

Comprehensive Security Assessment

www.tracesecurity.com

Overview of Regulations and Best Practices

IT Security Compliance regulations and guidelines (GLBA, FFIEC, FDIC, OCC, OTS) require an organization to conduct independent 3rd-party testing of the Information Security Program to identify vulnerabilities that could result in unauthorized disclosure, misuse, alteration, or destruction of confidential information, including Non-Public Personal Information (NPPI). An Information Security Program must include safeguards designed to protect against both technical and human vulnerabilities. Because the security program incorporates more than just the network, Best Practice guidelines suggest testing should include more than a simple network vulnerability scan. The recommended Best Practices methodology is a Security Assessment that incorporates testing of both technical and human vulnerabilities people related to the information security program.

Solution Overview

The TraceSecurity Comprehensive Security Assessment was designed specifically to meet the regulatory requirements and address the needs of organizations of all sizes. The assessment provides a thorough examination of your networks to determine the adequacy of existing security controls and to identify security deficiencies. The assessment process is managed through TraceSecurity Compliance Manager 5.0, a web-based portal designed to provide convenient access to a variety of tools used to continuously assess the three core components of an information security program: People, Processes, and Technology.



Web-based TraceCompliance Manager's integrated dashboard provides a real-time view of a risk and security compliance status.

TraceSecurity Compliance Manager 5.0

Because security assessments can only measure the security posture at a single point in time, it is necessary for an organization to continuously assess their Information Security program. TraceSecurity's Compliance Manager 5.0 helps organizations seamlessly transition to an in-house Self Assessment program. With TSCM 5.0, customers can schedule and perform vulnerability assessments **on-demand** which allow for testing on a daily, weekly, monthly, or quarterly basis. Each assessment will be reviewed by a TraceSecurity analyst for false-positives and a comprehensive report will be delivered via TSCM within 2 business days from the date of the vulnerability assessment. TSCM 5.0 enables the organization to use a repeatable process for each successive security assessment, providing a foundation for establishing an ongoing self assessment program.

The Comprehensive Security Assessment includes all these TSCM 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

Each Comprehensive Security Assessment includes the following:

- External port scan
- External network vulnerability scan
- Internal port scan
- Internal network vulnerability scan
- Asset classification assistance
- Policy Review
- In-depth Regulatory and/ or Best Practice Review through TraceComply Self-Assessment
 - Includes Third Party/Vendor Security Analysis
- Regulation Call to Assist with TraceComply Self-Assessment
- Network Topology Review (if provided by client)
 - Third Party/Vendor Connections Interface Security Analysis
 - Assistance with Vendor Due Diligence
- TraceSecurity Compliance Manager (TSCM) System Setup and Implementation
- Internal Network Vulnerability Review
 - False Positive Reduction of Scan Data through Manual 3rd-Party Review
 - Validation of False Positive Review through Manual 3rd-Party Analysis
 - Advanced Manual Vulnerability Analysis to Determine Vulnerability Severity

- Security Countermeasure Review
 - Anti-virus
 - Host Base or Network IDS/IPS
 - Network Access Control
 - Firewall
- TSCM “Basic Training”
- Present Preliminary Findings to Client Core Team through Exit Interview
- Deliver Final Deliverable through TSCM

If the comprehensive security assessment is conducted onsite, the Information Security Analyst (ISA) will perform the following:

- Policy Awareness Review through a Sampling of Employee Interviews
- Identify Wireless Access Points, including Rogue
- Physical Security Review
- Dumpster Diving at Main Facility
- Present Preliminary Findings to Client Core Team through Exit Interview
- Offsite Consultation and Remediation Strategy

Access to TSCM for the Service Term of the contract with the following benefits:

- On-demand Generation of Comprehensive Reports
- **TraceAssess:** Unlimited Client-Executed Scans with 3rd-Party Remote False Positive Validation
- **TraceComply:** Regulatory Compliance and Security Assessment Evaluation Metrics through Self-Assessment
- **TracePolicy:** Automated Policy Development Software and Policy Management
- **TraceTrain:** Automated Training Development Software and Training Management; Including Access to Security Awareness Training Content
- Automatic TSCM product updates as available

The CSA results are provided in an extensive report containing:

- Project Overview
- Comprehensive Security Assessment Methodology
- Executive Summary
- Prioritized Internal & External Network Risks and Recommendations
- Regulatory Compliance Analysis
- Information Security Policy Analysis
- Executive Level PowerPoint of Assessment
- Differential Reporting
- Appendix

About TraceSecurity: 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.