Healthcare Third-Party and Enterprise Risk Management:

A Product Evaluation and Buyer's Guide for Healthcare Leaders and Cyber Risk Practitioners

Table of Contents

Executive Summary

Confronting the New Normal in Cyber Risk Management

As far too many have learned the hard way, the health sector faces an unprecedented reckoning with cyber risk. It's no longer just about preventing data breaches; it's about protecting patient safety. In fact, managing third-party (TPRM) and enterprise risk (ERM) has evolved into managing sector-wide systemic risks that directly threaten both Margin and Mission. Managing cyber risk in healthcare means managing a highly interconnected and interdependent *ecosystem* – consisting of thousands of third-party products and services; extensive fourth-party risk exposures; hundreds of affiliates sharing our IT/EHR; and a tidal wave of AI applications moving closer to the bedside. Moreover, the entire health sector sits precariously atop a few high-impact, single points of failure (such as the Change Healthcare ransomware attack in February 2024 that crippled the sector for months) jeopardizing both balance sheets and people's lives. Within this ever-expanding and evolving ecosystem, how can a healthcare organization begin to identify and understand all these risks — let alone actively manage and mitigate them in a meaningful way?

Choosing the Right Healthcare TPRM Solution

While no organization can ever fully eliminate risk, they can significantly reduce the likelihood of a catastrophic cyberattack with the right solution for managing third-party and enterprise risk. This document helps your organization evaluate TPRM + ERM solutions and identify the unique capabilities that will help you and your team identify, assess, manage, monitor, and mitigate the vast landscape of cyber risk facing healthcare organizations today. The right cyber risk solution delivers a highly scalable, cyber risk program out-of-the-box, rooted in healthcare cybersecurity best practices and powered by process automation and advanced AI to enable your organization to reduce more risk in less time.

Key capabilities to look for in a TPRM + ERM solution include:

- Designed and curated to manage healthcare-specific risks against healthcare-specific standards
- Makes it easy for vendors to fill out security questionnaires in seconds and share them instantly
- Provides end-to-end assessment automation to boost productivity and scale TPRM programs
- Continuously monitors for changes in third-party risk posture and provides breach alerting
- Centralizes TPRM + ERM findings in Risk Register, drives enterprise-wide collaboration on risk
- Seamlessly integrates with existing workflow & ticketing systems and BI/reporting applications
- Optionality for "on-demand" managed services to backfill loss of FTEs, capacity constraints
- Assess enterprise cyber maturity against for recognized security practices (NIST CSF, HICP 2023)
- Assess enterprise compliance against established and emerging regulations (HIPAA, HPH CPGs)
- Assess broader ecosystem risk of affiliated orgs, IRB/research, and AI adoption (NIST AI RMF)

Cyber safety is patient safety – and an effective TPRM solution is critical for rapidly identifying and reducing cyber risk in a consistent, scalable, and affordable way to protect what matters most.

For more information, please visit censinet.com or email info@censinet.com.

Purpose-Built for Healthcare

Problem

The vast majority of third-party risk management (TPRM) tools on the market are built for pan-industry use, and are not designed to manage the unique complexities, challenges, and risks faced in healthcare. As a result, many of the most critical third-party risks are never captured, assessed, or remediated – leaving healthcare organizations exposed to catastrophic cyberattacks through no fault of their own.

Capabilities Required

First and foremost, managing TPRM in healthcare requires a solution designed for healthcare risks (e.g. assessing the risk of medical devices or new clinical AI applications; managing PHI access and myriad BAAs; or understanding the unique risk exposures between affiliated practices and health systems). Moreover, these risks need to be assessed against healthcare-specific standards, regulations, and recognized security practices (e.g. HIPAA, NIST CSF) to maximize risk identification and mitigation.

Why It Matters

Using a solution that is purpose-built for healthcare removes the need for complex configuration prior to implementation while ensuring 100% risk coverage. Most importantly, cyber risk is patient safety risk in healthcare, and the loss of a mission-critical application or service due to a ransomware attack not only disrupts care operations, but jeopardizes patient safety and people's lives.

Capabilities	Benefits	Censinet RiskOps™	Other Tools
Standardized third-party questionnaires	Ensures a more consistent, repeatable, and efficient TPRM process	✔	
Standardized questionnaires based on healthcare standards, regulations, and best practice frameworks (e.g. HIPAA, NIST CST)	Ensures a standards-based approach to risk assessment, mitigation, and reporting	✔	
Continuously curated questionnaires	Ensures assessment of third parties against the most current healthcare risks, threats, regulations, and standards	✔	
Assessments for all third party types	Ensures 100% coverage of all third parties and risk exposures (e.g. Vendors, Products, Services, Non-Tech Suppliers)	✔	

Detailed questionnaires for all product types	Captures appropriate risks for specific types of products or services, driving greater risk visibility and 100% coverage (e.g. on-premise software, SaaS, hardware, medical devices, consulting, etc.)	✔	
Proxy assessments for vendors, products, and services	Allows for independent, confidential assessment (without notifying vendor)	✔	
Clinical data exchange assessments	Dedicated assessment type for exchange of clinical data/PHI between two organizations; ensures HIPAA-compliant information sharing	✔	
Clinical risk SME review	Invite and assign questions to clinicians to assess clinical risk of vendors, products, and medical devices	✔	
Automated MDS2 2013 and MDS2 2019 ingestion, parsing	Helps populate responses in Medical Device assessments and expedite analysis	✔	
Curated CAP findings and corrective actions	CAP findings and recommended actions based on latest healthcare industry standards, regulations, and security frameworks (e.g. HIPAA, NIST CSF) to ensure vendor is compliant, uses best practices	✔	

Network Exchange Model

Problem

Healthcare organizations often struggle with inefficient and fragmented data exchange processes when managing third-party risks. This inefficiency can lead to incomplete assessments, delayed vendor responses, and an inability to scale risk management efforts. Consequently, all sides suffer – vendors are delayed in selling and renewing their products, and healthcare organizations are delayed in deploying mission-critical Health IT or medical devices, and remain vulnerable to emerging threats and risks.

Capabilities Required

An effective network model enables seamless and secure information sharing between healthcare organizations and their third-party vendors. AI and automation should accelerate the risk assessment process on both sides of the network: it should take only seconds for vendors to fill out security questionnaires, while risk assessors must always get the most up-to-date risk data – and get it fast. As such, vendors should "do the work once" and easily share previously-completed questionnaires and risk updates in a single click an unlimited number of times with customers and prospects on the network.

Why It Matters

A network model significantly enhances efficiency, scalability, and real-time risk visibility for TPRM leaders and risk assessors. By streamlining data exchange, it leverages network effects to provide assessing organizations with continuous, up-to-date risk data and evidence from vendors across the network. This interconnected approach establishes a single source of truth and trusted system-of-record for TPRM, delivering comprehensive intelligence on risk posture across the entire third-party portfolio.

Capabilities	**Benefits**	**Censinet RiskOps™**	**Other Tools**
Digital Risk Catalog™ with 14,400+ vendor organizations and 30,200+ products & services	Centralized, digital inventory of all third parties; many with pre-populated data ready for 1-Click Assessment sharing	✔	
1-Click Assessments™	Enables vendors to reuse completed questionnaires and share unlimited number of times with organizations on network, reducing vendor response time to a single click	✔	
Productized best practices for vendors	Best practices for completing questionnaires, expedites vendor response times and accelerates	✔	

	overall assessment completion times		
AI for vendors to complete Censinet questionnaire	Automatically populates responses in Censinet standardized questionnaires using previously-completed questionnaires and source documentation	✔	
AI for vendors to complete any external questionnaire	Automatically populates responses in any non-Censinet questionnaire (e.g. spreadsheets) using previously-completed questionnaires and source documentation; creates incentive for vendors to keep profile current as the “single source of truth” for answering all incoming questionnaires	✔	
1-Click Reassessments	Enables vendors to quickly share security profile with organizations for reassessments instead of filling out a profile from scratch, dramatically increasing the responsiveness for vendors who need to be reevaluated on an annual basis	✔	

Process and Workflow Automation

Problem

Many TPRM programs remain bogged down by manual labor, administrative tasks, and antiquated tools such as spreadsheets. This not only hinders the scalability of risk management efforts, but can delay deployment of mission-critical services. What's more, the procurement process in healthcare often requires collaboration across multiple teams, functions, and business owners – further complicating the ability to deploy new products and services promptly, securely, and safely.

Capabilities Required

The best solution offers a turnkey, best-practice TPRM program "in a box," eliminating the need for extensive configuration during implementation. The solution delivers end-to-end assessment through advanced automation and AI, significantly boosting TPRM productivity and performance. Additionally, it facilitates coordination and collaboration across various teams and stakeholders, streamlining the safe and secure evaluation of new products. This best practice approach to TPRM ensures risk management remains highly scalable, yet flexible and adaptive to the evolving, unique needs of the organization.

Why It Matters

With advanced automation and AI embedded into a TPRM solution, healthcare organizations can immediately stand up a high-performance, best-practice risk management program in just weeks. By unlocking greater scale and speed, TPRM teams can reduce more risk in less time while simultaneously expanding overall risk coverage. Moreover, healthcare leaders and risk assessors can focus exclusively on critical thinking and analysis, rather than being weighed down by administrative burdens.

Capabilities	**Benefits**	**Censinet RiskOps™**	**Other Tools**
Detailed risk assessor dashboard	Shows status of all assessments requested, in-progress, and completed; vendor progress on outstanding questionnaire(s)	✔	
Custom questions easily inserted	Enables risk assessors to ask specific questions not contained in the standardized questionnaires, and keep all risk data in centralized location	✔	
Built-in vendor evidence capture	Ensures vendors provide supporting documentation and evidence when completing standardized questionnaires	✔	

Technical integration data capture	Capture all integration and implementation details (e.g. network access, PHI) to enhance analysis and assessment of risks introduced into IT environment	✔	
Automated Corrective Action Plans (CAPs)	Auto-generates assessment findings and recommended corrective actions based on questionnaire responses, expediting risk analysis	✔	
Assign questionnaire responses, findings to Subject Matter Experts (SMEs) for review	SMEs provide recommended findings and actions; facilities enterprise-wide collaboration to reduce risk with all stakeholders (e.g. Legal, Procurement)	✔	
SME task management & workflow	Shows status and progress for assigned questions and findings, allows ability to reassign tasks; Provides total visibility into assessment/CAP status	✔	
In-platform CAP negotiation and asynchronous commenting with vendor	Eliminates need for myriad emails to negotiate CAP; tracks all outstanding actions; activity log provides full audit trail	✔	
Risk Tiering	Assigned by risk assessors to vendors/products based on business impact of disruption or downtime (e.g. Critical, High)	✔	
Tier-based Automated CAP Findings	CAPs auto-generate more appropriate findings based on vendor/product risk tiers (e.g. “mission-critical vendors must have 24/7 on-call support”)	✔	
Custom Automated CAP Findings	Enables risk assessors to create custom, tier-based automated findings	✔	

Custom Policy-Based CAP Findings	Enables risk assessors to create custom findings based on organizational policies, risk tolerances, or required contractual language	✔	
Automated reassessment scheduling	Reassessments automatically scheduled and requests sent to vendors based on assigned vendor/product risk tiers – timing is customizable by the customer	✔	
“Track changes” reassessment logic	Auto-compares current vendor security profile to the last assessment performed, highlighting key changes that impact risk; creates greater focus, efficiency for assessors	✔	
Auto-generated Risk Summary Reports	Summarizes all information captured during assessment, (e.g. risk scores, CAP status); enables risk assessors to spend time on critical thinking, analysis – not manual reporting writing	✔	
Managerial review/approval workflow	Automated routing for risk leaders to review, approve assessments (or ask for more information before sign off)	✔	

Continuous Monitoring & Analysis

Problem

Vendors can rapidly undergo changes in their risk posture due to many factors such as growth, new product launches, and updated controls. Most TPRM tools fail to provide real-time insights into these changes, leaving healthcare organizations essentially blind to how third-party risk is changing over time, and, more critically, delaying response and recovery when a third-party incident occurs.

Capabilities Required

A TPRM solution's monitoring capabilities must deliver real-time visibility into the evolving risk posture of third-party vendors and their distinct products and services. This requires advanced automation and risk scoring to track and assess changes as they occur as well as breach & ransomware alerts for the mission-critical services in your third-party portfolio and on the frontlines of care delivery. Additionally, it should support comprehensive reporting and trend analysis to inform strategic decision-making with the Board and enhance overall TPRM performance.

Why It Matters

Continuous risk monitoring not only enhances visibility into changes in third-party risk posture but also enables faster response and recovery during security incidents. Early intervention can limit the impact of both third-party and internal cyberattacks and reduce the risk of prolonged disruptions to care delivery.

Capabilities	**Benefits**	**Censinet RiskOps™**	**Other Tools**
Breach & ransomware alerts	Delivers breach & ransomware alerts for the vendors/products currently in third-party portfolio, expediting response, recovery	✔	
Longitudinal risk records for third parties	Centralizes all risk data and evidence, risk scores, CAPs, and assessment history; facilitates monitoring for changes in risk posture over contract lifecycle	✔	
Censinet Risk Ratings	Dynamic, automated risk scoring for vendors/products based on questionnaire responses and supporting evidence	✔	
Security Scan Ratings	"Outside-in" perimeter risk scoring for each vendor and	✔	

	product in third-party portfolio		
Inherent Risk Ratings	Vendor/product's risk to org in absence of direct actions taken to mitigate; defaults to Censinet Risk Rating, but can be manually updated by risk assessor	✔	
Residual Risk Ratings - vendors & products	Risk remaining for each vendor and product after actions taken; set by risk assessors	✔	
Residual Risk Ratings - third-party portfolio	Aggregated risk score for entire third-party portfolio	✔	
Dashboards with actionable insight	Conveys overall risk posture, including TPRM program performance, overdue CAPs, missing BAAs, total products and medical devices assessed, portfolio residual risk, and 4th-party risks; drill down into risk drivers for deeper analysis	✔	
Smart filters for portfolio analysis	Quickly find targeted information across the third-party portfolio (e.g. Which vendors/products have open findings, de-identified PHI, or offshore data access?)	✔	
Alerts for "Missing BAA"	Alerts assessors if no BAA is found for vendors or products, a critical open risk item that requires immediate attention	✔	
PHI Flagging	Risk assessors able to tag if vendors or product accesses, stores, and/or transmits PHI	✔	

Risk Register

Problem

With over 2,000 third-party vendors and products at a typical healthcare organization, managing a comprehensive set of risk assessment findings and recommended remediations across the entire third-party portfolio is extremely challenging. With many healthcare organizations still relying on spreadsheets to manually aggregate, assign, and close out all open risk items, critical issues may linger unresolved for years, exponentially increasing the organization's cyber risk exposure.

Capabilities Required

A best-in-class TPRM solution includes a Risk Register that captures all third-party and enterprise assessment findings in a highly-automated, centralized repository. This Risk Register enhances enterprise-wide coordination, collaboration, and accountability by enabling the assignment of open risk items to the appropriate stakeholders. Advanced features such as real-time updates, status tracking and task management, and a Risk Register Dashboard help prioritize and expedite risk management efforts.

Why It Matters

An automated Risk Register is critical for healthcare organizations to effectively track and manage all third-party and enterprise risks – ensuring that all assessment findings are reviewed by the right person at the right time and addressed promptly. By centralizing risk data and automating organization-wide collaboration, a Risk Register helps ensure rigorous, continuous, and comprehensive risk reduction.

Capabilities	**Benefits**	**Censinet RiskOps™**	**Other Tools**
Risk Register	Automatically captures all TPRM + ERM assessment findings and recommended actions in a centralized location, enabling enterprise-wide collaboration on cyber risk reduction	✔	
Risk Register with Findings Lifecycle Mgmt.	Ensures timely disposition of open risk items; Facilitates task management, coordination and accountability across all risk stakeholders;	✔	
Risk Register Dashboard	Summarizes cyber risk posture in real-time, surfaces highest risk concentrations, and prioritizes highest-risk vendors/products	✔	

Ecosystem Integration

Problem

Introducing a new solution often entails significant challenges in aligning with existing processes and business operations. Disjointed systems and workflows can lead to inefficiencies, data silos, and poor collaboration, making it difficult to achieve a unified approach to risk management. Ultimately, this can impede an organization's ability to respond effectively to emerging cyber risks and threats.

Capabilities Required

A new TPRM solution must fit into an organization's existing processes, systems, and operations. This includes the ability for business owners to request risk assessments for new products and services while, at the same time, enabling risk assessors to perform assessments with a clear understanding of intended use cases and potential risks. Furthermore, a TPRM solution should integrate seamlessly into current ticketing and workflow systems, like ServiceNow, and deliver actionable risk insights into preferred BI applications, existing GRC systems, and custom reporting tools.

Why It Matters

Seamless ecosystem integration maximizes the effectiveness and efficiency of a new TPRM solution by creating a unified approach to risk management without operational disruption, frustration, or distrust.

Capabilities	**Benefits**	**Censinet RiskOps™**	**Other Tools**
Business Owner Intake	Allows business owners to request a risk assessment with key third party information, enabling risk assessors to perform assessment with better understanding of intended use, potential risks	✔	
ServiceNow Workflow Connector	Enables TPRM process to integrate into current ticketing & workflow systems, allowing users to request assessments, track progress; risk assessors provide updates as needed	✔	
Open API	Enables customers to pull risk assessment data and insights into preferred BI applications, GRC systems, custom reporting	✔	

	and business analytics tools		
On-Demand Provisioning	When single sign-on (SSO) is used, On-Demand Provisioning enables admins to automatically provision accounts for any users (e.g. Business Owners) in Identity Provider directory, following the principle of least privilege (PoLP)	✔	

TPRM Program Benchmarking

Problem

Healthcare CIOs and CISOs often face significant challenges when requesting budget increases from leadership and the Board. Without a clear understanding of their TPRM program's maturity and performance, it becomes difficult to demonstrate the need for additional resources or justify investment.

Capabilities Required

Benchmarking enables CISOs to assess the maturity of their own TPRM programs objectively and compare their performance against industry peers. Assessing programs against gold-standard frameworks like NIST CSF reveals critical gaps in TPRM practices and identifies where additional resources and investments are needed to meet or exceed industry and peer standards. In addition, the benchmarking solution should generate intuitive, non-technical reports that help CIOs and CISOs articulate the value and necessity of cybersecurity investments to the Board.

Why It Matters

Benchmarking is essential for CIOs and CISOs to help validate the need and effectiveness of a TPRM program, secure the necessary funding to address gaps, and enhance overall program performance.

Capabilities	**Benefits**	**Censinet RiskOps™**	**Other Tools**
Peer Benchmarking for TPRM program	Compare TPRM program maturity to peer organizations using industry recognized security practices (e.g. NIST CSF)	✔	
Automated Action Plans	Use Automated Action Plans to identify and close critical gaps in TPRM program controls, policies, and procedures	✔	
Benchmarking Reporting	Use intuitive reports to allocate resources and justify investment to the Board to improve TPRM program maturity, performance	✔	

Comprehensive Services & Support

Problem

Most TPRM tools take too long to implement due to excess configuration and inadequate upfront training and support; as such, time-to-value is often measured in months. Moreover, once up and running, TPRM teams often face unexpected challenges such as capacity constraints, FTE churn, and budget shortages. These issues can severely limit the effectiveness of the TPRM team and the broader cybersecurity program, and lead to dangerous gaps in risk coverage or delayed incident response.

Capabilities Required

A top-tier TPRM solution must provide comprehensive services and support that extend beyond the software itself. This includes offering managed services "on-demand" to fully backfill any sudden capacity constraints or a loss in resources – ensuring that the TPRM program remains fully operational, efficient, and effective. The solution should also provide expert ongoing guidance, training, and support to ensure long-term success. Lastly, the best TRPM solutions let customers drive product innovation with a roadmap that solves for the specific problems and challenges they face every day.

Why It Matters

Dedicated services and support maximize the time-to-value of new solutions and strengthen the effectiveness of their TPRM team and the maturity of their overall enterprise cybersecurity program.

Capabilities	**Benefits**	**Censinet RiskOps™**	**Other Tools**
On-Demand TPRM Managed Services	Option to outsource all or a portion of risk assessments, in case of capacity constraints or loss of FTEs, with no trade-off in assessment speed, coverage, or risk mitigation	✔	
Dedicated Customer Success team	Ensures faster time-to-value with hands-on training, ongoing support, innovation partnership; customers perform first risk assessment during onboarding	✔	
Flat license fee	Incentivizes organizations to perform an unlimited number of assessments for 100% coverage	✔	

Enterprise Risk Management (ERM) & Benchmarking

Problem

As cyberattacks continue to escalate across the industry, healthcare leaders are under increasing pressure to strengthen their organization's cyber preparedness and resiliency. However, healthcare CIOs and CISOs often face significant challenges securing budget increases or investment. Without a precise and detailed understanding of their cybersecurity program's maturity, it becomes difficult to justify the need for investment and deploy those resources to the most under-developed, immature areas.

Capabilities Required

A comprehensive enterprise risk management (ERM) solution enables healthcare organizations to assess the maturity of their cybersecurity programs, benchmarking performance against peers, target areas for improvement, and secure investment from the Board. The solution should enable leaders to measure program maturity and compliance against a comprehensive set of healthcare standards – including regulations and emerging mandates (e.g. HIPAA, HPH CPGs) as well as recognized security practices and frameworks (e.g. NIST CSF 2.0, HICP 2023, NIST AI RMF). Additionally, the ERM solution should support assessment of the ever-expanding healthcare ecosystem, including affiliates, physician practices sharing IT/EHR infrastructure, research and clinical trials, and artificial intelligence. The solution should generate recommended remediations, integrate seamlessly with the Risk Register, and enable assessment findings to be routed to appropriate subject matter experts for review, tracking, and timely closure.

Why It Matters

With comprehensive enterprise assessment and peer benchmarking, CIOs and CISOs can allocate resources and investment to significantly strengthen cyber preparedness and resiliency. Moreover, objective, data-driven ERM reporting not only enables CIOs and CISOs to effectively communicate the value and necessity of cybersecurity to the Board but also facilitates their conversations with cyber insurers, helping to contain premium cost growth and demonstrating a lower risk profile.

Capabilities	**Benefits**	**Censinet RiskOps™**	**Other Tools**
Enterprise Assessments - Industry Standards and Security Frameworks	For recognized security practices and best practice frameworks: - NIST CSF 1.1 / 2.0 - HICP 2023 - HPH CPGs - NIST AI RMF - HIPAA Security & Privacy	✔	
Enterprise Assessments - Expanded Ecosystem	Enterprise assessments for: - Affiliate organizations - Affiliates connected to	✔	

	organization's network - IRB/research & trials		
Enterprise-Wide Questionnaire Routing	CISOs can assign selected questions to internal SMEs and stakeholders to enrich responses, expedite completion of enterprise assessments	✔	
Automated Action Plans	Auto-generated ERM findings and recommended actions rapidly identifies critical gaps in controls against industry standards, accelerates closure	✔	
Peer Benchmarking	Cybersecurity benchmarks for: - NIST CSF 2.0 - HPH CPGs - Organizational Metrics - NIST AI RMF - HICP 2023	✔	
AI for risk assessors to complete any external questionnaire	Automatically populates responses in external questionnaires (e.g. insurance forms) using completed ERM assessment questionnaires	✔	