IT Security Audit

DATA SHEET

Assessing and Sharpening Your Security Controls

An IT security audit involves the examination of the practices, procedures, technical controls, personnel, and other resources that are leveraged to manage your security risks and assures that you adhere to recognized best practices and IT security mandates.

The Compliance Overview

If your organization is subject to IT security mandates such as FDIC, GLBA, HIPAA, HITECH, NCUA, OCC and PCI DSS, you are required to undergo 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. Then, having determined your risks, you must initiate and maintain security controls that are in line with standards established by regulators and best practices. Effectively auditing and evaluating those controls require deep expertise and experience in IT security and up-to-date knowledge of regulatory details.

The TraceSecurity IT Security Audit Overview

Leveraging the company's cloud-based software solution, information security experts thoroughly audit your existing security controls. This involves the collection and examination of your practices and procedures documentation as well as technological control data. A TraceSecurity IT audit also includes access to audit management capabilities that enable your organization to streamline and automate the collection process.

Also included in your audit are key personnel interviews, a walk-through of your physical location(s) and any other asset(s) that impact the effectiveness of your information security program. These measures are designed to verify that existing controls adhere to your organization's risk assessment, best practice standards, and applicable regulatory compliance

TraceSecurity IT Security Audit Services:

- Authentication and access controls
- Network security
- Host security
- User equipment security (e.g. workstation, laptop, handheld)
- Personnel security
- Physical security
- Application security
- Software development and acquisition
- Business continuity – security
- Service provider oversight – security
- Encryption
- Data security
- Security monitoring

IT Security Audit results are provided in an extensive report containing:

- Introduction
- Executive summary
- Remediation action plan
- Detailed audit results
- Control descriptions and verification procedures
- Script injection attacks
- Supporting documentation