

Network Protection for Design Professionals

Assess and Upgrade

Background:

A periodic comprehensive assessment of the management, operational and technical security controls in an information system is necessary to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The results of the assessment are used to reassess the risks and update the system security strategy and policies.

How to implement appropriate controls:

Test information security procedures and technical controls annually at a minimum. Utilize a reputable outside vendor or adequately trained staff member.

- Assess the vulnerability of your networks to commonly known or reasonably foreseeable attacks.
- Scan computers on your network to identify and profile the operating system and open network services.
- Utilize resources such as US-CERT, the SANS Institute, and the Federal Trade Commission, to monitor the constantly evolving threat environment and to stay abreast of emerging privacy issues.
- Update your security plan according to the results of testing, changes in operations or other circumstances that might impact information security.

Resources:

Protecting Personal Information: A Guide for Business, Federal Trade Commission, <http://www.ftc.gov/infosecurity/>

Security Check: Reducing Risks to your Computer Systems, Federal Trade Commission, <http://www.ftc.gov/bcp/online/pubs/buspubs/security.shtm>

SANS Top-20 2007 Security Risks (Annual Update), SANS Institute, <http://www.sans.org/top20/#prevent>

US-CERT – United States Computer Security Readiness Team, <http://www.us-cert.gov/>

Information Security Handbook: A Guide for Managers, National Institute for Standards and Technology, <http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf>

