

TraceSecurity Risk Manager

TraceSecurity Risk Manager™ is a cloud-based tool that helps the organization facilitate an ongoing risk management program.

Risk Manager is a specialized module contained within TraceSecurity's Compliance Manager, a comprehensive solution that provides access to a host of security compliance tools organizations used to manage an ongoing security compliance program.

Risk Manager is used to analyze an organization's vulnerabilities, threats, asset information, controls and loss expectancies. It assists in the analysis process and enables the user to assess critical focus areas to determine the overall level of risk. Plus, the entire risk assessment process is captured and managed through the software which automates the process and provides a foundation for future risk assessments.

TraceSecurity Risk Manager offers many benefits to your organization:

Reduces employee resource costs of Risk Assessments

- Streamlines the entire Risk Management process through an preconfigured framework of threats, assets and controls
- Fully customizable threats, assets and control parameters
- Measures risk level of each asset related to: Confidentiality, Integrity, Availability
- Provides both quantitative and qualitative methodologies
- Leverages previous risk assessment responses to minimize the time associated with controls that have not changed since the previous risk assessments

Develops a standard, repeatable audit process

- Based on standard risk assessment approaches including OCTAVE & NIST
- Integrated regulation information to aid in compliance
- Can easily be mapped to company-specific regulations and standards
- Customizable levels of risk assessment; one size does NOT fit all
- Framework guides multiple employees through the same risk assessment methodologies providing a standardized risk assessment process

Creates standardized, accurate reports and thoroughly prepares the IT department for audits by regulatory boards

- Creates a concise executive summary for management, boards and auditors
- Detailed reporting capabilities including charts and graphs
- User note section helps create a trail and lessens the time wasted trying to track information during examiner review

TraceSecurity Compliance Manager

At the core of our solution is **TraceSecurity Compliance Manager**, a comprehensive cloud-based solution that integrates a variety of tools to automate the most critical functions of a continuous security compliance program:

- **Vulnerability Assessment**
- **Compliance Analysis**
- **Policy Development, Distribution and Management**
- **Learning Management System**
- **Risk Assessments***
- **IT Audits***

* Available as optional products

Key Features of Risk Manager

- Cloud-based; always available, on-demand
- Automates the risk assessment process
- Based on industry standard risk assessment approaches including OCTAVE and NIST
- Built-in framework of threats, assets & controls
 - Fifteen unique threat types
 - Over 100 security controls
 - Predefined asset information
 - Predefined severity levels for threats, controls and vulnerabilities
- Parameters for threats, assets and controls are fully customizable
- Detailed reporting capabilities with charts & graphs
- Built to scale
- Multi-user access
- Integrated regulation data aids in compliance
- Continuously updated with new threats/controls

RiskManager saves time and money by automating the steps involved with the risk management process:

- 1. Asset group analysis.** Identifies core assets and assigns a level of criticality to each asset in the areas of CIA.
- 2. Threat analysis.** Identifies relevant threats, evaluates each threat to determine which assets are affected, then assigns a level of criticality to each asset in the areas of CIA.
- 3. Control analysis.** Identifies safeguards that can be used to protect each asset, assigns values to each control in terms of how it protects against specified threats.
- 4. Risk assessment reporting.** Automatically associates & calculates data to produce a detailed risk assessment report.



What is a risk assesment?

A risk assessment essentially determines what type of controls are required to protect an institution's assets and resources from threats in order to maintain stability. The process evaluates the likelihood and potential damage of the identified threats, measures the individual risk level of each information asset as they relate to Confidentiality, Integrity and Availability (CIA), and then gauges the effectiveness of existing controls in limiting exposure to risk. These results help the organization identify which assets are the most critical, provides a basis for prioritization and recommends courses of action to protect the assets at risk.

Why do organizations need a risk assessment?

The increased frequency of security incidents has resulted in new legislation at both the federal and state levels. Fundamental to meeting these regulations, including (GLBA, NCUA, FFIEC, HIPAA, etc.), are regularly-scheduled risk assessments.

Why do organizations fail to perform regular risk assessments?

Whether you are in a regulated industry, a government agency or an organization seeking to benchmark against widely-accepted Best Practices, you will need to conduct regular, recurring information risk assessments as part of your information security program. Because methodologies are often viewed as complex and cumbersome, many organizations have relied on external firms to perform these activities on a contract basis. Unfortunately, it can be expensive to engage a third-party assessment team, and more importantly, it is unlikely that they will understand your business well enough to yield a meaningful result. Additionally, the organization may try to implement its own internal Risk Assessments program, but this usually puts a strain on key personnel's time.

RiskManager allows the institution to manage their processes locally with TraceSecurity providing technical support and enhancing their efforts with additional services. This method helps the organization facilitate a continuous risk management program without straining internal resources or incurring high vendor costs each time a risk assessment is needed.