

TraceSecurity Compliance Manager

TraceSecurity Compliance Manager™ (TSCM) is a cloud-based tool that provides convenient access to a host of products used to manage the processes involved in an ongoing security compliance program.

One of the most beneficial advantages of TraceSecurity Compliance Manager™ is the ability to have access to all the necessary tools administer every aspect of a security compliance program within one comprehensive portal. TSCM gives organizations the ability to:

Streamline Security/Vulnerability Assessments

- Schedule and perform on-demand vulnerability assessments
- Produce 3rd party expert verified and false-positive tested assessments at any time
- Comprehensive assessment report delivered via TSCM within 2 business days
- Develop a repeatable process for each successive security assessment

Automate the Risk Assessment and IT Audit Processes

- Streamlines the Risk Management and IT Audit processes through a preconfigured framework of threats, assets and controls that are fully customizable
- Develops a standard, repeatable audit process that meets compliance standards
- Creates standardized reports and thoroughly prepares the IT department for audits

Facilitate Security Compliance Tracking and Reporting

- Choose applicable regulations and/or best practices to monitor and self assess
- Customizable compliance reporting for Management, board, & auditor reports
- Online database for up-to-date regulations and best practices
- Customizable alerting to new or modified regulations and/or best practices

Develop and Disseminate Policies Through a Centralized System

- Create policies based on templates that meet applicable regulations
- Upload all organizational policies into a centralized database
- Modify existing policies and alert employees on the changes
- Disseminate policies to appropriate employees and track acceptance
- Printable reports for internal use or examiners

Develop and Manage an Information Security Training Program

- Deliver customized training courses through a centralized online system
- Administer tests for each course, send email notifications and track the results
- Generate comprehensive reports for internal use or examiners
- Compatible with third-party web-based training

What is involved in an ongoing Information Security Program?

- Regular testing for network vulnerabilities, including infrastructure, servers/workstations
- Proactively identify the latest network vulnerabilities that could impact the organization
- Monitor compliance of existing & new regulatory requirements
- Develop, implement and update Information Security Policies and Procedures
- Train users on Information Security Policies & Procedures
- Test employees for understanding of Information Security Policies and Procedures
- Report to management, board of directors, and auditors

**TSCM continuously addresses the 3 core components of an information security program:
People, Processes, and Technology.**

TraceSecurity Compliance Manager is a comprehensive software solution that integrates a variety of security compliance products into one convenient web interface.

TSCM includes the following standard modules:

Modules	Benefit
TraceAssess	Unlimited, on-demand network vulnerability scanning
TraceComply	Review of compliance with security requirements
TracePolicy	Security Policy creation and distribution
TraceTrain	Online employee training management
TraceReport	On-demand board, auditor, and technical reporting

These modules may be added to expand TSCM’s functionality:

Risk Manager	Helps automate the Risk Assessment process
IT Audit Manager	Helps automate the IT Security Audit process

TraceSecurity Compliance Manager helps reduce the burden of managing a security compliance program.

Pre-configured software: Complete with a matrix of options in easy-to-navigate menus, reducing the amount of configuration and helps eliminate errors.

Multiple levels of support: Customers have access to TraceSecurity experts for assistance with a variety of compliance-related needs.

Independent of institution’s network: TSCM is cloud-based software, so the IT department is freed up from performing updates or maintenance.

A scalable solution: TSCM can be modified and enhanced as the security needs of the organization mature.

Customizable and integrated reports: TSCM can integrate results from several processes in order to generate customizable, easy to read reports that help streamline the audit process.

A cost-effective solution: TSCM offers a variety of security compliance tools, which helps eliminate or reduce costs of managing multiple technology vendors, purchasing unnecessary hardware, and expenses associated with deploying in-house IT resources.

Why does an organization need an on-going Information Security Program?

A basic Information Security Program is needed in order to meet many of the regulatory requirements facing an organization, as well as an important first step in protecting its critical information. However, because the people, processes and technology of an organization are continually changing, the security threats to that organization are also changing. Therefore, in order to identify new threats and prevent a security breach, an organization must have an ONGOING Information Security Program.

How can organizations “Jump Start” their Information Security Program?

Regulatory requirements insist organizations have regular Security Assessments performed by an independent third-party who is in no way responsible for the design, maintenance or administration of the network infrastructure or its security controls. Moreover, organizations are also required to have an ongoing security testing program that include periodic self assessments.

By choosing TraceSecurity to perform a **Comprehensive Security Assessment**, customers get the benefit of having ongoing access to the same tools and customized information that TraceSecurity analysts used to perform the initial assessment through TSCM. This combination of service and software solutions not only satisfies the requirements of independent assessments, but also helps quickly establish a solid foundation for an ongoing self assessment program in a cost-effective manner.



TraceSecurity provides compliance and risk management solutions to organizations of all sizes that help them achieve, maintain and demonstrate security compliance while significantly improving their security posture. Over 1,000 organizations currently leverage our on-demand, web-based applications backed by expert professional services and analysis to address all critical components of their security compliance program, including people, process and technology. TraceSecurity’s flagship **TraceSecurity Compliance Manager** is the first comprehensive software-as-a service platform to integrate and automate vulnerability assessment, vulnerability alerting, regulatory compliance audits, policy management and dissemination, file/URL integrity monitoring and employee education and testing.

TraceAssess

An information security program should include ongoing network vulnerability testing. The TraceAssess module of TSCM is an automated vulnerability assessment utility that evaluates a network for security risks. The TraceAssess scanner is delivered through a VMware Player eliminating the need to purchase a hardware appliance. The interface to TraceAssess is through the SaaS based TSCM portal making it available anywhere

Key Features and Benefits of TraceAssess include:

- **Template based scan configurations for consistent, repeatable process**
 - Port scan, vulnerability scan or simultaneous scan
 - Test Single IP address or a range of IP addresses
 - User definable "exclude" IP address list
 - Network Discovery option
 - Configurable Signature Scanning
 - Single Vulnerability
 - User defined group of vulnerabilities
 - Predefined "safe" signatures
 - Predefined "dangerous" signatures
- **False Positive Management**
- **Template Groups to combine multiple templates**
- **Scheduler Frequency**
(once, daily, weekly, biweekly, monthly, bimonthly, quarterly, yearly)
 - Date and Time
 - Pause Schedule
 - Email notification
 - "Allow" schedule to facilitate real-time scanning during off peak hours
- **Filter Results based on**
 - Risk Level
 - Classification
 - Status (Resolved, unresolved, false positive)
 - Operation System
 - Assignee
 - Templates

TraceAssess can be used as a standalone solution or integrated with other TSCM modules. Summary dashboard reporting provides a quick view of vulnerability data to allow for immediate awareness of network vulnerabilities. In-depth reporting is available for system administrators, managers, board of directors and auditors.

Mark Ross, VP of IT Burbank City FCU

"Prior to partnering with TraceSecurity, we couldn't see all of our existing vulnerabilities...and we weren't able to implement the right controls to provide adequate security. But with the expert help of TraceSecurity, we're confident that we can identify any vulnerabilities much quicker than before"

Assistant VP of IT at a Major Credit Union

"I can't say what the cost would be if we didn't identify and remediate [vulnerabilities]. We work hard to make sure no one can access our internal network. However, if someone was to get on our internal network, obtain our member information and expose it, there would be a great cost. We would lose the trust of this community and we wouldn't be able to do business here anymore."

TraceComply

A proper Information Security Program should be in compliance with applicable Regulatory and Best Practices requirements. Common issues with preventing compliance with these requirements include: lack of expertise and understanding of the regulations, employee time involved reporting on compliance, and monitoring new or modified requirements.

TraceSecurity has developed **TraceComply**, a module of TSCM that facilitates security compliance tracking and reporting. TraceComply allows the user to choose applicable regulations and/or best practices to monitor and self assess for compliance.

Key Features and Benefits of TraceComply include:

- **Online regulatory self assessment solution**
 - Choose regulations and/or best practices applicable to the organization
 - A single answer addresses all regulations with similar requirements, reducing time needed to complete
 - Responses include "Compliant", "Not Compliant", "Partially Compliant", "Not Applicable"
 - Note fields to provide explanation
 - Results can be saved for later completion
- **Customizable compliance reporting**
 - Management, board of directors, & auditor reports
 - Filter for laws, guidelines or standards
 - Dashboard detailed and summary reporting
 - Printable reports
- **Online database for current regulations & best practices**
- **Customizable alerting to new or modified regulations and/or best practices**
- **Utilizes "Assets" and "Vendors" to provide segmentation of compliance at the Asset or Vendor Level**
- **Includes information on the regulations, code, related policy and other reference materials**

TraceComply can be used as a standalone solution or integrated with other TSCM modules. Summary dashboard reporting provides a quick view of compliance data to allow for immediate awareness of gaps in compliance. In-depth reporting is available for managers, board of directors and auditors.

Ernesto Segovia AVP at Meriwest CU

"From the very beginning, we were confident that TraceSecurity had the solutions we needed to enhance our security posture."

VP of Information Services, IL Financial Institution

"The other major driver in choosing TraceSecurity was the whole area of compliance ... the fact that TraceSecurity has software that provides questions that, when answered, reveal where you stand on compliance. Before, we were just doing periodic scans...

We didn't even know if we were compliant."

Assistant VP of IT IL Financial Institution

"The auditing firm wouldn't list all the areas where we were non-compliant and they wouldn't ask all the questions because it takes an inordinate amount of time."

TracePolicy

To effectively implement an Information Security Program, the organization must address vulnerabilities associated not only with its technology, but also with its people and processes. The “people” vulnerabilities are one of the largest risks associated with an Information Security Program, and also, one of the most overlooked areas. A 2006 study by the Computing Technology Industry Association indicated that human error was responsible for nearly 60% of data breaches, as opposed to hardware or software vulnerabilities.

Despite all the time, effort, and money invested in the acquisition, deployment and ongoing management of security technology, an organization must address the “people” risk. Organizations must therefore implement best practices that help prevent employees from engaging in behaviors that can compromise sensitive data.

These best practices include:

- Defining appropriate policies and procedures governing employee behavior in regards to information security
- Educating employees about the policies and procedures relevant to them
- Verifying their understanding of relevant policies and procedures
- Managing change over time – including changes in staff, changes in the IT environment, and changes in the nature of present threats

While TracePolicy was originally designed to facilitate an Information Security Program, the solution should be used by all organizational departments, including Human Resources, to efficiently manage all departmental policies.

This allows an organization to have a centralized policy management system for all organizational policies.

TraceSecurity has developed TracePolicy, a module of TSCM, to facilitate an organization’s Information Security Program by specifically addressing the “people” vulnerability issues.

Key Features and Benefits of TracePolicy include:

- **Ability to Develop Information Security Policies**
- **Templated questionnaires that facilitate the creation of policies to meet applicable regulations (with additional Best Practices templates as needed)**
- **Upload/Modify Existing Policies**
 - Upload all existing organizational policies for one centralized database
 - Modify existing policies and update employees on the current policy
- **Disseminate Policies**
 - Simplified policy distribution through email notification
 - Online employee policy review
 - Online policy acceptance
 - Ability to group employees to only receive policies that are applicable to the specific group
- **Centralized, online policy management and reporting accessible by authorized users anywhere & anytime**
 - Eliminates paper-based systems
 - Online policy database
 - Online employee policy acceptance database
 - Online policy approval
 - Track creation date
 - Acceptance reporting including date accepted
- **Automatic email alerts for employees that have not accepted policies**
- **Printable policies and reports**

TracePolicy can be used as a standalone solution or integrated with other TSCM modules. Summary dashboard reporting provides quick view of policy data to allow for immediate awareness of gaps in policy acceptance. In-depth reporting is available for managers, board of directors and auditors.

TraceTrain

To effectively implement an Information Security Program, the organization must address vulnerabilities associated not only with its technology, but also with its people and processes. The “people” vulnerabilities are one of the largest risks associated with an Information Security Program, and also, one of the most overlooked areas. A 2006 study by the Computing Technology Industry Association indicated that human error was responsible for nearly 60% of data breaches, as opposed to hardware or software vulnerabilities.

Despite all the time, effort, and money invested in the acquisition, deployment and ongoing management of security technology, an organization must address the “people” risk. An organization must implement an employee training program designed to help prevent behaviors that can compromise sensitive data.

The training program should:

- Educate employees on the Information Security policies and procedures
- Manage training requirements related to:
 - Change to staff
 - Changes to IT environment
 - Changes to organizational risk
 - Changes in policies and procedures
- Verifying their understanding of relevant policies and procedures

While TraceTrain was originally designed to facilitate an Information Security Program, the solution should be used by all organizational departments, including Human Resources, to efficiently manage all departmental training.

This allows an organization to have a centralized training program for all organizational training.

TraceSecurity has developed TraceTrain, a module of TSCM, to efficiently facilitate an organization’s Information Security Training Program.

Key Features and Benefits of TraceTrain include:

- **Customizable training relevant to an organization’s Information Security Program**
 - Administrator defined Courses
 - Compatible with third party web based training
- **Create Training Groups**
 - Facilitates automatic email notification of required training
 - Deliver training applicable to specific employees
- **Centralized, Online Training Management & Reporting**
 - Reduces business impact related to live training classes
 - Modify existing policies and update employees on the current policy
 - On-demand training provides flexible training times
 - Email alerting on required training
 - Track Training status by user or department
 - “Taken/Not Taken”
 - Date Taken
 - Printable training materials
 - Printable reporting
- **Test employees’ understanding of training courses**
 - Customizable testing for each training course
 - Track Testing status by user or department
 - “Passed/Failed”
 - “Taken/Not Taken”
 - Date Completed
- **Centralized, online policy management and reporting accessible by authorized users anywhere & anytime**
 - Eliminates paper-based systems

TraceTrain can be used as a standalone solution or integrated with other TSCM modules. Summary dashboard reporting provides quick view of training and testing data to allow for immediate awareness of gaps in employee security awareness. In-depth reporting is available for managers, board of directors and auditors.