

Security & Risk SecAssure Assessments

Overview

Security and Risk SecAssure Assessment (SecAssure Assessment) includes an analysis of the effectiveness of a company's or specific system's security controls. Our service includes adaptive techniques to work with organizations to review the risk associated with a company's overall security design, implementations of sensitive e-commerce applications, and overall risk identification to ensure that proper security controls are utilized.

Benefits

A SecAssure Assessment can help save your company time, money and the embarrassment of a bad audit by finding discrepancies before an audit occurs and before a hacker does. In addition, by allowing Emagined Security to perform the assessment for you, you receive the most accurate and unbiased report of your strengths and vulnerabilities in the information security arena.

Description of Service

SecAssure Assessments start by evaluating crucial components at the corporate and technical levels. These reviews are broken into Security Foundation Assessments and Security Implementation & Configuration Reviews.

- Security Foundation Assessment
 - Security Program Assessment
 - Security Technology Assessment
- Security Implementation & Configuration Review
 - Configuration Reviews
 - Internal / External Vulnerability Scans

The **Security Program Assessment** provides an analysis of the effectiveness of a company's security controls based upon ISO 27001, 27002. This task will assess the current security posture, contrast it against industry standards and best practices, and make recommendations to attain your security goals. Emagined Security recommends that you periodically assess your security environment to ensure that you are in compliance with each regulation that governs your industry.

- Review of current documentation, policies and practices
- Interviews with key personnel
- Comparisons against "best practice"

The **Security Technology Assessment** performs a high-level security review of the external security boundary along with selected key areas and systems to determine potential vulnerabilities and risks. The primary systems and areas of interest include:

- Internet Connectivity
- Remote Access
- Business Partner Connections
- Critical Internal Network Infrastructure
- Application Security Infrastructure

The **Configuration Reviews** will perform key Technology Equipment reviews (e.g., firewalls, routers, servers) and make cost effective recommendations. This review provides an internal perspective of technology to determine if configurations are adequate.

The **Internal / External Vulnerability Scans** performs a limited external vulnerability assessment against the COMPANY Internet architecture (i.e., firewalls, DNS servers, routers, hubs, load balancers, and supporting systems). By attempting to gain access to the systems on the Demilitarized Zone (DMZ), Emagined Security will attempt to identify risks associated with the current security configuration.