

Technology Risk Manager (TRM) - Data Sheet

Technology Risk Manager (TRM) provides instrumentation, via predictive analytics, that enable senior managers to quantitatively measure IT Risks to information. TRM factors both technology data and compliance data to illuminate where risk lies and what to do about it.

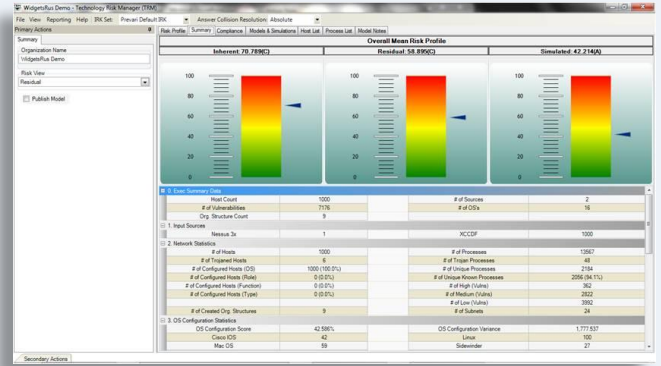
TRM is a risk calculation engine that determines the probability of compromise. TRM provides organizations with actionable metrics that specifically determine how resilient the organization is to both known vulnerabilities, and more importantly, unknown threats & vulnerabilities.

TRM's results are presented as the Prevari Risk Index in a dashboard that supports drill down to specific device details. Risk Indices directly support the concept of "Framing Risk" as required by all major risk management frameworks. Compliance with the most widely used regulations and standards for information security is factored into the calculations as well (see CRM data sheet for details).

For senior management, TRM uses inferential statistics to establish a mean, standard deviation and variance in the risk profile of a system, a location, a business unit, or the entire network.

For security technologists, the modeling interface presents a complete view of the environment including controls deployed and rigorous machine-level detail. Sortable risk-ranked host and process lists enable analysis and identification of quick hit opportunities for risk reduction. Anomalous outliers are easily identified

Managers have the metrics needed to make both strategic and tactical business decisions to improve security and manage risk - metrics that are objective, quantitative, repeatable, and defensible. TRM directly answers the question, **"If you have \$1 to spend on security and compliance, where should you spend that \$1 and why?"**



TRM operates on the risk-relevant data already being collected by your organization's scanners, sensors, security technologies, and audit & compliance teams.

Inherent Risk— With nothing more than a security scan containing network port, service, protocol and vulnerability data, TRM immediately calculates Inherent Risk. Inherent Risk is risk you incur just operating the technologies required to run your business.

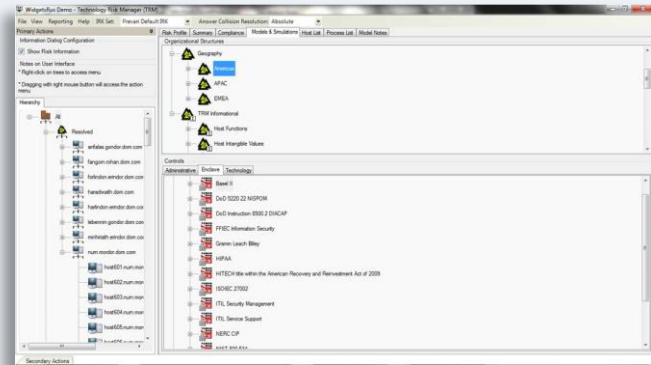
Control Impact - TRM is unique in the industry with the capability to factor both technology controls as well as administrative controls (processes and procedures). Leveraging Network Frontiers' Unified Compliance Framework, TRM includes detailed mappings of process and procedure controls directly into the Risk Index calculations.

Technology controls (single sign-on, two-factor authentication, encryption, etc...) are layered into a TRM model via GUI and risk indices are further refined by modeling additions, deletions, or modifications to technology controls, administrative controls, hosts, and processes deployed.

Residual Risk = Inherent Risk—Control Impact

Residual Risk indices provide a comprehensive, proactive view of your technology environment's information risk presented in over one-hundred graphs, charts, and tables.

Organizational Structures - TRM provides unlimited nested organizational structures to ensure your models have the greatest utility (business unit, geography, compliance standard, business process, application owner, device type, etc...). Prevari Risk Indices are determined for each, enabling business owners to understand specific risk for their portfolio of responsibility.

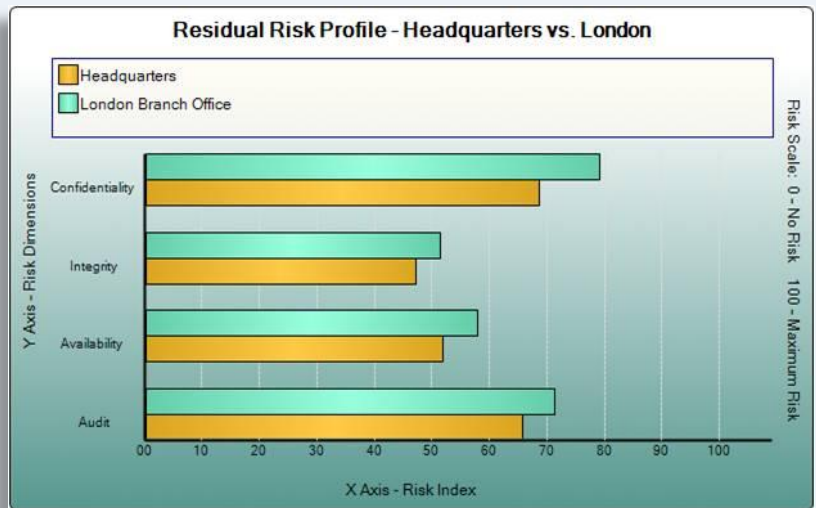


Technology Risk Manager (TRM) - Data Sheet

Answer the hard questions

Using simulations and comparisons, TRM provides answers to the most difficult questions:

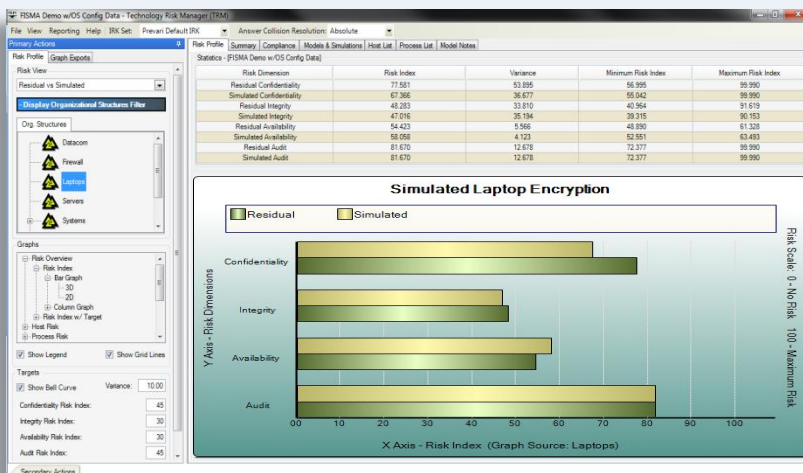
- How secure is my organization?
- How has risk to information changed over time?
- How do we compare? - business units, networks, peers.
- How will this new system or control impact risk?
- How does that product or software impact the risk of the existing systems and networks?
- How do we spend our limited security/compliance resources for maximum risk reduction?
- How resilient are we against cyber threats, mis-configuration, and environmental effects?



Simulations and Comparisons

TRM provides simulations to identify the specific risk impact of adding or removing controls. To understand the risk reduction value of encrypting all your data, just ask TRM. Simulations can be performed for both technology controls and administrative controls (compliance controls) as well as for other new technologies or applications prior to implementation. Simulations are a remarkably powerful solution to help one determine how to best manage information risk before spending on people, process or technology.

Comparisons are created to conduct trend analysis or to compare geography, business units, business processes, or device types.



TRM Technical Specifications

TRM is a client-server application using Microsoft® technologies including the Microsoft .NET framework. It operates on Microsoft SQL Server® 2005 or 2008 and can be operated in a one, two or three-tiered architecture and employs encryption between the client and server. Supported Microsoft Windows® operating systems include: XP Pro®, Server 2003® and 2008, Vista®, Windows® 7. TRM requires Microsoft Word® 2003, 2007, or 2010 and one of the following web browsers: Internet Explorer®, Firefox®, or Safari®.