EFFECTIVE SECURITY STARTS WITH UNDERSTANDING YOUR RISKS

When properly conducted, a risk assessment can determine what type of controls are required to protect your organization’s assets and resources (physical locations, networks/servers, staff, etc.) from both internal and external threats. An assessment should:

- Evaluate the likelihood and potential damage of identified threats
- Measure the individual risk level of each asset as they relate to Confidentiality, Integrity and Availability (CIA)
- Gauge the effectiveness of existing controls to limit the organization’s exposure and risk

From these efforts it should be possible to identify which assets are the most critical, provide a basis for prioritization, and recommend a course for remediation.

THE COMPLIANCE OVERVIEW

Like millions of other data-driven organizations – including financial institutions, retailers, consumer service companies, healthcare providers, government agencies, insurance companies, and educational institutions – your company is subject to threats that can impact IT infrastructure. This means you are subject to strict compliance standards and have a responsibility to implement and maintain a formal risk assessment process to identify and evaluate risks.

Any number of the many IT security mandates (such as FDIC, GLBA, HIPAA, HITECH, NCUA, OCC, and PCI DSS) require you to conduct regular risk assessments in order to identify reasonably foreseeable risks that, if left unchecked, could lead to service interruption or unauthorized disclosure, misuse, alteration, or destruction of confidential information. Chances are that you lack the resources and expertise to manage such assessments on your own.

TRACESECURITY RISK ASSESSMENT OVERVIEW

TraceSecurity advances the risk assessment process to its most comprehensive and effective form, with a methodology that exceeds best practices and regulatory standards for compliance.

Our experts closely scrutinize your organization’s controls, vulnerabilities, threat vectors, asset information, and loss expectancies. Each individual risk is analyzed and compared against other identified risks, enabling the organization to prioritize remediation efforts and preempt losses with the most exposure.

In addition to providing the most thorough, objective, and easy-to-read risk assessment available, our risk assessment methodology offers significant advantages if you are in a highly regulated industry. Advantages include:

- Based on NIST 800-30
- Customizable assessments created to your organization’s specific needs and compliance requirements
- Dynamic integration with your audit program
- Influence by regulatory requirements and industry standards
- Streamlined development of a standard and repeatable compliance processes to help you achieve and maintain an ongoing risk-based information security program
- The ability to generate standardized, easy-to-understand reports for examiners, management, and board members
Key service activities include:

- Data gathering (based on interviews and documentation)
  - Identify key personnel
  - Identify and collect key documentation
- Based on the data gathered, the analyst performs:
  - Asset Group Analysis
  - Threat Analysis
  - Control Analysis
  - Risk Analysis
  - Reporting
  - Report Briefing

Results are provided in an extensive report containing:

- Project overview
- Risk assessment methodology
- Executive summary
- Detailed risk analysis by asset group
- Control group summary
- Information security policy analysis
- Recommended action plan
- Appendix

Automation of the risk management process includes:

- **Asset group analysis** — Identifies core assets and assigns a level of criticality to each asset in the areas of CIA
- **Threat analysis** — Identifies all 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
- **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
- **Risk assessment reporting** — Automatically associates and calculates data to produce a detailed risk assessment report

Other capabilities include:

- Creation of new assessments using preconfigured templates or existing, customized templates
- Addition of new threats, assets, and controls from a centralized repository
- Ability to revise risk assessments, then track and log each revision
- Summary reports for boards or examiners
- Detailed reporting capabilities with charts and graphs
- Integrated regulation information to aid in compliance
YOUR SINGLE SOURCE FOR A FULL RANGE OF IT GRC INFORMATION SECURITY SERVICES

The complex and constantly evolving nature of IT GRC (governance, risk and compliance) requires a range of experience and expertise that is nearly impossible for most companies to maintain internally. TraceSecurity’s comprehensive suite of information security services is the answer. Our seasoned experts help enhance your security posture, reduce risk, facilitate compliance, and improve operational efficiency. To provide maximum effectiveness, the TraceSecurity information security services listed can be delivered in combination with TraceCSO, our integrated cloud-based IT GRC management platform.

- Security Assessment
- Risk Assessment
- IT Security Audit
- Penetration Testing
- Social Engineering
- Web Application Testing
- Wireless Assessment
- Security Training

To learn more about TraceSecurity, call 877-275-3009 or visit www.tracesecurity.com

GRC Simplified... Finally.