

Breaking the Language Barrier—Clarifying Information Security Terminology

In a recent meeting with a prospect, I was asked if our company could perform an IT audit.

“Sure,” I replied, “What policies or standards would you like to have audited?”

With a confused look on his face, he said, “I don’t know. Maybe I just need a penetration test.”

“Do you want a penetration test or a vulnerability assessment?”

After a long pause, he asked, “What’s the difference?”

I then gave a brief description of what each service included, and together, we quickly concluded that he actually needed a risk assessment and a vulnerability assessment. He was not a security neophyte. He simply had heard the terms “IT Audit” and “pen test” interchangeably so many times that he started doing it himself.

Information security terms can be confusing. Subtle changes to terminology over time, combined with inconsistent vernacular used by vendors and examiners alike, make it difficult to stay on top of what the terms actually mean. Knowing what services to request and evaluate is even more difficult.

In an attempt to provide some clarity, I’ve outlined below the industry-accepted definitions (*italicized*) for the most common types of security services, the value of the services and recommendations on how they should be applied.

Vulnerability Scan

A computer program designed to map systems and search for weaknesses in an application, computer or network.

Vulnerability scans are the most basic form of security testing and may be done on the external (internet-facing) perimeter of the network, or on internal devices using automated tools. Scans provide a shallow but quick exploratory view of the network.

Because hackers use scans to reconnaissance a network before an attack, it is helpful to scan your own systems routinely to uncover easily exploitable vulnerabilities on your network. Automated scans, however, can miss a high percentage of vulnerabilities that would require a deeper analysis (e.g., configuration flaws and access controls). Used alone, scans do not adequately identify all vulnerabilities (see next section on Vulnerability Assessments).

We recommend that, at a minimum, you perform external scans quarterly and internal scans annually and any time changes are made to the network (e.g. new system, firewall, new internet service provider, etc.). Additionally, companies that are required to comply with Payment Card Industry (PCI) security standards are required to have quarterly scans completed by an Approved Scanning Vendor (ASV).

Vulnerability Assessment

A formal description and evaluation of the vulnerabilities in information systems.

Vulnerability Assessments (or Security Assessments) take a much deeper look into companies' technical safeguards, including network architecture, device configurations, access controls, data segmentation, systems administration (e.g. patch management, virus protection, backups, etc.) and the security of workstations and servers on the network.

These assessments use a combination of automated tools and manual analysis by an experienced and qualified security professional, preferably with industry certifications such as CISSP or CISA, and should include recommendations to improve the company's security posture.

Vulnerability assessments take longer to complete and are more expensive than security scans but provide a more comprehensive view of security risk.

We recommend performing vulnerability assessments every 12-18 months and when major changes are made to IT.

Penetration Testing

A test method in which the security of a computer program or network is subjected to deliberate simulated attack.

Penetration (pen) testing exploits vulnerabilities to achieve a desired result, such as gain unauthorized access to the network or data, or crash a system. A security scan typically precedes a penetration test to identify vulnerabilities that the tester would then attempt to compromise, adding cost and complexity to this type of test.

Scanning vs. penetration testing is analogous to checking that your doors are locked vs. hiring someone to break into your home to steal your television set. Although you wouldn't likely need such advanced security testing for your home, your IT systems are another story.

Testing can exploit external (internet) or internal vulnerabilities, programming flaws within software applications or policy violations by tricking employees into giving the tester unauthorized access, referred to as "social engineering."

Organizations generally use pen tests as a method to increase internal security awareness by "proving" that vulnerabilities can be exploited or as part of quality assurance process for web-facing applications. Pen tests may be disruptive and introduce additional risk to a company (including possible employee embarrassment). So, it is critical to carefully manage and monitor this activity.

IT Audit

An independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

An IT audit is solely about compliance with regulatory requirements and/or internal security controls. Like a financial audit, the IT audit needs to have a policy or standard to be compared against. Just as financial audits look at compliance with Generally Accepted Accounting Principles (GAAP), the IT audit should be evaluated for compliance with internal security policies, regulations (e.g., FFIEC, PCI) and/or industry standards (e.g., NIST, ISO).

The IT audit staff must be able to independently and objectively assess the reliability and integrity of the organization's IT controls to help maintain and improve the efficiency and effectiveness of IT risk management and corporate governance. Audits may be completed



internally, assuming personnel is independent from operating management and has sufficient skill level to audit IT. It may also be outsourced or “co-sourced” to a qualified vendor that has no conflicts of interest that may compromise independence.

While the audit should identify non-compliance with standards, policies or regulations, it may not identify weaknesses that lay outside the scope of the audit. In other words, an audit will validate “compliance” with policies, standards or regulations, but may not verify “security.”

Risk Assessment

The process of identifying the risks to systems’ security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate the impact.

The risk assessment puts vulnerabilities into context for an organization by determining the criticality of the company’s IT assets and the reasonable threats and risk that remain, considering the technical, physical and administrative safeguards in place.

When done correctly, the risk assessment becomes an invaluable two-way communication tool among senior management, the board of directors (those responsible for oversight responsibility) and IT / Operations. It allows IT and Operations to communicate the organizational risks in non-technical terms and allows senior management to communicate its tolerance for risk exposure.

As stated in the definition, risk assessment is a “process,” not a point-in-time activity to manage risk. Too often, we see risk assessment spreadsheets casually updated for board approval only before an examination. This approach offers little value to the organization and becomes simply a compliance check-off.

The goal is effective risk management, and this should be part of the organizational culture. The risk assessment process is a core component to the information security program. Risk needs to be consistently assessed as new technology, business services and vendors are evaluated. It should also drive the security test schedule and assist in the development of a “risk-based” IT Audit program.

So the next time your IT Manager or vendor starts spewing technical terms at you, remember this handy reference guide, and make sure you understand not only the terms but also the implication of any actions on your institution.

By: Jeff Olejnik, President
Assurity River Group, Inc.
4500 Park Glen Road, Ste. 120
Minneapolis, MN 55416
952-230-6488
jolejnik@assurityriver.com
www.assurityriver.com