







RiskVision Applications

The RiskVision applications are listed in the table below:

ICON	APPLICATION	DESCRIPTION
	Compliance Manager	RiskVision Application enables an organization to effectively manage and measure compliance programs across multiple regulations, standards, and frameworks. It also automates the compliance process through general computer controls (GCC) and questionnaires. The evidence and control results can be automatically collected through connectors or questionnaire results from business users. RiskVision Application enables data classification, ownership configuration, compliance assessment, mitigation, and reporting. It supports popular frameworks, standards, and regulations such as ISO 27002, CIS, HIPAA and PCI, and others. Compliance Manager improves process efficiency and integrity as well as data quality and reliability.
	Enterprise Risk Manager	Enterprise Risk Manager is a comprehensive risk lifecycle management solution. Using Enterprise Risk Manager, a company can identify, assess, and mitigate risk with an appropriate risk treatment plan. Its flexible risk model supports both qualitative and quantitative methodologies, including calculation of inherent risk, current risk, and residual risk within the context of mitigating controls. This application features rich reports and dashboards, as well as easy to use risk assessment tools. It will help your organization understand and monitor its enterprise risk position by providing out-of-the box support for popular risk methodologies, such as COSO, AZ/NZS 4360 and ISO.
	Vendor Risk Manager	Vendor Risk Manager helps organizations audit and manage third-party risks, as mandated by regulations and standards, such as ISO 27001, PCI, and FISMA. This application classifies, assesses, and reports on third-party risk, based on the standard control framework from shared assessment programs, or an organization's custom control framework. Vendor Risk Manager provides a portal where vendors participate in assessments and the results are retrieved by an organization's risk analysts. Vendors are classified automatically into appropriate tiers and

		<p>applicable controls are applied based on the vendor tier. Powerful delegated administration and automation features allow Vendor Risk Manager to scale to large numbers of vendors.</p>
	<p>Threat and Vulnerability Manager</p>	<p>Threat and Vulnerability Manager allows organizations to consolidate their threat and vulnerability programs on a single platform. It integrates vulnerability and early warning data feeds from iDefense and National Vulnerability, and correlates these feeds with vulnerability scanner results to eliminate false positives and report incidents. Inferred scans are performed by correlating the vulnerability data feeds to a company's RiskVision asset database, which mitigates risks for assets not reachable by vulnerability scanners. Once detected, vulnerabilities are assessed and remediated using the system's workflow for true closed-loop vulnerability management.</p>
	<p>Policy Manager</p>	<p>Policy Manager manages enterprise policies on a single centralized platform. Organizations can enforce policy and process standards across different locations, departments, and programs. Policy Manager supports simultaneous policy editing across multiple stakeholders using a rich WYSIWYG user interface. An organization can automate processes for policy authoring, reviewing and approval. Policy templates help enforce consistent formatting and structure. Policy Manager has a highly configurable workflow which allows your organization to enforce change control and maintain accountability. It supports policy awareness campaigns with policy distribution, attestation, and comprehension testing tools.</p>
	<p>Incident Manager</p>	<p>Incident Manager allows organizations to collect, classify, and manage multiple IT and non-IT incidents. It's a single collection point for all manually reported and automatically imported incidents. It imports incidents reported from most monitoring systems and scanners as well as Security Incident Management (SIM) solutions. All incidents, including business, operational, and environmental can be reported in the incident-reporting portal. Incidents are assessed based on a configurable workflow and automatically created and classified based on rules that are tracked throughout the incident's lifecycle. Incidents are tied to controls, policies, and risks to provide closed loop feedback for policy and control</p>

assessment and risk monitoring. Incidents are rated based on the criticality so that organizations can respond based on the impact to the business.