**Security Testing Frameworks**

There are numerous security testing methodologies being used today by security auditors for technical control assessment. Four of the most common are as follows:

* Open Source Security Testing Methodology Manual (OSSTMM)
* Information Systems Security Assessment Framework (ISSAF)
* NIST 800-115
* Open Web Application Security Project (OWASP)

All of these frameworks provide a detailed, process-oriented manner in which to conduct a security test, and each has its particular strengths and weaknesses. Most auditors and penetration testers use these frameworks as a starting point to create their own testing process, and they find a lot of value in referencing them.

**OSSTMM**

OSSTMM was developed under the Creative Commons License as a free methodology to conduct security testing in a thorough and repeatable manner. The current released version 2.2 of the manual highlights the systems approach to security testing by dividing assessment areas into six interconnected modules:

* **Information Security:** Competitive intelligence, data leakage, and privacy review
* **Process Security:** Access granting processes and social engineering testing
* **Internet Technologies Security:** Network mapping, port scanning, service and operating system (OS) identification, vulnerability scanning, Internet app testing, router/firewall testing, IDS testing, malicious code detection, password cracking, denial of service, and policy review
* **Communications Security:** Private branch exchange (PBX)/phone fraud, voicemail, fax, and modem
* **Wireless Security:** 802.11, Bluetooth, handheld scanning, surveillance, radio frequency identification (RFID), and infrared
* **Physical Security:** Perimeter, monitoring, access control, alarm systems, and environment

The OSSTMM has a strong following in the community and provides a good reference for what areas need to be examined and what types of results to expect. It is not a "click here, do that" type of document; rather, it requires a level of knowledge of various tools and techniques to accomplish the goals of the tests. Version 3.0 of the OSSTMM is a significant update that is still a work in progress. As of this writing, it is in beta with no timeline announced for release. Becoming a member of the project will provide access to the current beta draft and other documents such as templates and spreadsheets that can be used in conducting an audit with this methodology.

**ISSAF**

The ISSAF is one of the largest free-assessment methodologies available. Weighing in at 1200 pages, it provides a level of detail that is staggering. The authors believe that is it better to provide all of the information possible that an auditor might need than to limit it to high-level objectives. Each control test has detailed instruction for operating testing tools and what results to look for. It is split into two primary documents. One is focused on the business aspect of security, and the other is designed as a penetration test framework. The framework has not been updated in sometime (file date is 2006), but it is still useful as source material for controls testing and as a full-assessment methodology. The level of detailed explanation of services, security tools to use, and potential exploits is high and can help an experienced security auditor and someone getting started in auditing.

**NIST 800-115**

The NIST 800-115, Technical Guide to Information Security Testing, provides guidance and a methodology for reviewing security that is required for the U.S. government's various departments to follow. Like all NIST-created documents, 800-115 is free for use in the private sector. It includes templates, techniques, and tools that can be used for assessing many types of systems and scenarios. It is not as detailed as the ISSAF or OSSTMM, but it does provide a repeatable process for the conduction of security reviews. The document includes guidance on the following:

* Security testing policies
* Management's role in security testing
* Testing methods
* Security review techniques
* Identification and analysis of systems
* Scanning and vulnerability assessments
* Vulnerability validation (pentesting)
* Information security test planning
* Security test execution
* Post-test activities

**OWASAP**

The OWASP testing guide was created to assist web developers and security practitioners to better secure web applications. A proliferation of poorly written and executed web applications has resulted in numerous, easily exploitable vulnerabilities that put the Internet community at risk to malware, identity theft, and other attacks. As a nonprofit organization, OWASP has created a number of tools, guides, and testing methodologies that are free for anyone to use. The OWASP testing guide has become the standard for web application testing. Version 3 was released in December of 2008 and has helped increase the awareness of security issues in web applications through testing and better coding practices.

The OWASP testing methodology is split as follows:

* Information gathering
* Configuration management
* Authentication testing
* Session management
* Authorization testing
* Business logic testing
* Data validation testing
* Denial of service testing
* Denial of service testing
* Web services testing
* AJAX testing

Each test provides a summary of the issues, tools that can be used to assess the service, and examples of expected results. The information and examples given are thorough, and reference materials on the tools used or issues discussed are included at the end of each of the individual tests. The OWASP project also has a subproject called WEBGOAT that enables you to load a vulnerable website in a controlled environment to test these techniques against a live system.

Whatever your approach is to testing security controls, you must ensure that it is consistent, repeatable, and based on best practices. Your audits will be more thorough and you will be less likely to miss major issues that might slip by if you are "winging" your tests. Leverage the great resources that are available free from the security community and feel free to contribute your own ideas, so that everyone can benefit.