Risk Calculation and Predictive Analytics:
Optimizing Governance, Risk and Compliance.

Prevari makes organizations safer by providing instrumentation for managing risks to information. Prevari solutions improve productivity, information system resilience, and organizational effectiveness through objective, quantitative measurement and predictive analytics. Prevari metrics enable decisions and activities to continuously enhance information security, compliance, and information risk management.
Overview

Most modern organizations already collect a wealth of risk-relevant data about people, process and technology. The problem is that this data is often siloed and only used for the most narrow of purposes and activities. Prevari leverages existing risk-relevant data to calculate measures of inherent and residual risks to information by applying the methods described in US Patent #7,900,259 - Predictive Assessment of Network Risks.

As our core offering, Prevari provides a risk calculation engine that measures an organization's resilience to both known and unknown threats to the confidentiality, integrity and availability of information. We accomplish this by analyzing risk-relevant information provided by the sensors, scanners, and management systems used to operate and manage the information systems that support complex organizations.

Organizational maturity with Governance, Risk and Compliance (GRC) functions within IT vary from seat of the pants to robust implementations of eGRC tools supported by a risk-focused culture and processes. Prevari's metrics and predictive analytics enable customers all along the GRC maturity scale to increase productivity and improve GRC maturity.

Prevari provides tactical and strategic decision makers with the information required to make well-informed risk-based decisions. Decisions that balance the operational benefits of complex information systems with the risk of those same information systems being conduits for attack, error or disruption that causes mission or business failure.

Current practices for managing risk to information are more art than science. Most information risk management decisions are based on subjective interpretation of best practice, the compliance-driven reactive application of controls, and by fear, uncertainty, and doubt. Today's metrics for information risk tend to be summaries of events that have occurred in the past; incidents resolved, vulnerabilities patched, attacks repelled, and machines configured to standard. While of some use for process improvement, this is equivalent to driving by looking in the rearview mirror. Prevari products and services are purpose-built to mature the current art to the science of information risk management.

This paper briefly describes Prevari's TRM solution and its impact to improve decisions and provide quantitative, objective, repeatable metrics to answer the questions:
1. How secure is my organization?
2. How has risk to information changed over time?
4. How will this new system or control impact risk?
5. How does that product or software fit into the existing systems and networks?
6. How do we spend our limited security/compliance resources for maximum risk reduction?
7. How resilient are we against cyber threats, mis-configuration, and environmental effects?
Technology Risk Manager
TRM provides analytics that evaluate the strength of information systems and their resilience to attack. TRM consumes risk-relevant data from common tools supporting IT, security, audit, and compliance functions (e.g. scanners, CMDBs, audit automation, SIEMs, eGRC and compliance repositories).

Figure 1 - Data flow and functional overview.
The Metrics
TRM calculates probability of compromise expressed as a risk index on a scale between zero and 100 (zero indicates no risk, 100 indicates compromise - both are practical and statistical impossibilities).

Risk Indices are produced for:
- Confidentiality,
- Integrity,
- Availability, and
- Audit.

TRM provides CIAA risk indices and variances at the host level and aggregates the risk indices up to the network and enterprise levels. Merge functionality supports combining models from various parts of the organization and combining them into a single risk model.

Figure 1 shows the overall data flow and functional modules of TRM. TRM is first and foremost a risk calculation engine. Using risk-relevant data that most organizations already produce as a part of normal operations, TRM mines this data and calculates objective measures of the probability that the system can be compromised.

TRM’s risk calculation engine relies upon the Information Risk Knowledge-base (IRK) which contains values ranking the risk characteristics of system components. More than fifteen years of research and analysis is captured in the IRK database and an interface is provided to either modify values or to add information not covered by the IRK's 10,000+ entries. If you disagree with Prevari’s values, change them - the important practice here is to use a consistent yardstick across all systems in your environment. Prevari's IRK draws data from the Unified Compliance Framework™ (UCF) dataset describing the normalized set of legal-reviewed controls that span more than 400 US and international regulations, standards and best practices. Prevari maps the UCF data to its specific mathematical impact on confidentiality, integrity, availability and audit. Other external data sources include the National Vulnerability Database as well as operating system Security Configuration Checklists, both from the National Institute of Standards and Technology.

TRM first calculates inherent risk - the risk, absent any controls whatsoever, that the system can be compromised. Both automated and manual interfaces are provided to inform TRM about the controls deployed to protect the system. Again referencing the IRK, TRM calculates the risk reduction value of the controls and presents the values for residual risk - the inherent risk net of the impact of the controls deployed to the system. In other words, residual risk is the net risk the system faces today (probability of compromise).
The Value
TRM is used to describe the current state of risk and to simulate alternate future states by constructing 'what if' analyses that depict different combinations of technology controls and administrative controls (policy and process controls). This capability allows decision makers to quickly consider numerous alternatives before making a decision to purchase additional technology controls or change operations to implement superior administrative controls. Simulations are also used to hold Program Managers accountable for the risk-reduction results used to justify the program in the first place.

TRM provides more than one hundred different graphs for executive presentation and nearly unlimited options for lists and tables that present both summary and drill-down capable views into the system's risk. All TRM risk data is exportable to office productivity suites and the IRKs underlying SQL Server™ database is exposed for analysis by Business Intelligence and reporting tools if desired.

TRM's value proposition includes:

- **Increase productivity** and improve the focus of security, compliance and audit functions.
- **Reduce the cost** of deployed controls by only purchasing what is necessary to manage risk,
- **Ease of deployment and use** - most installations are completed in a day and begin generating actionable information immediately - users are trained in one day,
- **Reduce staff effort** required to support security operations, audit and compliance functions,
- **Reduce audit fatigue** through the use of metrics to focus activities on the areas of greatest risk,

TRM operates on standard Microsoft® technologies and can be deployed in a one, two or three tier technology architecture. Performance testing has shown that TRM can easily compute risk for a network that includes two million hosts.
Notional example
This notional example of a risk analysis using TRM is based upon a network of 1000 hosts running over 2,184 different network services, a variety of operating systems variously configured, and all the procedural controls prescribed by NIST 800-53A.

Figure 2 shows the Risk Profile tab of TRM displaying graphically the inherent and residual risk for the notional system, answering the question ‘How secure is my organization today?’. Put another way, the difference between the orange and green bars highlights the value of the controls currently deployed to the system to reduce risk. The controls for this system include full compliance with NIST 800-53A, use of directory authentication and virus protection with current signatures on all hosts.

Figure 2 - TRM Risk Profile
The Models & Simulations tab of TRM enables one to create unlimited and nested organizational structures by which to view and report on the risk data. Figure 3 shows a model of the notional system organized by system and computer type as well as the simulation of adding an intrusion prevention system as a control protecting the entire system.

The Models & Simulations tab provides a drag and drop interface to build a detailed model of the system with both technical and administrative controls applied and simulated to hosts, subnets, organizational structures, or entire systems. This model persists over time and is updated with new information as it becomes available, allowing comparisons of the risk profile of the system at appropriate intervals.
Figure 4 displays some of the various views within TRM that enable quick, accurate decision making to manage information risk.

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Residual Risk</th>
<th>Simulated Risk</th>
<th>Difference</th>
<th>XCCDF (Unweighted)</th>
<th>XCCDF Weighted</th>
</tr>
</thead>
<tbody>
<tr>
<td>host154</td>
<td>99.990</td>
<td>99.990</td>
<td>0.000</td>
<td>70% (676/967)</td>
<td>30% (272/1000)</td>
</tr>
<tr>
<td>host155</td>
<td>99.990</td>
<td>99.990</td>
<td>0.000</td>
<td>37% (125/335)</td>
<td>63% (207/328)</td>
</tr>
<tr>
<td>host156</td>
<td>99.990</td>
<td>99.990</td>
<td>0.000</td>
<td>37% (117/335)</td>
<td>63% (218/328)</td>
</tr>
</tbody>
</table>

By calculating on both technical security and compliance data, TRM provides a uniquely holistic understanding of how to proactively manage the many risks to your information. Please contact us at 763.545.4876 or sales@prevari.com for a deeper dive.