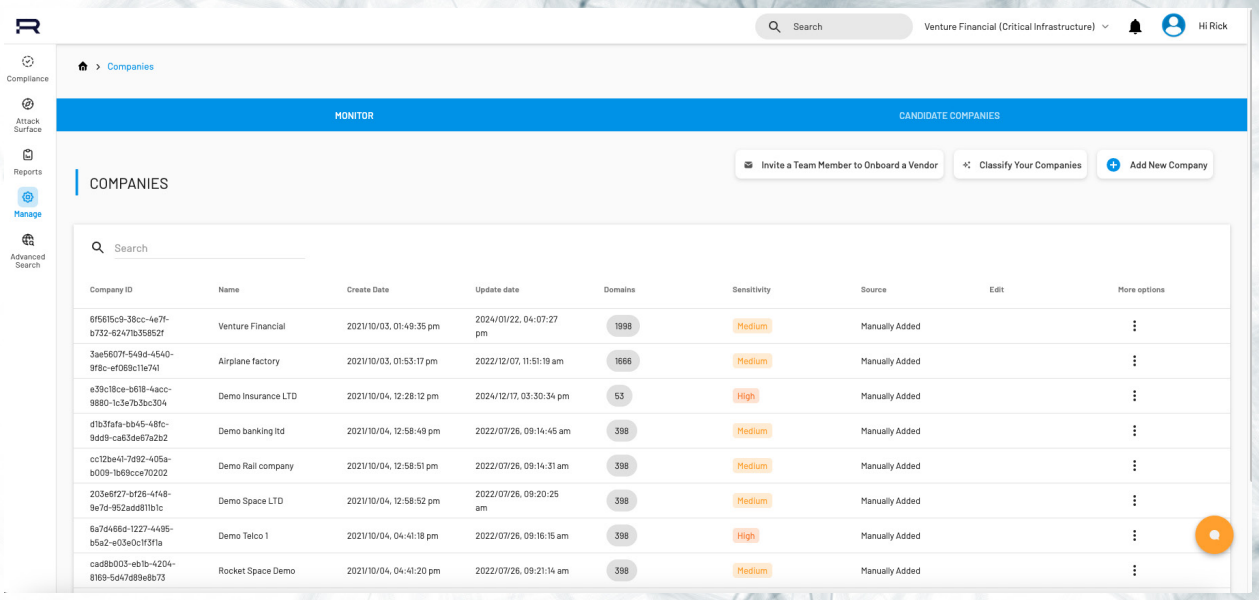
Autonomous Vendor Risk Management Datasheet

Rescana empowers vendor risk managers to work smarter, faster, and at greater scale by combining intelligent automation with comprehensive risk oversight.

Overview



Rescana is an enterprise-grade third-party risk management platform that leverages agentic AI (autonomous software agents) to streamline and enhance every phase of vendor risk management. From automatically discovering and classifying your vendors to conducting risk assessments and driving remediation, Rescana's swarm of AI agents works collaboratively to reduce manual effort and improve accuracy. Vendor risk teams can define their policies in natural language and let Rescana autonomously execute the rest - ensuring that risk assessments are completed faster, more consistently, and with deeper insights than ever before.

Vendor Discovery & Classification

- **Automated Vendor Discovery:** Identify and inventory all vendors across your organization, including third-party and fourth-party suppliers that may be hidden in your

supply chain. Rescana continuously scans internal systems and open-source intelligence (OSINT) sources to automatically uncover vendors, even those without a direct web presence . This comprehensive discovery ensures no vendor is overlooked.

- **Intelligent Classification:** Use AI-driven analysis and natural language-defined policies to classify each vendor by criticality, industry sector, and compliance requirements . Rescana prioritizes vendors based on inherent risk factors (e.g. access to sensitive data or systems) so you can focus on high-risk suppliers first. Integration with procurement data guarantees vendors are accurately categorized from the start .

Asset Classification & Prioritization

- **Critical Asset Mapping:** Go beyond vendor lists by identifying the specific assets or data each vendor interacts with. Rescana's AI maps out which systems, data types, and business processes are tied to each vendor, helping determine the impact of a vendor on your organization's risk profile.
- **Risk-Informed Prioritization:** Automatically adjust risk scoring and assessment depth based on asset criticality. If a vendor handles confidential customer data or mission-critical services, Rescana will flag it for deeper scrutiny and more frequent monitoring. This asset-driven context ensures that the most impactful vendor risks are addressed first, improving the prioritization of remediation efforts.

Configurable AI Agent Swarm

- **Agentic AI Automation:** Rescana deploys a swarm of specialized AI agents, each tasked with different parts of the vendor risk process. These agents can research OSINT data, fill out questionnaires, validate evidence, scan for vulnerabilities, and even communicate with vendors - all working in concert. This isn't basic script automation; the agents reason through tasks (for example, correlating questionnaire answers with evidence) and adapt their actions based on context .

- **Natural Language Direction:** Vendor risk managers can direct the AI agents using simple natural language commands and high-level policies. Instead of complex configurations, you can tell Rescana what goals or standards to achieve (e.g. "Ensure all critical vendors comply with GDPR and our security policy") and the AI swarm will interpret and execute those instructions. The system learns your requirements over time (via "Vega," Rescana's AI engine) and follows your policies with minimal training .

- **Transparent and Configurable:** Each AI agent's actions and decision logic are transparent to the user. You can review how an agent reached a conclusion and adjust

parameters as needed. The swarm is fully configurable - enable or disable certain agents, set their operating boundaries, or insert manual checkpoints to maintain the level of control you need.

Autonomous Operations with Human-in-the-Loop Control

- **Fully Autonomous Mode:** Rescana can run in a *hands-off autonomous mode*, handling the entire third-party risk management workflow end-to-end. In this mode, the platform will automatically discover new vendors, send out assessments, perform scans, evaluate responses, and follow up on issues without requiring human intervention . This dramatically reduces administrative overhead and keeps the process moving continuously, even outside of business hours.
- **Configurable Human Oversight:** You remain in control - Rescana allows **human-in-the-loop** configuration at any stage. You can require human approval before certain actions (such as sending a final risk report to a vendor or escalating an issue) or have an analyst review AI-generated findings before they are finalized. This ensures critical decisions are vetted by experts while routine tasks are fully automated.
- **Autonomous Escalation & Follow-Up:** Leverage AI agents that don't just send one-off emails, but persistently "nag" vendors and escalate issues until they are resolved. If a vendor is unresponsive or misses a deadline, Rescana's agents will automatically follow up with reminder communications. They can even identify alternate points of contact through public sources if the primary contact is unavailable, ensuring that remediation efforts aren't stuck waiting on a human response.

Robust Questionnaire Management

- **Flexible Questionnaires:** Streamline due diligence with a powerful questionnaire engine. Rescana supports all question types - multiple-choice, yes/no, free-text, file uploads, and more - enabling you to cover technical, procedural, and compliance queries in one assessment. You can design nested conditional logic that adjusts questions based on previous answers (for example, if a vendor indicates they have ISO 27001 certification, follow-up questions about their ISMS appear automatically).
- **AI-Assisted Response Filling:** Make it easier for vendors to complete questionnaires accurately. Rescana's platform provides AI assistance that can suggest or auto-fill answers by extracting information from the vendor's documentation . Vendors can simply upload policies, certifications, or audit reports, and the AI will parse these to answer relevant questions - reducing effort on the vendor side and speeding up response time.

- **Template Library & Custom Forms:** Leverage a comprehensive library of pre-built questionnaires aligned with common standards and regulations (ISO 27001, NIST CSF, SIG, etc.), or import your own question sets . Rescana's form engine is highly customizable - you can tweak scoring for individual questions, add explanatory guidance, or modify wording to fit your organization's tone. The platform can accommodate any existing questionnaire format, preserving your legacy vendor assessments within the new system.
- **Multiple Formats per Vendor Type:** Tailor assessments to different types of vendors with ease. Rescana allows you to maintain multiple questionnaire templates and automatically assigns the right one based on vendor categorization. For example, a cloud service provider can receive a detailed cloud security questionnaire, while a marketing agency gets a privacy-focused assessment. This ensures relevance and avoids burdening vendors with non-applicable questions .

Case Management & Automated Workflows

- **Integrated Case Tracking:** Manage the full lifecycle of vendor assessments and remediation tasks in one place. Whenever a risk is detected - whether from a questionnaire answer, scan result, or OSINT finding - Rescana creates a case record and logs all related information and communications. This provides an audit trail and a single source of truth for each vendor's risk status.
- **Automated Vendor Communication:** Eliminate tedious back-and-forth emails. Rescana's AI agents automatically handle routine outreach to vendors, sending assessment invitations, reminders, and escalation notices as needed . You no longer need a separate ticketing system or manual email follow-ups - the platform ensures vendors are kept on track with minimal human effort.
- **AI-Powered Q&A with Vendors:** Rescana not only sends questionnaires but also helps vendors understand and resolve requirements. The AI agents can answer vendors' clarifying questions about the assessment or required evidence (acting as a virtual analyst), using your provided guidelines and policy information . This interactive support means vendors get instant answers to common queries, accelerating the overall process and reducing confusion.
- **Persistent Follow-Up & Escalation:** If vendors fail to respond or if identified risks remain unresolved past due dates, Rescana will automatically escalate the case. The system sends polite but persistent follow-up messages and can notify internal stakeholders if a vendor remains non-compliant. These autonomous follow-ups ensure nothing falls through the cracks - outstanding issues are continually chased until completion.

- **Workflow Customization:** Adapt the process to your organization's needs. Insert manual review steps (e.g. require risk team approval before sending a remediation plan to a vendor), set SLA deadlines for vendor responses, and configure escalation paths (for instance, automatically notify a supervisor or create a ticket in your ITSM system if a high-risk issue isn't addressed in X days). Rescana's workflow engine is fully configurable, so you maintain governance over the process while still benefiting from end-to-end automation.

Transparent Risk Scoring & Analytics

- **Customizable Scoring Algorithm:** Benefit from a transparent risk scoring mechanism that you can tailor to your risk appetite. Rescana computes a risk score for each vendor by evaluating multiple factors - questionnaire responses, evidence quality, scan results, incident history, and more - with each factor weighted according to your preferences . You can adjust these weightings (for example, placing more emphasis on security questionnaire results vs. external scan findings) to align with your organization's priorities and regulatory requirements.

- **Balanced Quantitative & Qualitative Inputs:** The platform intelligently blends qualitative questionnaire data with quantitative technical scan data to form a holistic view of vendor risk. Instead of relying solely on self-reported answers or only on external scanning, Rescana combines both, yielding a balanced score that reflects both compliance posture and actual security indicators. Users can fine-tune how much each component contributes to the score, ensuring neither aspect is undervalued.

- **Continuous Risk Assessment:** Rescana continuously reassesses vendor risk levels over time. Through scheduled scans, ongoing monitoring of OSINT feeds, and periodic questionnaire refreshes, the platform updates vendor risk scores in real time whenever new information arises . This continuous assessment ensures you are immediately aware of changes - such as a new vulnerability on a vendor's system or a lapse in their compliance - rather than waiting for the next annual review.

- **Advanced AI Risk Analysis:** An advanced risk assessment agent correlates data from all sources to uncover deeper insights. For example, it can cross-verify a vendor's questionnaire answers against external intelligence (if a vendor claims data is encrypted at rest, but public breach data suggests otherwise, the AI flags a discrepancy). It analyzes trends and inconsistencies across questionnaire and scan data, and can automatically highlight high-risk issues or contradictions that warrant attention . The AI generates narrative explanations for each risk finding, so you can easily understand *why* a vendor was rated high or low risk and communicate those insights to stakeholders.

- **Executive Summary Reporting:** With one click, generate executive-level summaries of your vendor risk landscape. Rescana's AI produces concise reports highlighting key

findings, notable risks, and remediation status for top vendors. These summaries translate technical details into business terms, allowing you to brief senior management or regulators on third-party risk in a clear, actionable manner. Report content is continuously updated as new assessments are completed, ensuring your dashboard and summaries are always current.

Active & Multi-Layered Scanning

- **Active Vulnerability Scanning:** Augment questionnaires with direct verification through active testing. Rescana can perform authorized security scans on vendor-provided assets - for example, scanning a vendor's web application or cloud infrastructure for known vulnerabilities and misconfigurations. This active scanning capability uncovers issues that questionnaires alone might miss, providing an extra layer of assurance in the risk evaluation.
- **External Attack Surface Monitoring:** Using techniques from External Attack Surface Management (EASM), Rescana maps each vendor's internet-facing presence to discover domains, subdomains, IP addresses, cloud services, and other assets that could pose risk . The platform continuously monitors these assets for changes or new exposures (like an open port or an expired certificate) and ties any findings back to the vendor's profile for evaluation. This ensures you stay informed of emerging threats in your vendors' environments.
- **Multi-Layer Validation:** Rescana employs a multi-layered approach to validate potential issues, drastically reducing false positives. AI "collector" agents gather data from multiple sources and cross-correlate findings - for instance, confirming that a detected vulnerability is truly associated with the vendor's systems and not a shared infrastructure - before raising an alert. This context-aware validation means only credible, verified risks are escalated to your team , letting you focus on real threats instead of chasing erroneous findings.
- **Reduced False Positives:** Thanks to intelligent asset attribution and contextual analysis, Rescana reports significantly fewer false positives compared to traditional scanning tools . Every alert includes evidence and confidence indicators, so you can immediately understand why it was flagged. Over time, you can further tune the system's detection rules to align with your environment, virtually eliminating noise from the risk assessment process.

Multi-Tiered Assessments & Tailored Questionnaires

- **Risk-Based Vendor Tiers:** One size doesn't fit all - Rescana supports different assessment levels for different vendor tiers or risk categories. You can define separate workflows for critical vendors vs. low-risk vendors. For example, high-criticality vendors might undergo a full security review (comprehensive questionnaire, active scans, and perhaps an on-site audit), whereas low-risk vendors complete a lightweight self-assessment. The platform automatically applies the appropriate level of rigor based on the vendor's tier, ensuring efficiency without sacrificing thoroughness.
- **Industry-Specific Content:** Rescana comes pre-loaded with questionnaires and checks tailored to various industries and compliance domains. Whether it's a healthcare privacy assessment (HIPAA), a cloud security questionnaire aligned with CSA CAIQ, or a financial due diligence checklist, the system provides templates to get you started. Each template can be customized or expanded, accelerating the setup of vendor assessments that reflect best practices for your sector.
- **ESG and Supplemental Questionnaires:** For organizations that evaluate more than cybersecurity, Rescana also supports Environmental, Social, and Governance (ESG) assessments and other specialized questionnaires. This allows you to manage all vendor-related risk surveys within one platform, giving a 360° view of vendor risk that includes security, privacy, resiliency, ethical considerations, and beyond.

Deployment & Integration Options

- **Dedicated VPC Deployment:** Rescana offers flexible deployment models to meet enterprise security requirements. For customers needing isolation, Rescana can be deployed in a dedicated, isolated Virtual Private Cloud - ensuring that your vendor data and assessment results reside in a segregated environment with no shared resources. This single-tenant option provides greater control over data residency and network access, helping meet strict internal policies.
- **Seamless Integrations:** Rescana easily integrates into your existing GRC and procurement workflows. Pre-built connectors and APIs allow synchronization with procurement systems (to automatically import new vendors), IT service management tools, identity directories, and communication platforms. For example, integrating Rescana with your vendor management or ERP system ensures that newly onboarded vendors trigger an immediate risk assessment, and integration with Slack or email can notify stakeholders of assessment results or vendor issues in real time. This interoperability helps Rescana fit into your organization's processes without disruption.

Regulatory Compliance & Standards Support

- **Built-In Framework Mappings:** Keep your vendor risk assessments aligned with regulatory and industry standards. Rescana includes mappings to all major frameworks and laws - including **GDPR**, **CCPA**, **NIS2**, **ISO 27001**, **NIST 800-53**, **PCI DSS**, and more - so that questionnaires and risk evaluations automatically cover the required controls. You can easily generate reports to demonstrate each vendor's compliance posture with respect to specific regulations, simplifying audits and due diligence checks.
- **Up-to-Date Compliance Content:** As regulations evolve, Rescana updates its content library to reflect the latest requirements. Your vendor assessments remain current with minimal effort. The platform's out-of-the-box questionnaire library covers key standards such as ISO 27001, NIST, GDPR and others , which you can extend or tailor to match your internal control frameworks. This ensures you're always using current best-practice criteria in vendor evaluations.
- **Custom Framework Support:** If your organization uses a proprietary risk framework or has unique compliance needs, Rescana's flexible design allows you to incorporate those as well. You can define custom risk domains, control questions, and scoring schemes, and the system will include them in assessments and reporting. This way, nothing important to your business is left out of the vendor risk review process.

Security & Trust Assurances

- **Enterprise-Grade Security:** Rescana is built with a security-first approach and undergoes regular independent audits. The platform is **SOC 2 Type II** audited, verifying that its security controls and data handling practices meet strict trust criteria. Rescana is also compliant with **ISO/IEC 27001** (information security management) and **ISO/IEC 27018** (protection of personal data in cloud) standards, demonstrating a strong commitment to safeguarding customer data.
- **Data Privacy & Isolation:** All customer data within Rescana is logically isolated and encrypted at rest and in transit. Strict access controls, monitoring, and data retention policies ensure that sensitive vendor information remains confidential. For clients with heightened privacy concerns, deploying Rescana in a dedicated VPC or on-premises environment provides complete control over data location and access. By adhering to data protection best practices and compliance requirements, Rescana gives you confidence that the risk management process itself does not introduce new risks.
- **High Availability & Reliability:** Designed for mission-critical operations, Rescana's architecture is highly available and scalable. The system can handle large volumes of vendors and assessment data, growing with your needs while maintaining performance. Redundant infrastructure and regular backups protect against downtime or data loss, and Rescana's service level agreements ensure you have continuous access to the platform. This reliability means your vendor risk management program can run 24/7

without interruption.

Empower Smarter, Faster, Scalable Vendor Risk Management: With Rescana, your third-party risk management becomes both proactive and efficient. The platform's AI-driven automation dramatically accelerates vendor assessments and reduces manual workload, while its intelligent analysis provides deeper insight into vendor risks. This means your team can manage more vendors in less time (greater scalability), focus on truly important risks by cutting out noise, and respond quickly to emerging issues (faster remediation). Rescana enables vendor risk managers to move beyond checklist compliance and towards a dynamic, continuous risk oversight model - ultimately strengthening your security posture across the supply chain .