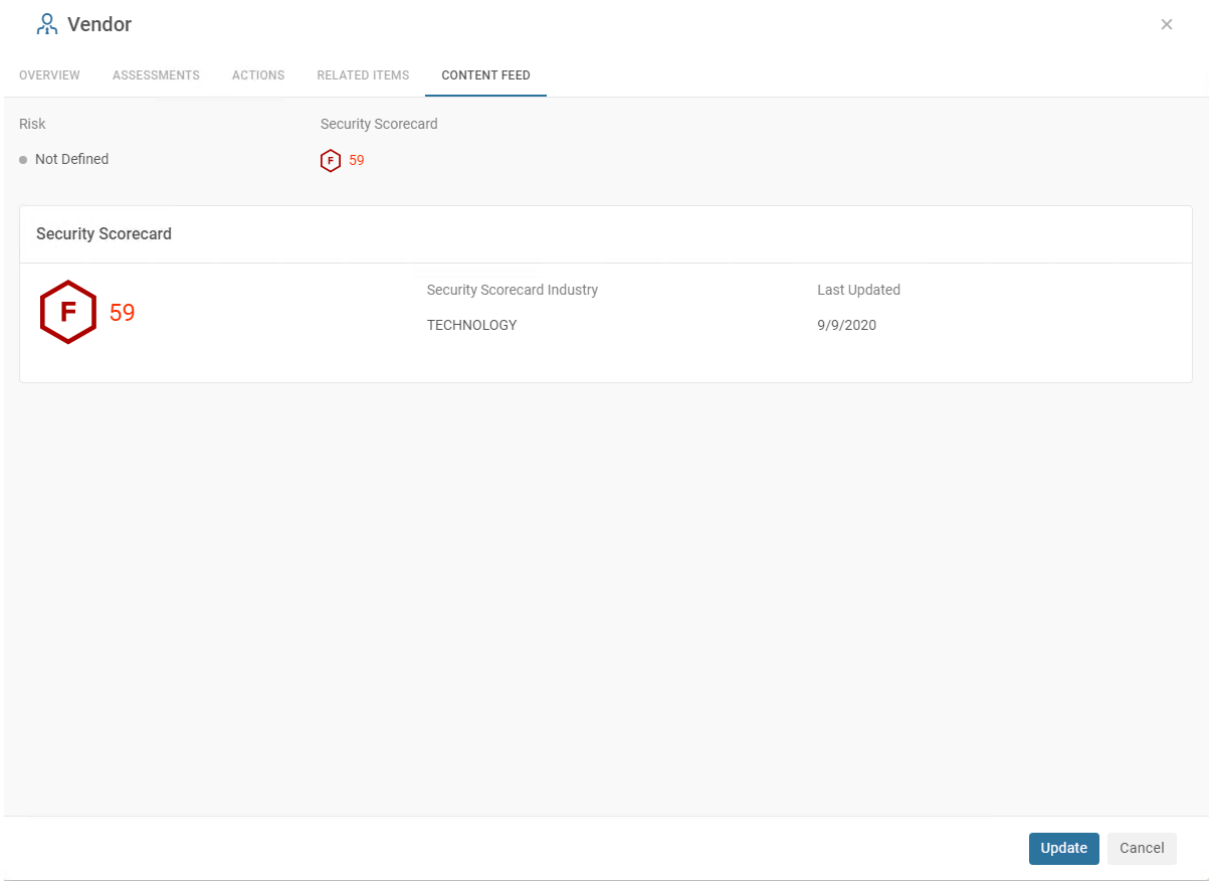


Figure 5: Vendor Grading and Scoring

VENDOR RISK MITIGATION

With SAI360 Vendor Risk Management, once an unacceptable issue is identified during the risk assessment, the risk analyst prioritizes, evaluates, and implements the appropriate risk-reducing controls/countermeasures by creating mitigation plans to follow up on the progress, review, approvals, or rejections of countermeasures.

The risk mitigation process automatically notifies the relevant vendor contact to initiate the implementation of corrective actions or procedures to satisfy the established mitigation plan for all the issues associated with it.

The Mitigations workspace is used to maintain and relate mitigations to issues identified in the risk assessments. Here you can also inspect mitigation details and related information and monitor and follow up the current mitigation plans in place. You can drill down into mitigations to see their details and relations, as well as track the evolution of vendors' proposed corrective measures to remediate issues.

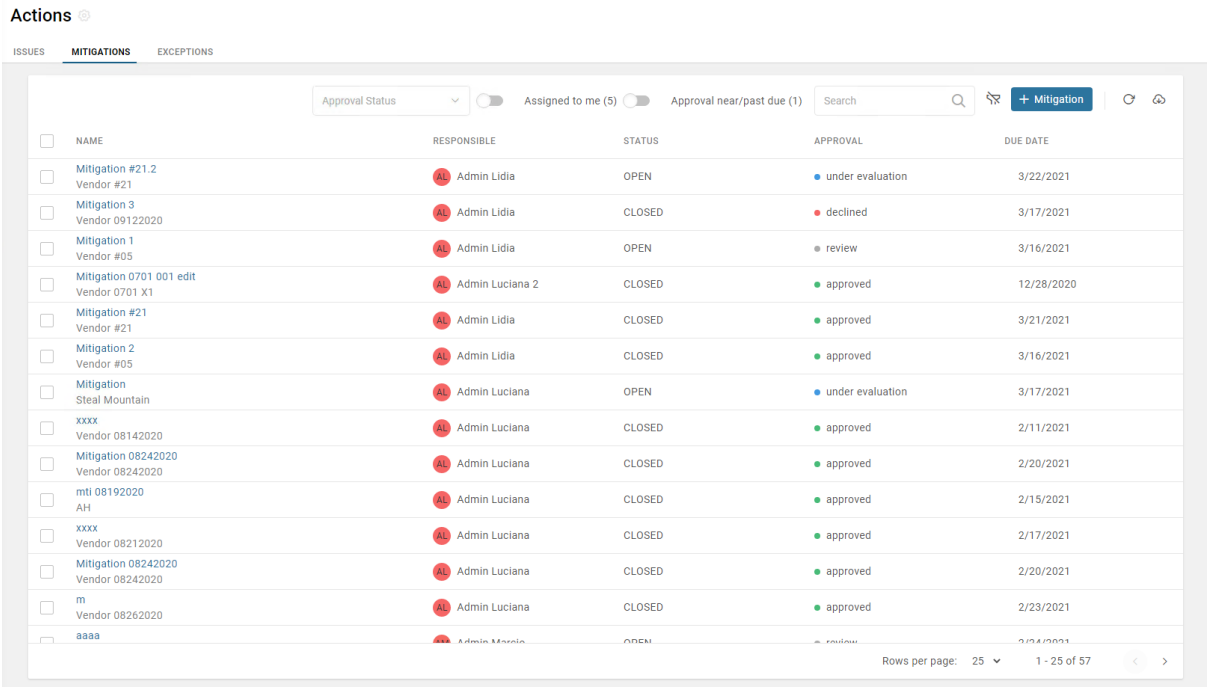


Figure 6: Mitigations Workspace

VENDOR EXCEPTION

After the risk assessment, the risk analyst will proceed with the recommendation on the vendor. Some vendors can be recommended, and others not recommended. The relationship owner can request a waiver to start (or keep doing) business with a vendor that was not recommended. In the waiver request, which will pass through an approval, the relationship owner needs to justify the business criticality and the reasons for working with a vendor that was not recommended by the Vendor Risk Management team.

All exceptions are associated with the originating risks and their scores, so customers can report and follow up to understand how exceptions affect the overall risk posture.

The Exceptions workspace displays all exception requests and related details, including the request owner, approval status, and validity of the waiver.

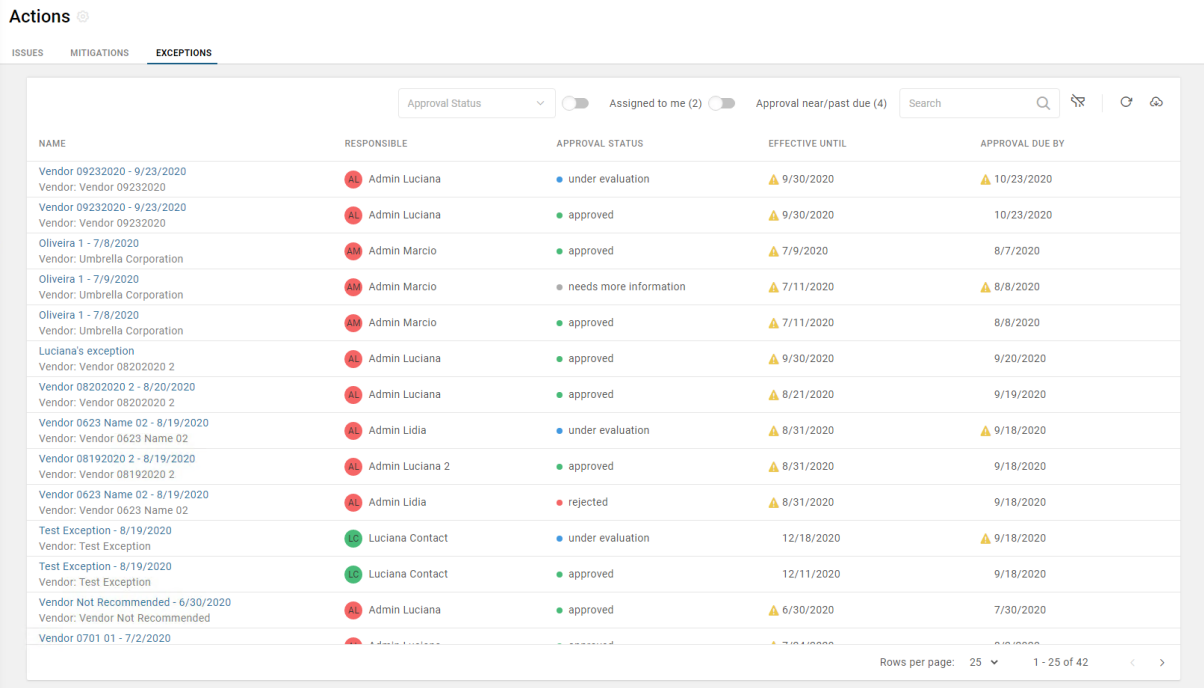


Figure 7: Exceptions Workspace

MANAGEMENT REPORTING

In addition to the various overviews available on SAI360, the solution includes a set of predefined reports, dashboards, and analysis, which provide insights at different levels of the organization. You can slice and dice into specific regions, organizations, classifications, and other filters to drill down into detailed results. Report formats remain the same, but the information displayed is specific for the selected items. Authorizations and permissions set in the application are applicable and synchronized in reports as well. In this chapter, the main reports are introduced.

DASHBOARDS

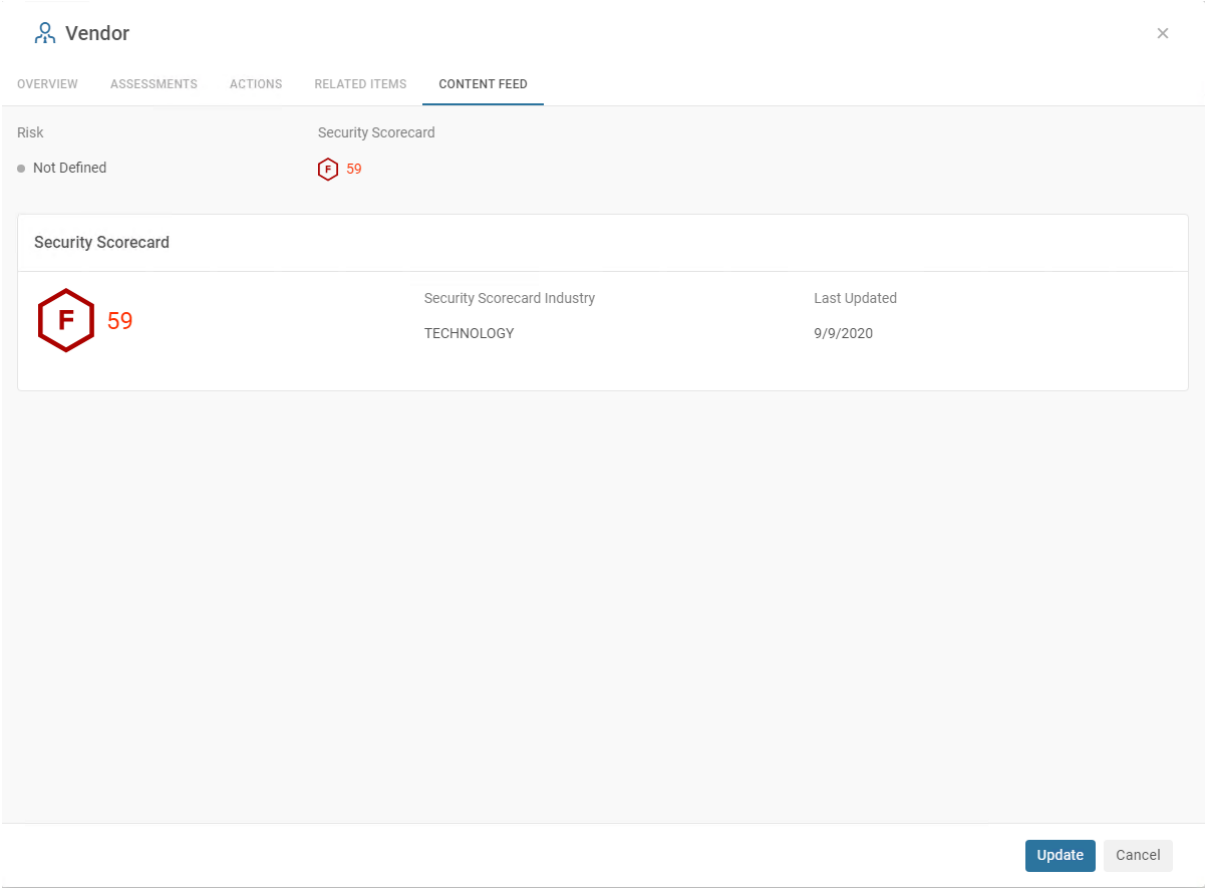
Meaningful information about overall vendor risk management can be used to motivate and inform the organization on a regular basis. As part of the FastStart, dashboards provide useful indicators to manage the VRM cycle, and allow you to track overall vendor risk, drill down into assessment details, and perform a root cause analysis of issues and mitigation actions that need follow up.

OPTIONAL ADD-ONS

FastStart for Vendor Risk Management allows customers to enhance their Vendor Risk Management solution with the following add-ons:

SECURITYSCORECARD

The vendor grade and score are retrieved from SecurityScorecard along with the Industry name, which contributes to ensure a consistent categorization across all your vendors.



VENDOR RISK INTELLIGENCE

While risk management concentrates on remediation activities, risk intelligence focuses on monitoring data generated by these activities to support decision-making and planning of initiatives that enable profitable growth, turn crises into opportunities, and create lasting value.

Additional Risk Intelligence capabilities on SAI360 can be added for an additional fee. The Risk Intelligence allows users to create, edit, and share reports that provide an integrated view of data from SAI360's governance, risk, and compliance processes. These reports use interactive data visualizations from Microsoft's Power BI engine (https://powerbi.microsoft.com/en-us/), which allow metrics to be consolidated and drilled into for increased granularity.

SAI Global provides a number of out-of-the-box reports: Vendor Profile, Vendor Risk Assessments, Issues and Mitigations, and an Advanced Blank Report template with custom visualizations. Each report groups multiple views into a customizable and shareable template.

For example, you can view physical security threats plotted on a map alongside the respective

risk scores of your vendors to help predict how each vendor may be impacted by these threats. Another report view, as the one in the image below, gives you an interactive dashboard with a geographical representation of the organizational elements that are most prone to IT vulnerability breaches, as well as other relevant metrics. These are just a few examples of the visualization possibilities available.

Figure 8: Vendor Risk Management Summary Report

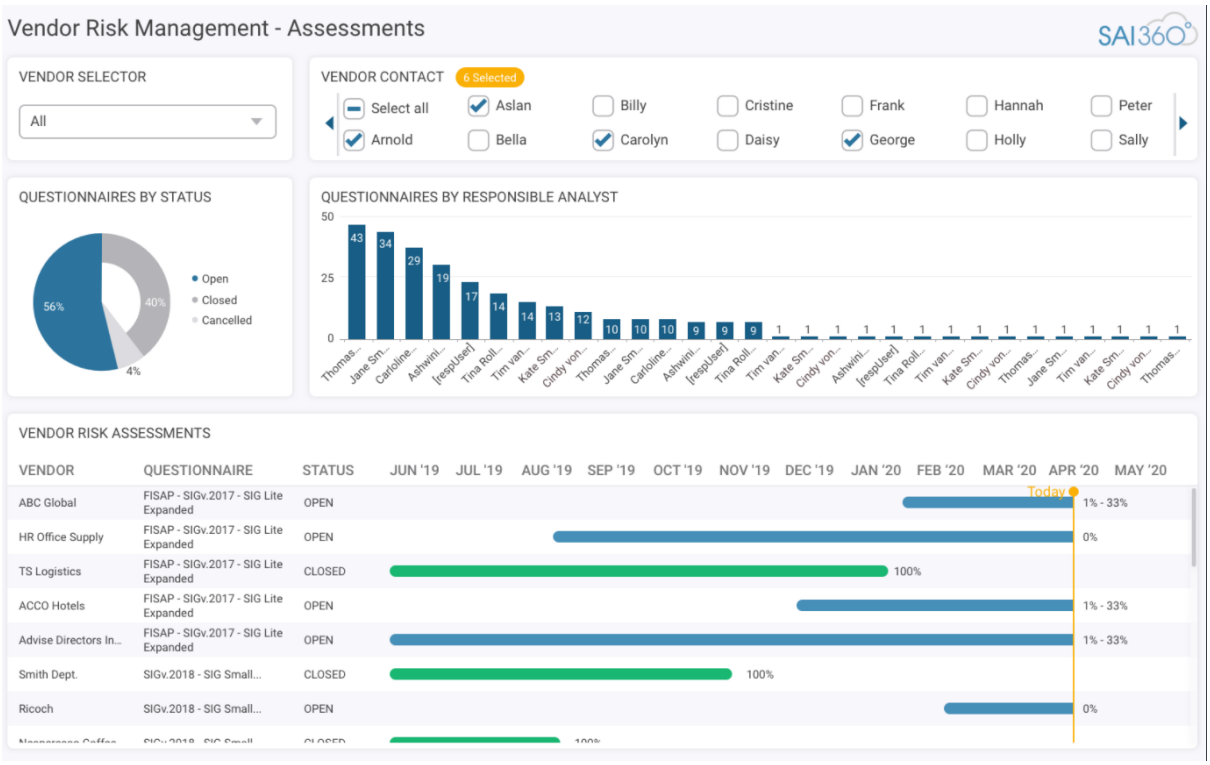


Figure 9: Vendor Risk Assessment Report

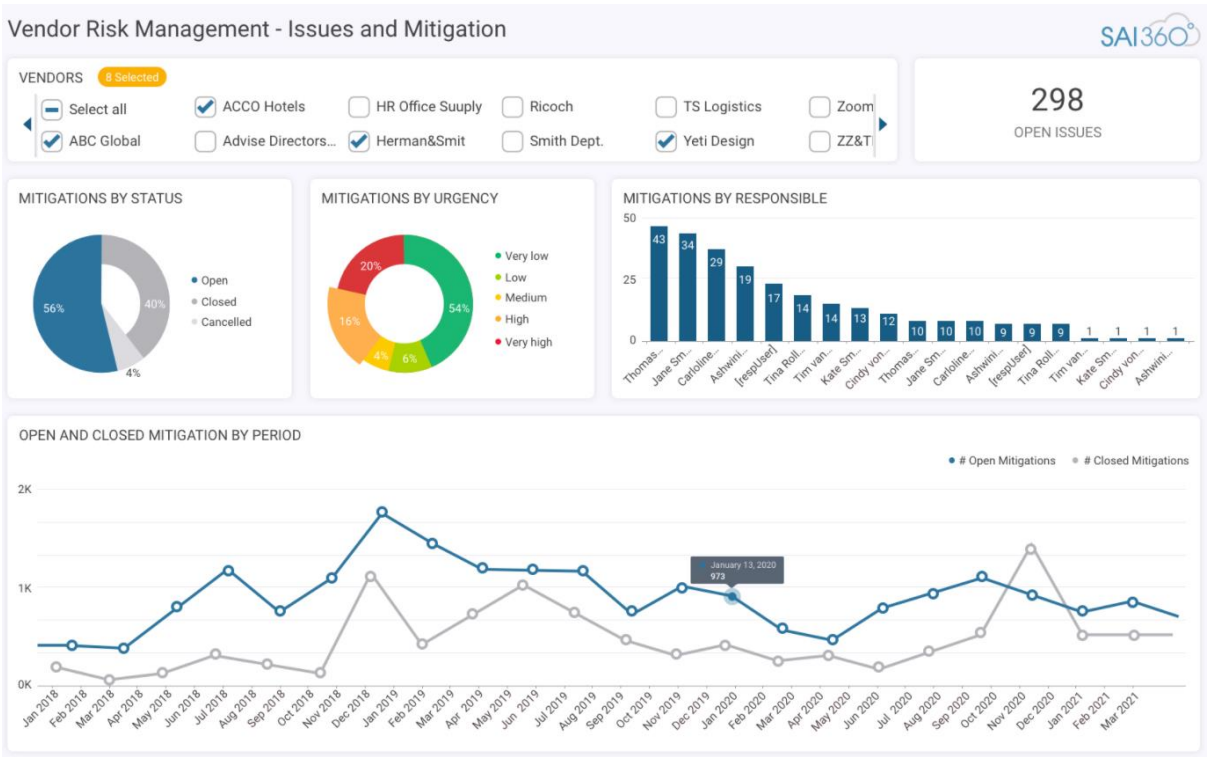


Figure 10: Vendor Issues and Mitigations Report

Several risk intelligence reports are provided out-of-the-box with SAI360:

- Risk Management Overview: to summarize the risk for a vendor and to consolidate the risk results at the business level, which can be easily shared with leadership.
- Risk Assessment: to communicate an overview of the risk assessments undertaken by the organization, grouped by status, duration, and completion level, as well as detail the progress of the questionnaires used to answer controls.
- Issues and Mitigations: to present risk results at the individual vendor level, to be used as the basis for the decision-making process with respect to risk acceptance or action plans to remedy the findings.
- These default reports can be copied and then customized as needed, and custom reports can also be created from scratch. You can also import reports from Power BI Desktop (.pbix) files, allowing you to enjoy more advanced Power BI features that include adding images to your reports.