OSSTMM 3

L I T E

Introduction and Sample to the Open Source Security Testing Methodology Manual

Contemporary security testing and analysis.

Created by Pete Herzog

Developed by ISECOM

Instructions

While this manual itself is an instruction on operational security testing, those who want to jump right into testing while using it may find the following quick-start information helpful.

Quick Start

To start making an OSSTMM test you will need to track what you test (the targets), how you test it (the parts of the targets tested and not the tools or techniques used), and what you did not test (targets and parts of the targets). Then you may conduct the test as you are accustomed to with the objective of being able to answer the questions in the Security Test Audit Report (STAR) available at the end of this manual or as its own document at http://www.isecom.org/ravs. The details on the required information in the STAR is available throughout this manual and can be referenced as needed. As you may see, taking this approach means that very little time is required in addition to a test and the formalization of the report should not add more than an hour or two. This has been done so as there is no time or financial reason to avoid using the OSSTMM and no restrictions are made to the tester. To be an OSSTMM compliant security provider, such as an ISECOM Licensed Auditor, requires more effort however.

Upgrading from Older Versions

If you are familiar with the OSSTMM 2.x series then you will find that the methodology has completely changed here and that the RAVs will provide a factual attack surface metric instead of a risk rating. There are many other changes and enhancements as well but the primary focus has been to move away from solution-based testing which assumes specific security solutions will be found in a scope and are required for security (like a firewall). Another change you may notice is that there is now a single security testing methodology for all channels: Physical, Wireless, Telecommunications, Human, and Data Networks.

The RAV information from 2.x to 3.0 is incompatible. Those with early 3.0 draft RAVs (prior to RC 12) will require that the values be re-calculated using this final RAV calculation and available as a spreadsheet calculator at http://www.isecom.org/ravs. Previous RAVs measured risk with degradation however this version does not. Instead, the focus now is on a metric for the attack surface (the exposure) of a target or scope. This allows for a factual metric that has no bias or opinion like risk does.

Much of the terminology has changed in this version to provide a professional definition of that which can actually be created or developed. This is most notable in definitions for security and safety which take more specific and concrete meanings for operations within.

Since so much has changed from previous versions, as this is a completely re-written methodology, we recommend you read through it once before using it. Further help is available at http://www.isecom.org. Courses to help you make proper, thorough, and professional security tests, systems, and processes are available through ISECOM and will help you get the most of the OSSTMM.

Version Information

This is an introduction to the Open Source Security Testing Methodology Manual (OSSTMM) 3.0. The full version of this manual includes the Risk Assessment Values for the quantification of security, the Rules of Engagement for driving a proper test, four additional Channel tests (Wireless, Physical, Telecommunications, and Human), Error Types, and a detailed testing process. It is currently available to contributors and team members at www.isecom.org. A full, free, public release of OSSTMM 3.0 will be made once it has been finalized.

The original version was published on Monday, December 18, 2000. This current version is published on Saturday, August 2, 2008.

About this Project

This project is maintained by the Institute for Security and Open Methodologies (ISECOM), developed in an open community, and subjected to peer and cross-disciplinary review. This project, like all ISECOM projects, is free from commercial and political influence. Financing for all ISECOM projects is provided through partnerships, subscriptions, certifications, licensing, and case-study-based research. ISECOM is registered in Catalonia, Spain as a Non-Profit Organization and maintains a business office in New York, USA.

Reader evaluation of this document, suggestions for improvements, and results of its application for further study are required for development. Contact us at www.isecom.org to offer research support, review, and editing assistance.

Restrictions

Foreword

Security verification used to require cross-disciplinary specialists who understood security as deeply as they understood the rules, laws, underlying premise, operation, process, and technology involved. Sometime later, third party verification came from the popular notion of builder blindness that says those closest to the target will generally and usually involuntarily miss the most problems. This became the standard procedure for a while and is still widely regarded as true even though it actually means that an outsider with less knowledge of the target is supposedly more capable of understanding that target than the operator. At some point, the pendulum began to swing back the other way. Whether this happened for either efficiency or economic reasons is unclear, but it has brought about an important shift to provide the operators with security testing ability. It has led to simplified frameworks, software, checklists, toolkits, and many other ways to make security testing easy enough that anyone can do it. And that's a good thing.

Unfortunately, there is no complex subject for which the simplification process is not itself complex nor the end result significantly less than the whole. This means that to make a security testing solution simple enough for non-experts to execute, the solution requires a complex back-end to collect the data according to preconceived rules. This assumes that operations always run according to design and configuration. It also assumes the solution developer has taken into account all the possibilities for where, what, and how data can be gathered. Furthermore it assumes that the data gathered can be properly sorted into a uniform format for comparison and rule-based analysis. None of those tasks are simple.

Assuming that can be done, it would still require an exhaustive database of possibilities for the numerous representations of security and layers of loss controls to deduce security problems. While minimizing false positives through correlations based on the rules, laws, underlying premise, operation, process, and technology involved. This solution could then be able to provide a clear, concise report and metric. And this solution would need to have more than just the framework, software, checklist, or toolkit which it produces; it would need a methodology.

A security methodology is not a simple thing. It is the back-end of a process or solution which defines what or who is tested as well as when and where. It must take a complex process and reduce it into elemental processes and sufficiently explain the components of those processes. Then the methodology must explain the tests for verifying what those elemental processes are doing while they are doing, moving and changing. Finally, the methodology must contain metrics both to assure the methodology has been carried out correctly and to comprehend or grade the result of applying the methodology. So, making a security testing methodology is no small feat.

With each new version of the OSSTMM we get closer to expressing security more satisfactorily than previous versions. It's not that this OSSTMM 3 promotes revolutionary ideas but rather it applies many new pragmatic concepts which will improve security. We are coming ever closer to truly understanding what makes us safe and secure.

For a chance of having this enlightenment, I want to thank all the contributors to the OSSTMM, the ISECOM team, all OPST and OPSA students who care about the right way to do security testing, all those teaching Hacker Highschool to the next generation, all supporters of the ISECOM projects including the ISECOM Partners and Affiliates, and finally my very patient and supportive wife who understands how important this is to me and to the world we need to improve.

Thank you all for all your help.

Pete Herzog

Managing Director, ISECOM

Table of Contents

Introduction to the OSSTMM

The Open Source Security Testing Methodology Manual (OSSTMM) provides a methodology for a thorough security test, here referred to as an OSSTMM audit. An OSSTMM audit is an accurate measurement of security at an operational level that is clear of assumptions and anecdotal evidence. As a methodology it is designed to be consistent and repeatable. As an open source methodology, it allows for free dissemination of information and intellectual property.

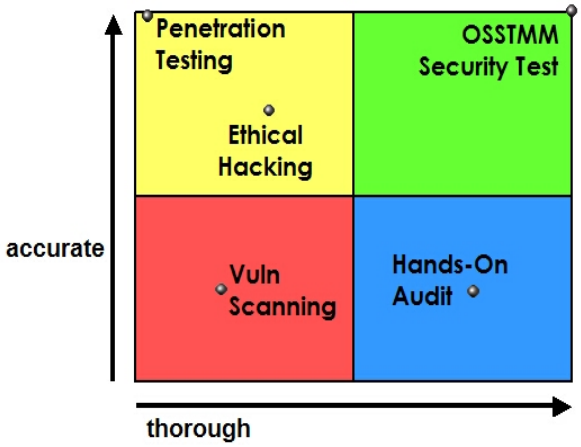
Since its start at the end of 2000, the OSSTMM quickly grew to encompass all security channels with the applied experience of thousands of reviewers. By 2005, the OSSTMM was no longer considered just an ethical hacking framework. It had become a methodology to assure security was being done right at the operational level. As audits became mainstream, the need for a solid methodology became critical. In 2006, the OSSTMM changed from defining tests based on solutions such as firewall tests and router tests to a standard for those who needed a reliable security test rather than just a compliance report for a specific regulation or legislation.

With Version 3, the OSSTMM encompasses tests from all channels - Human , Physical, Wireless, Telecommunications, and Data Networks. A set of security metrics, called Risk Assessment Values (RAVs), provide a powerful tool that can provide a graphical representation of state, and show changes in state over time. This integrates well with a 'dashboard' for management and is beneficial for both internal and external testing, allowing a comparison/combination of the two. Quantitative Risk Management can be done from the OSSTMM Audit report findings, providing a much improved result due to more accurate, error free results. The OSSTMM includes information for project planning, quantifying results, and the rules of engagement for performing security audits. The methodology can be easily integrated with existing laws and policies to assure a thorough security audit through all channels.

It is recommended that you read through the OSSTMM once completely before putting it into practice. It aims to be a straight-forward tool for the implementation and documentation of a security test. Further assistance for those who need help in understanding and implementing this methodology is available at the ISECOM website.

Purpose

The primary purpose of this manual is to provide a scientific methodology for the accurate characterization of security through examination and correlation of test results in a consistent and reliable way. This manual is adaptable to almost any audit type, including penetration tests, ethical hacking, security assessments, vulnerability assessments, red-teaming, blue-teaming, and so forth. It is written as a security research document and is designed for factual security verification and presentation of metrics on a professional level.



A secondary purpose is to provide guidelines which, when followed correctly, will allow the auditor to perform a certified OSSTMM audit. These guidelines exist to assure the following:

1. The test was conducted thoroughly.
2. The test included all necessary channels.
3. The posture for the test complied with the law.
4. The results are measurable in a quantifiable way.
5. The results are consistent and repeatable.
6. The results contain only facts as derived from the tests themselves.

An indirect benefit of this manual is that it can act as a central reference in all security tests regardless of the size of the organization, technology, or protection.

Document Scope

The scope of this document is to provide specific descriptions for operational security tests over all channels- Physical, Human, Telecommunications, Wireless, and Data Networks- over any vector, and the description of derived factual metrics.

Intended Audience

Although many of the concepts in this manual are explained well enough so that any competent professional can test security within their area of expertise, the intended audience is comprised of auditors of information systems, security testers, and security analysts.

Related Terms And Definitions

This manual uses specific words and terms that may have unfamiliar meanings. This is especially true with international translations. Therefore all translations of this manual must include the original term in English with the attempted translation. This manual also uses standard terms and definitions as found in international testing vocabularies and is based on NCSC-TG-004 (Teal Green Book) from the U.S. Department of Defense. For specific tasks where no definition exists, this manual will describe the task as clearly as possible to avoid any misleading interpretation.

Liability

This manual describes certain tests which are designed to elicit a response. Should these tests cause harm or damage, the auditor may be liable according to the laws governing the auditor's location as well as the location of the tested systems. ISECOM makes no guarantee as to a harmless outcome of any test. Any auditor applying this methodology cannot hold ISECOM liable for problems which arise during testing. In using this methodology, the auditor agrees to assume this liability.

Final Results

Test results are often accompanied by recommended solutions or consulting offers, neither of which is required in an OSSTMM audit. Recommended solutions may be provided as a value-add to a security test but are not considered mandatory. Often, there are no proper solutions based on the limited view an auditor has of the client environment. Therefore, solutions are not required as part of an OSSTMM audit.

Frequently, a test will exceed the limits of a security control. Within an engagement, the auditor must always report the factual current state of security, any limitations within that current state, and any of the processes which caused those limitations of the applied controls and protections.

To measure both the thoroughness of the test and the security of the target, use of this methodology should conclude with the Security Test Audit Report (STAR), available with this manual at the ISECOM website. STAR requires the following information:

1. Date and time of test
2. Duration of test
3. Auditors and analysts involved
4. Test type
5. Scope of test
6. Test Index (method of target enumeration)
7. Channels tested
8. Test Vectors
9. Verified test and metrics calculations of the operational protection levels, loss controls, and security limitations
10. Knowledge of which tests have been completed, not completed, or only partially completed, and to what extent
11. Any issues regarding the test and the validity of the results
12. Test error margins
13. Any processes which influence the security limitations
14. Any unknowns or anomalies

Successful reporting of an OSSTMM audit shows an actual measurement of security and loss controls. Misrepresentation of results in reporting may lead to fraudulent verification of security controls, and an inaccurate security level. For this, the auditor must accept responsibility and limited liability for inaccurate reporting.

Report Certification and Accreditation

To produce an OSSTMM certified test which can receive accreditation for the operational security of the target, a STAR is required to be signed by the auditor(s) or analyst(s) who performed the test. The STAR must also meet the reporting requirements in this manual. The STAR can be submitted to ISECOM for review and official OSSTMM certification. A certified test and an accredited report does not need to show that this entire manual or any specific subsections were followed. It needs only to show what was and was not tested to be applicable for certification.

A certified OSSTMM audit provides the following benefits:

1. Serves as proof of a factual test
2. Holds auditor responsible for the test
3. Provides a clear result to the client
4. Provides a more comprehensive overview than an executive summary
5. Provides understandable metrics

Test review, certification, and accreditation by ISECOM or an accredited third party is subject to further conditions and an operations fee.

Professional Certifications

Anyone who uses this methodology for security testing and analysis and completes a valid STAR is said to have performed an OSSTMM audit and is referred to as an OSSTMM Auditor. However, individual certification is also available through ISECOM for the applied skills in professional security testing, analysis, methodical process, and high ethical standards as outlined in the OSSTMM Rules of Engagement. The OPST (OSSTMM Professional Security Tester), the OPSA (OSSTMM Professional Security Analyst), the OPSE (OSSTMM Professional Security Expert), and OWSE (OSSTMM Wireless Security Expert) are among the official certifications for OSSTMM Auditors showing the knowledge and skills required to properly apply the OSSTMM. More information is available on the ISECOM website.

Certifications of Validation

Organizations
OSSTMM certification is available for organizations or parts of organizations which maintain a quarterly minimum RAV level of 90% and validate an annual STAR from a third-party auditor. Validation of security tests or quarterly metrics are subject to the ISECOM validation requirements to assure consistency and integrity.

Products and Services
OSSTMM evaluation seals are available for products, services, and business processes. This seal defines an operational state of security, privacy, and legislative governance. The successfully evaluated products, services, and processes carry their visible certification seal and RAV score. This allows a purchaser to see precisely the amount and type of change in security that the evaluated solutions present. It removes the guess work from procurement and allows one to find and compare alternative solutions.

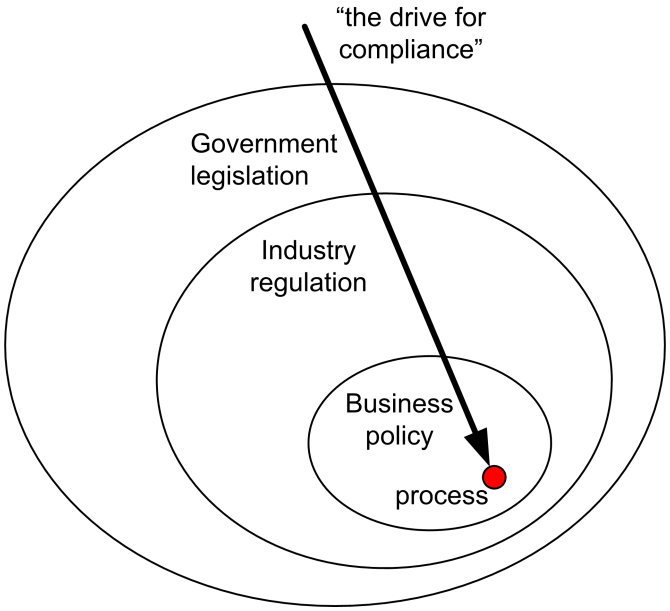
Compliance

Compliance is alignment with a set of general policies, where the type of compliance required depends upon the region and currently ruling government, industry and business types, and supporting legislation. Compliance is compulsory; however, as with any other threat, a risk assessment must be made whether or not to invest in any type of compliance. Often, compliance is not as black and white as it appears to be. The OSSTMM recognizes three types of compliance:

1. Legislation. Compliance with legislation is in accordance to the region where the legislation can be enforced. The strength and commitment to the legislation comes from previously successful legal arguments and appropriately set and just enforcement measures. Failure to comply with legislation may lead to criminal charges.

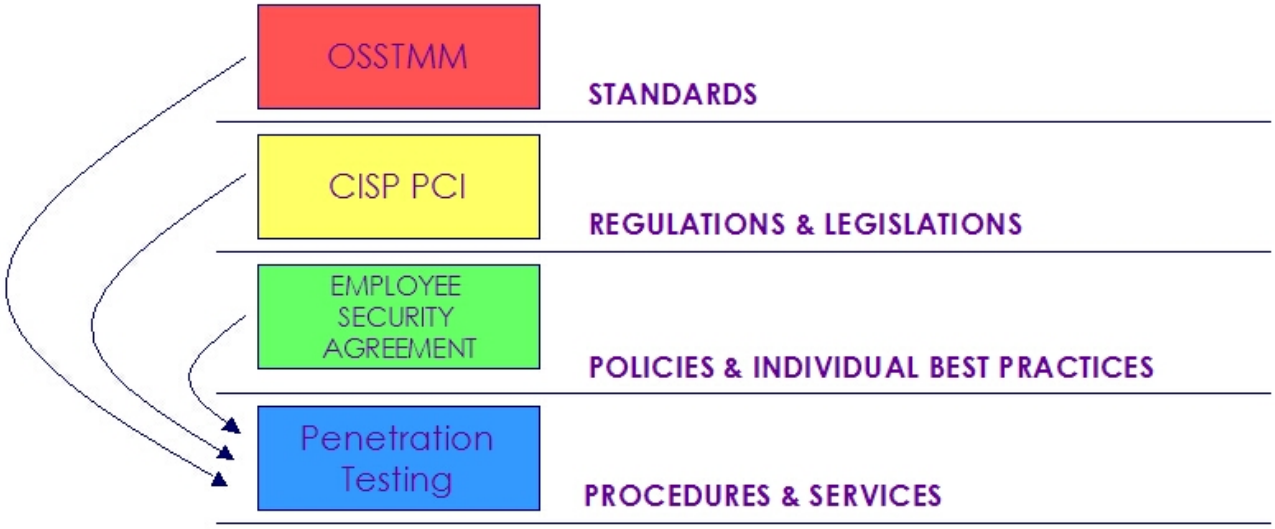
2. Regulation. Compliance to regulation is in accordance to the industry or within the group where the regulation can be enforced. Failure to comply with established regulations often leads to dismissal from the group, a loss of privileges, a monetary fine, civil charges, and in some cases where legislation exists to support the regulatory body, criminal charges.

3. Policy. Compliance to policy is in accordance to the business or organization where the policy can be enforced. Failure to comply with policy often leads to dismissal from the organization, a loss of privileges, a monetary fine, civil charges, and in some cases where legislation exists to support the policy makers, criminal charges.



The OSSTMM is developed with concern for major legislation and regulations. As not all compliance is created equally, the main focus of the OSSTMM is security. Legislation and regulation that detail the purchasing of specific products or services, often through specially lobbied efforts, may have good intentions; however, the OSSTMM cannot directly meet these particular requirements. As legislation and regulation may be audited either under the letter of the law or the spirit of the law, depending upon the auditing body, proof proper and valid operational protection and controls such that as can

be proved by an OSSTMM test may or may not be satisfactory. In cases of a regulation or legislation without priorly tried cases, one cannot know if the letter of the law will trump the spirit of the law. Unfortunately, this is the proof for the case of a risk assessment and whether or not priorly tried judgments of the same issue had acceptable consequences. Therefore, the OSSTMM has also been designed for discovering where elements of special products and services can be determined as to know if another mandated audit will show compliance. In this way, one can meet both the letter and the spirit of the law whenever possible and the two do not conflict.



The following list is only for legislation which has been verified with the OSSTMM and does not limit the actual scope of regulatory and legislative bodies for which this standard may apply, at least in the spirit of the law.

Regulations

Australia

- Privacy Act Amendments of Australia-- Act No. 119 of 1988 as amended, prepared on 2 August 2001 incorporating amendments up to Act No. 55 of 2001. The Privacy Act 1988 (the Privacy Act) seeks to balance individual privacy with the public interest in law enforcement and regulatory objectives of government.
- National Privacy Principle (NPP) 6 provides an individual with a right of access to information held about them by an organization.
- National Privacy Principle (NPP) 4.1 provides that an organization must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorized access, modification or disclosure.
- Commonwealth Privacy Act.

Austria

- Austrian Data Protection Act 2000 (Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000)), specifically the requirements of §14.

Canada

- Privacy Act, 1983.
- Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), 1991.
- Quebec's Act Respecting the Protection of Personal Information in the Private Sector, 1993.
- Personal Information Protection and Electronic Documents Act (PIPEDA), 2000.
- Ontario's Bill 198, 2002.
- Personal Information Protection Act (PIPA), provinces of Alberta and British Columbia, 2004.
- Personal Health Information Protection Act (PHIPA), 2004.

Germany

- Deutsche Bundesdatenschutzgesetz (BDSG)-- Artikel 1 des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes from 20. December 1990, BGBl. I S. 2954, 2955, zuletzt geändert durch das Gesetz zur Neuordnung des Postwesens und der Telekommunikation vom 14. September 1994, BGBl. I S. 2325.
- IT Baseline Protection Manual (IT Grundschutzhandbuch) Issued by Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security (BSI)) available at http://www.bsi.de/gshb/english/menue.htm.
- German IT Systems. S6.68 (Testing the effectiveness of the management system for the handling of security incidents) and tests S6.67 (Use of detection measures for security incidents).

India

- The Information Technology Act, 2000.

Italy

- D.Lgs. n. 196/2003 - Codice in materia di protezione dei dati personali.

Malaysia

- Computer Fraud and Abuse Act.
- The Computer Crimes Act.

Mexico

- Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
- Ley de Propiedad Industrial (LPI).
- Ley Federal de Derechos de Autor (LFDA) and its rules book (RLFDA).
- Código Penal Federal y Código Federal de Procedimientos Penales.

Singapore

- Computer Misuse Act.
- E-Commerce Code for Protection of Personal Information and Communications of Consumers of Internet Commerce.

Spain

- Spanish LOPD Ley Organica de Protección de Datos de Carácter Personal.
- LSSICE 31/2002 (Ley de Servicios de la Sociedad de la Información y el Correo Electronico), July 11, 2002.
- RD 14/1999 (Real Decreto de Regulación de la Firma Electrónica), September 17, 1999.
- RD 994/1999 (Real Decreto sobre el Reglamento de Seguridad de los Ficheros con Información de Carácter Personal), June 11, 1999.

Switzerland

- Bundesverfassung (BV) vom 18. Dezember 1998, Artikel 7 und 13.
- Obligationenrecht (OR) 2002 (Stand am 1. Oktober 2002), Artikel 707, 716, 716b, 717, 727ff und 321a.
- Datenschutzgesetz (DSG) vom 19. Juni 1992 (Stand am 3. Oktober 2000).

Thailand

- Computer Crime Law.
- Privacy Data Protection Law.

United Kingdom

- UK Data Protection Act 1998.
- Corporate Governance requirements.
- IT Information Library available at http://www.ogc.gov.uk/index.asp?id=2261 issued by the British Office for Government Commerce (OGC).
- BSI ISO 17799-2000 (BS 7799) - this manual fully complies with all of the remote auditing and testing requirements of BS7799 (and its International equivalent ISO 17799) for information security auditing.
- UK CESG CHECK - specifically the CESG IT Health CHECK service.

United States of America

- AICPA SAS 70 - verifications of process control activities are applicable to the Service Auditor's Report in the Statement on Auditing Standards (SAS) no. 70 from the American Institute of Certified Public Accountants guidance for Internal Auditors.
- Clinger-Cohen Act.
- Government Performance and Results Act.
- FTC Act, 15 U.S.C. 45(a), Section 5(a).
- Children's Online Privacy Protection Act (COPPA).
- Anticybersquatting Protection Act (ACPA).
- Federal Information Security Management Act.
- U.S. Sarbanes-Oxley Act (SOX).
- California Individual Privacy Senate Bill – SB1386.
- USA Government Information Security Reform Act of 2000 section 3534(a)(1)(A).
- MITRE Common Vulnerabilities and Exposures - the RAV Security Limitations described within this manual comply to the CVE descriptions for more efficient categorizations (http://cve.mitre.org/about/terminology.html).
- DoD FM 31-21, Guerrilla Warfare and Special Forces Operations.
- Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- OCR HIPAA Privacy TA 164.502E.001, Business Associates [45 CFR §§ 160.103, 164.502(e), 164.514(e)].
- OCR HIPAA Privacy TA 164.514E.001, Health-Related Communications and Marketing [45 CFR §§ 164.501, 164.514(e)].
- OCR HIPAA Privacy TA 164.502B.001, Minimum Necessary [45 CFR §§ 164.502(b), 164.514(d)].
- OCR HIPAA Privacy TA 164.501.002, Payment [45 CFR 164.501].
- HIPAA Standards for Privacy of Individually Identifiable Health Information (45 CFR parts 160 and 164).
- FDA: Computerized Systems used in Clinical Trails. Electronic Records; Electronic Signatures; [21 CFR Part 11].

- U.S. Gramm-Leach-Bliley Act (GLBA).

NIST Publications

The OSSTMM has matched compliance through methodology in remote security testing and auditing as per the following National Institute of Standards and Technology (NIST) publications:

- An Introduction to Computer Security: The NIST Handbook, 800-12.
- Guidelines on Firewalls and Firewall Policy, 800-41.
- Information Technology Security Training Requirements: A Role- and Performance-Based Model, 800-16.
- Guideline on Network Security Testing, 800-42.
- Security Self-Assessment Guide for Information Technology Systems.
- PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does, 800-24.
- Risk Management Guide for Information Technology Systems, 800-30.
- Intrusion Detection Systems, 800-31.
- Building an Information Technology Security Awareness and Training Program, 800-50.
- DRAFT NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.
- Security Metrics Guide for Information Technology Systems, 800-55.
- Guide for the Security Certification and Accreditation of Federal Information Systems, 800-37.
- DRAFT: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 800-66.

Federal Financial Institutions Examination Council (FFIEC):

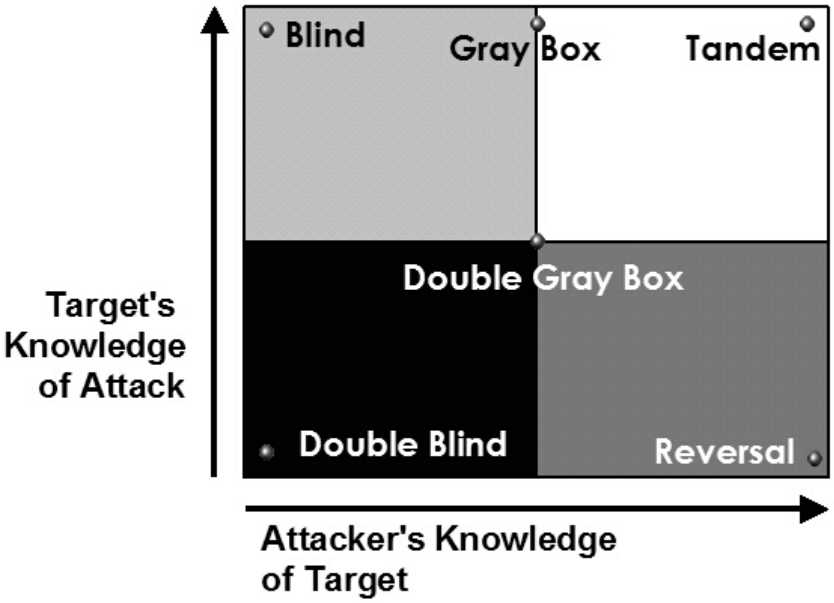
- Electronic Operations, 12 CFR Part 555.
- Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 12 CFR 570 Appendix B.
- Interagency Guidelines Establishing Standards for Safety and Soundness, 12 CFR 570, Appendix A.
- Privacy of Consumer Financial Information, 12 CFR 573.
- Procedures for Monitoring Bank Secrecy Act Compliance, 12 CFR 563.177.
- Security Procedures Under the Bank Protection Act, 12 CFR 568.
- Suspicious Activity Reports and Other Reports and Statements, 12 CFR 563.180.

General

- Payment Card Industry (PCI) Data Security Requirements Version 1.0 December 15, 2004.
- SAC - this manual is compliant in design to the The Institute of Internal Auditors (IIA) Systems Assurance and Control (SAC) model.
- ITIL - this manual is applicable to the operational security controls review and processes inter-relations according to the IT Infrastructure Library (ITIL).

Security Test Types

"Security Testing" is an umbrella term to encompass all forms and styles of security tests from the intrusion to the hands-on audit. The application of the methodology from this manual will not deter from the chosen type of testing.



However, as a standard, this methodology is not to be followed "off-the-shelf". Practical implementation of the OSSTMM requires defining individual testing practices to meet the requirements defined here. This means that even when following this methodology, your application of it and your technique will reflect the type of test you have chosen. Test types may be, but aren't limited to, one of these six common types:

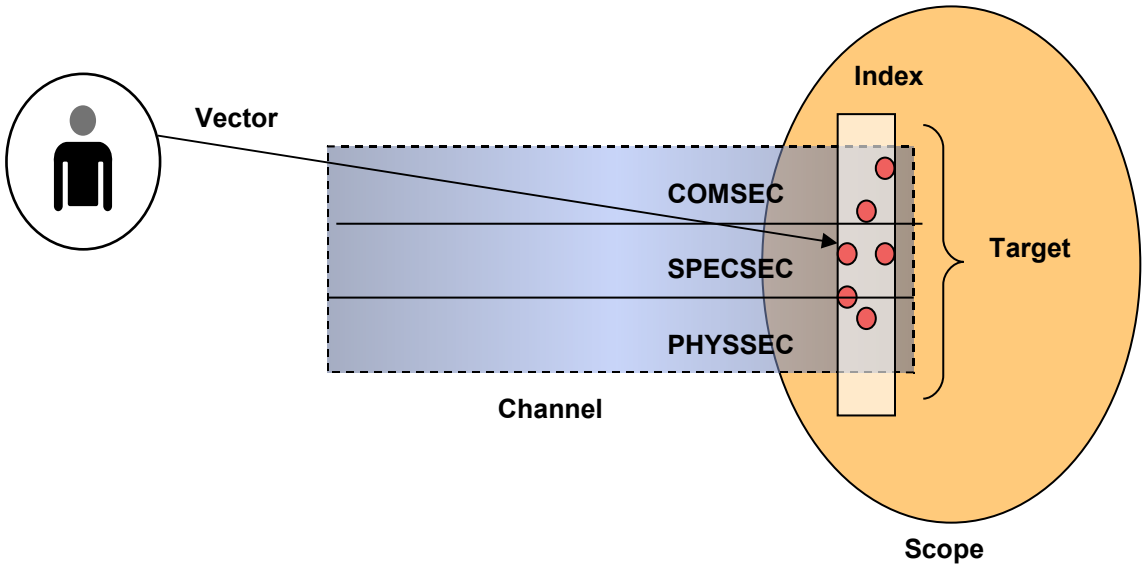
1	**Blind**	The auditor engages the target with no prior knowledge of its defenses, assets, or channels. The target is prepared for the audit, knowing in advance all the details of the audit. A blind audit primarily tests the skills of the auditor. The breadth and depth of a blind audit can only be as vast as the auditor's applicable knowledge and efficiency allows. In COMSEC and SPECSEC, this is often referred to as Ethical Hacking and in other PHYSSEC and HUMSEC channels, this is generally scripted as War Gaming or Role Playing.
2	**Double Blind**	The auditor engages the target with no prior knowledge of its defenses, assets, or channels. The target is not notified in advance of the scope of the audit, the channels tested, or the test vectors. A double blind audit tests the skills of the auditor and the preparedness of the target to unknown variables of agitation. The breadth and depth of a blind audit can only be as vast as the auditor's applicable knowledge and efficiency allows. This is also known as a Black Box Audit or Penetration Test.

3	**Gray Box**	The auditor engages the target with limited knowledge of its defenses and assets and full knowledge of channels. The target is prepared for the audit, knowing in advance all the details of the audit. A gray box audit tests the skills of the auditor and the preparedness of the target to unknown variables of agitation. The nature of the test is efficiency. The breadth and depth depends upon the quality of the information provided to the auditor before the test as well as the auditor's applicable knowledge. This type of test is often referred to as a Vulnerability Test and is most often initiated by the target as a self-assessment.
4	**Double Gray Box**	The auditor engages the target with limited knowledge of its defenses and assets and full knowledge of channels. The target is notified in advance of the scope and time frame of the audit but not the channels tested or the test vectors. A double gray box audit tests the skills of the auditor and the target's preparedness to unknown variables of agitation. The nature of the test is efficiency. The breadth and depth depends upon the quality of the information provided to the auditor and the target before the test as well as the auditor's applicable knowledge. This is also known as a White Box Audit.
5	**Tandem**	The auditor and the target are prepared for the audit, both knowing in advance all the details of the audit. A tandem audit tests the protection and controls of the target. However, it cannot test the preparedness of the target to unknown variables of agitation. The true nature of the test is thoroughness as the auditor does have full view of all tests and their responses. The breadth and depth depends upon the quality of the information provided to the auditor before the test (transparency) as well as the auditor's applicable knowledge. This is often known as an In-House Audit or a Crystal Box Audit and the Auditor is often part of the security process.
6	**Reversal**	The auditor engages the target with full knowledge of its processes and operational security, but the target knows nothing of what, how, or when the auditor will be testing. The true nature of this test is to audit the preparedness of the target to unknown variables and vectors of agitation. The breadth and depth depends upon the quality of the information provided to the auditor and the auditor's applicable knowledge and creativity. This is also often called a Red Team exercise.

In the event of reporting the audit, it is required to identify exactly the type of audit performed. Too often, audits of different test types are compared to track the delta (deviations) from an established baseline of the scope. If the precise test type is not available to a third-party reviewer or regulator, the audit itself should be considered a Blind test, which is one with the least merit towards a thorough security test.

The Scope

The scope is the total possible operating security environment for any interaction with any asset which may include the physical components of security measures as well. The scope is comprised of three channels: COMSEC (communications security), PHYSSEC (physical security), and SPECSEC (spectrum security). Channels are the means of interacting with assets. An asset is what has value to the owner. Assets can be physical property like gold, people, blueprints, laptops, the typical 900 MHz frequency phone signal, and money, or intellectual property such as personnel data, a relationship, a brand, business processes, passwords, and something which is said over the 900 MHz phone signal. The scope is where interactivity can occur with a channel, whether passive like snooping or active like stealing. Often, the scope extends far beyond the reach of the asset owner as dependencies are beyond the asset owner's ability to provide for independently. The scope requires that all threats be considered possible, even if not probable. Although, it must be made clear that a security audit often restricts parameters to that which is within a certain risk range and ignores the remote risks like a volcano eruption where no volcano exists, the non-impacting like moonlight through the window into the data center, or the global-impacting such as a catastrophic meteor shower.



While a thorough security audit requires testing all three channels, realistically, audits are conducted and categorized by the required expertise of the auditor and the required equipment for the audit. This manual addresses these three channels in five logical sections:

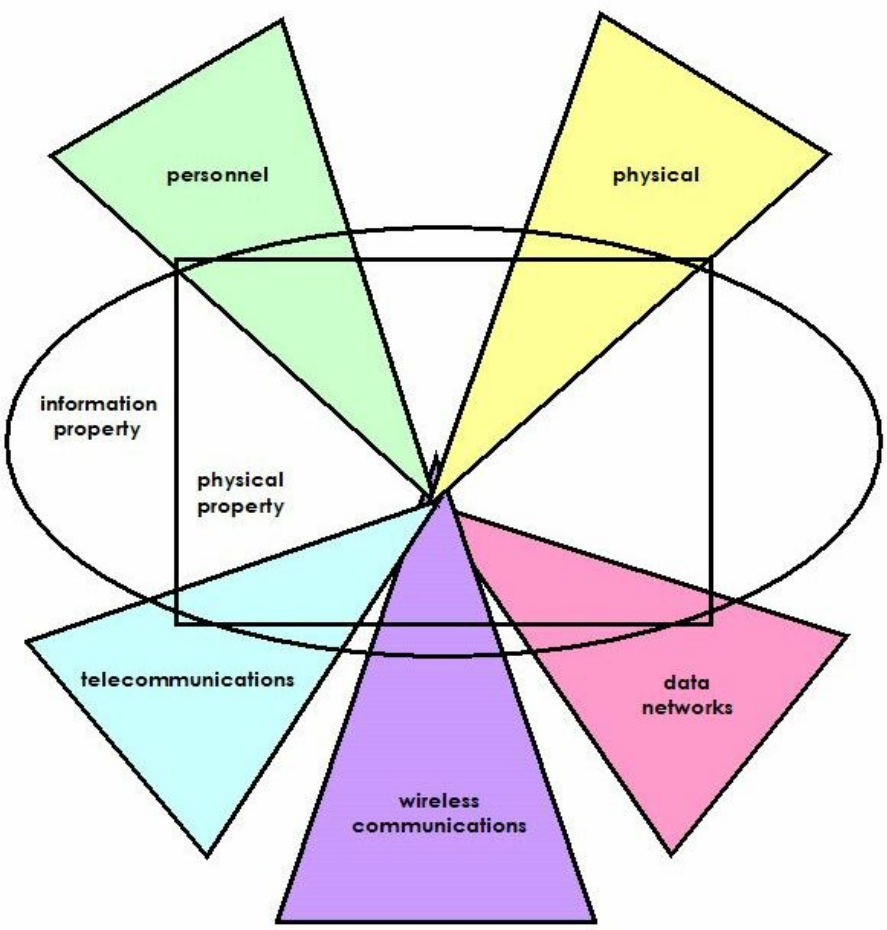


Table 1, OSSTMM Channel / Section Descriptions

Channel	OSSTMM Section	Description
PHYSSEC	Human	Comprises the human element of communication where interaction is either physical or psychological.
	Physical	Physical security testing where the channel is both physical and non-electronic in nature. Comprises the tangible element of security where interaction requires physical effort or an energy transmitter to manipulate.
SPECSEC	Wireless Communications	Comprises all electronic communications, signals, and emanations which take place over the known EM spectrum. This includes ELSEC as electronic communications, SIGSEC as signals, and EMSEC which are emanations untethered by cables.
COMSEC	Data Networks	Comprises all electronic systems and data networks where interaction takes place over established cable and wired network lines.
	Telecommunications	Comprises all telecommunication networks, digital or analog, where interaction takes place over established telephone or telephone-like network lines.

While the channels and their divisions may be represented in any way, within this manual they are organized as recognizable means of communication and interaction. This organization is designed to facilitate the test process while minimizing the inefficient overhead that is often associated with strict methodologies.

Modules

The OSSTMM flow begins with a review of the target's posture. The posture is the culture, rules, norms, regulations, legislation, and policies defining the target. It ends with result comparisons to any alarms, alerts, reports, or access logs. This is a full-circle concept where the first step is to be aware of the operational requirements for interacting with the target, and the last one is the review of the records of the audit trail. For the auditor, this is simply: you know what you need to do, you do it, and then you check what you have done.

This methodology separates the "doing" in a hierarchal format:

CHANNEL > MODULE > TASK

The "doing" is described in the module description for each particular channel audit. Some audits apply to technologies which may straddle the border between two or more channels. For example, commonly found wireless LANs must be tested under both the COMSEC data networks channel and the SPECSEC wireless communications channel. This is why a properly defined testing scope is so important. Channel hybridization is a constant and should not be overlooked. The OSSTMM is fully capable of a "sidewalk to kernel" security audit and therefore is completely capable of applying an audit to a target whether the audit's channels are clearly distinct and separate or comprised of multiple channels. Therefore, for all targets, the auditor should anticipate the need to define an audit to include multiple channels. Sometimes only under investigation will it become evident whether the scope contains any targets under a particular channel or if the auditor will miss targets only available under other channels.

This methodology applies to all five channels and sub-channels. It has 17 modules and all the same

properties apply to all five channels and sub-channels. While the methodology itself may be the same, each channel differs in tasks.

Each module has an input and an output. The input is the information used in performing each task. The output is the result of completed tasks. This output may or may not be intelligence (analyzed data) to serve as an input for another module and this output may further serve as the input for more than one module or section. Therefore, failure to complete certain modules or tasks may limit the successful completion of other modules or tasks. This would limit the thoroughness of the audit far more than just an accounting for the missing tasks would reveal.

Some tasks yield no output, meaning that modules will exist for which there is no input. Modules which have no input can be ignored during testing but must be later documented with an explanation for not having been performed. Also, tasks with no output do not necessarily indicate an inferior test; rather, they may indicate superior security. In detail, tasks that have no resulting output can mean one of five things:

1. The channel was obstructed in some way during the performing of the tasks.
2. The tasks were not properly performed.
3. The tasks were not applicable.
4. The task result data has been improperly analyzed.
5. The task reveals superior security.

It is important that impartiality and open-mindedness exist in performing the tasks of each module. The primary tenet for auditing states, in similar regard to a conformational bias: "When one searches for something, one expects to find it, which may lead you to finding only what you are searching for." In the OSSTMM, each module begins as an input and ends as an output exactly for the reason of keeping bias minimal. Therefore, each task gives a direction of what should be revealed to move to another point within the methodology.

A previous risk assessment may be incorporated to determine scope according to vector and channel. A risk assessment should not predetermine which modules need to be performed as they are not independent tests. Modules are parts of a whole and the assumption that any particular module can be omitted is false and will lead to an improper test. However, if there is no input which is required for a particular module, it may be omitted without degrading the quality of the test. The difference is that, in the first case, the module or task is ignored based on an assumption, while in the second the test itself dictated that the module or task cannot be performed.

With the provision of testing as a service, it is important to communicate to the target owner exactly what of the scope has not or will not be tested. This manages expectations and potentially inappropriate risk assurances in the security of a system.

Testing time with the modules is relative to the scope. The scope is not the predefined range of targets, rather it is the targets as determined by channel, test type and vector. This collection of targets is classified according to an index, where each target can be uniquely identified from the test vector. For example, of a group of people, the index may be their employee ID numbers as their names may not be unique. For a network, the index can be the MAC addresses or the IP addresses, depending on the test type and vector. The vector is a quantity of direction in relation to the security of the operations being tested. For example, if the auditor tests the physical security of a door, then the test would have at least two vectors: the door's functional security from the outside of the room to the inside, and then from the inside of the room to the outside. Determining the proper scope based

on vector is important because there may still be targets outside of the vector and still within the scope which will not make up the current testing scope. This combination of channel, test type, vector, and index imposed on the targets is the Audit Scope. Overall, larger scopes with multiple channels and multiple vectors require more time spent on each module and its tasks. The amount of time allowed before returning with output data is not determined by this methodology and depends on the auditor, the target, the test environment, and the audit scope.

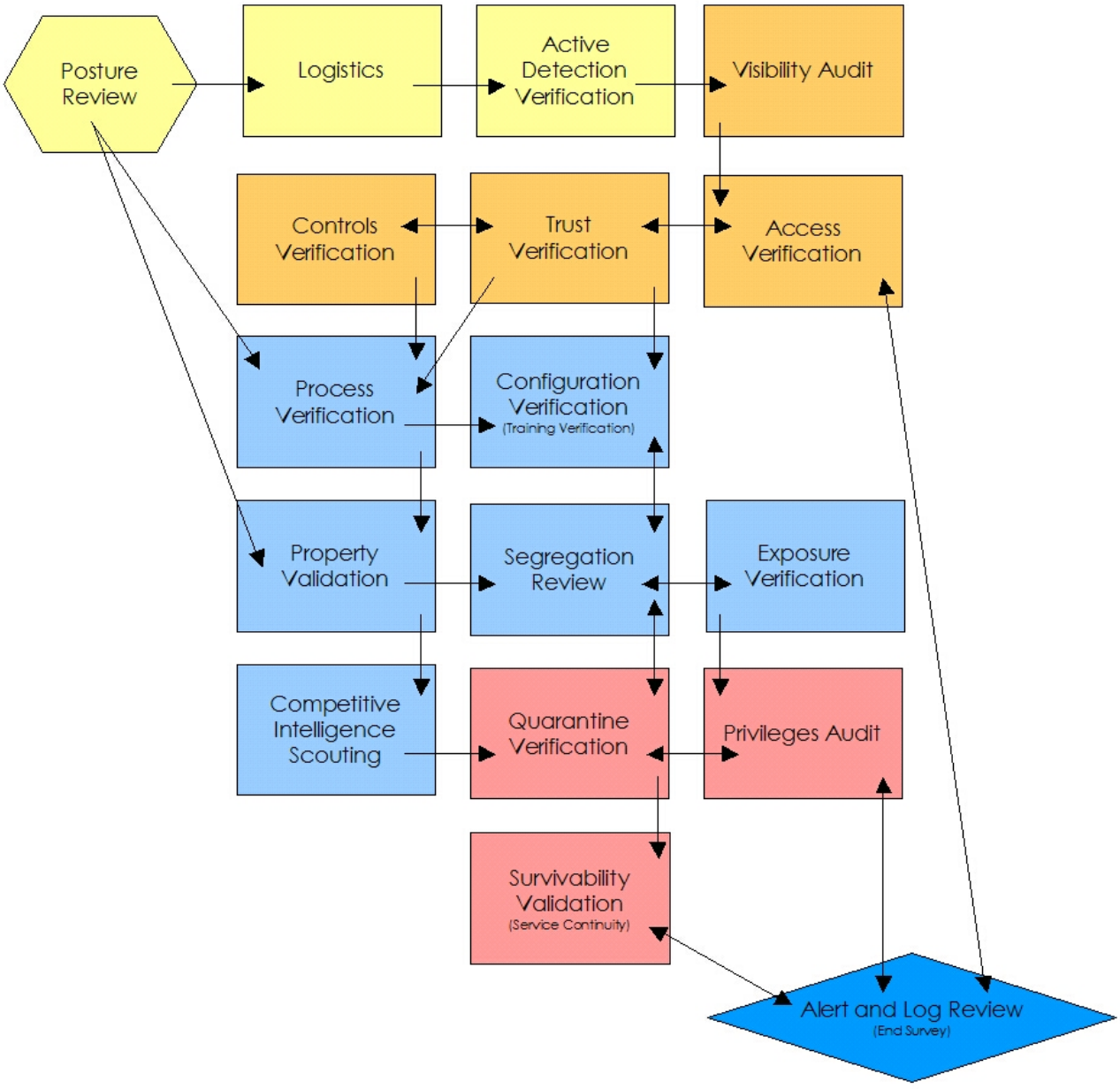
Methodology Flow

The OSSTMM does not allow for a separation between what is considered active data collection and verification through agitation because, in both cases, interaction is required. Nor does it differentiate between active and passive testing where active testing is the agitation to create an interaction with the target and passive testing is the recording, aggregation, and analysis of emanations from the target. This methodology requires both active and passive tests. Furthermore, the auditor may not be able to differentiate between data collected passively from emanations of the operations and that which is the delayed or misdirected response to agitation. e The introduction of any outside event, including the passive kind, has the potential to change the nature of the target's operations and lower the quality of an uninfluenced test on operational security. However, this is not an error of the auditor or the audit process, but simply an unavoidable evil of testing a system in a stochastic environment over a linear time frame. Simply put, the auditor often cannot "take back" the agitation once it has been set in motion and any corrections will cause additional and varied results that do not match the aim of the original task. This is important because it will make it difficult to later compare results. It will also mean that prior tests will influence later tests due to the "memory" of the impact of the test. This is very noticeable in testing over the PHYSSEC channel.

It is important to note that when harmonizing the OSSTMM with other testing standards, it is important not to constrict the flow of this methodology by introducing standards so formal and unrelenting that the quality of the test suffers.

Methodology By Channel

The methodology is made up of 17 test modules per Channel:



Understanding the Test Modules

To choose the appropriate test type, it is best to first understand how the modules are designed to work. Depending on the thoroughness, business, time allotment, and requirements of the audit, the auditor may want to schedule the details of the audit by phase.

There are four phases in the execution of this methodology:

A. Regulatory Phase
B. Definitions Phase
C. Information Phase
D. Interactive Controls Test Phase

Each phase lends a different depth to the audit, but no one phase is less important than another in terms of Actual Security.

Methodology Overview

Module		Description	Explanation
A. Regulatory Phase Every trip begins with a direction. In the regulatory phase, the auditor begins the audit with an understanding of the audit requirements, the scope, and the constraints to the auditing of this scope. Often, the test type is best determined after this phase.			
A.1	Posture Review	The review of the culture, rules, norms, regulations, legislation, and policies applicable to the target.	Know the scope and what tests must be done. Required if Phase C is to be properly conducted.
A.2	Logistics	The measurement of interaction constraints such as distance, speed, and fallibility to determine margins of accuracy within the results.	Know the limitations of the audit itself. This will minimize error and improve efficiency.
A.3	Active Detection Verification	The verification of the practice and breadth of interaction detection, response, and response predictability.	Know the restrictions imposed on interactive tests. This is required to properly conduct Phases B and D.
B. Definitions Phase The core of the basic security test requires knowing the scope in relation to interactions with the targets conveyed to interactions with assets. This phase will define the scope.			
B.4	Visibility Audit	The determination of the applicable targets to be tested within the scope. Visibility is regarded as "presence" and not limited to human sight.	Know what targets exist and how they interact with the scope, if at all. A dead or missing target is also an unresponsive target. However, an unresponsive target is not necessarily a missing target.

	Module	Description	Explanation
B.5	Access Verification	The measurement of the breadth and depth of interactive access points within the target and required authentication.	The access point is the main point of any asset interaction. Verifying an access point exists is one part of determining its purpose. Full verification requires knowing all there is to know about the access point.
B.6	Trust Verification	The determination of trust relationships from and between the targets. A trust relationship exists wherever the target accepts interaction freely and without credentials.	Trusts for new processes are often very limited where older processes have a seemingly chaotic evolution to the outsider. Knowing trust relationships between targets will show the age or value of the interaction.
B.7	Controls Verification	The measurement of the use and effectiveness of the process-based (Class B) loss controls: non-repudiation, confidentiality, privacy, and integrity. The control of alarm is verified at the end of the methodology.	Most processes are defined in response to a necessary interaction and some remain long after that interaction stops or has changed. Knowing what process controls are in place is a type of security archeology.
C. Information Phase Much of security auditing is about the information that the auditor uncovers. In this phase, the various types of value and detriment of misplaced and mismanaged information as an asset are brought to light.			
C.8	Process Verification	The determination of the existence and effectiveness of the record and maintenance of existing actual security levels and/or diligence defined by the posture review and indemnification controls.	Know the controllers and their routines for the controls. Most processes will have a defined set of rules, however actual operations reflect any efficiency, laziness, or paranoia which may redefine the rules. So it's not just that the process is there but also how it works.
C.9	Configuration Verification Training Verification (HUMSEC)	The research of the steady state (normal operation) of the targets as they have been designed to operate under normal conditions to determine underlying problems outside of the application of security stress tests.	This module explores the default conditions under which the targets operate regularly to understand the intent, business justification, and reasoning for the targets. Additionally, many regulations require information regarding how something is planned to work and this is not always evident in the execution of that work.
C.10	Property Validation	The measurement of the breadth and depth in the use of illegal and/or unlicensed intellectual property or applications within the target.	Know the status of property ownership rights.
C.11	Segregation Review	A determination of the levels of personally identifiable information defined by the posture review.	Know which privacy rights apply and to what extent the uncovered personally identifiable information can be classified based on these requirements.

	Module	Description	Explanation
C.12	Exposure Verification	The search for freely available information which describes indirect visibility of targets or assets within the chosen channel of the scope.	The word on the street has value. Uncover information on targets and assets from public sources including that from the targets themselves.
C.13	Competitive Intelligence Scouting	The search for freely available information, directly or indirectly, which could harm or adversely affect the target owner through external, competitive means.	There may be more value in the information from processes and targets than the assets which they are protecting. Uncover information that by itself or in aggregate can influence competitive business decisions.
D. Interactive Controls Test Phase These tests are focused on penetration and disruption. This is often the final phase of a security test to assure disruptions do not affect responses of less invasive tests and because the information for making these tests may not be known until other phases have been carried through. The final module, D17, of Alert and Log Review, is required to verify that prior test assumptions are true. Most security tests that do not include this phase may still need to run an end review from the vector of the targets and assets to clarify disruptions that did not respond during standard echo tests.			
D.14	Quarantine Verification	The determination and measurement of effective use of quarantine for all access to and within the target.	Determine the effectiveness of authentication and subjugation controls in terms of black and white list quarantines.
D.15	Privileges Audit	The mapping and measurement of the impact of misuse of subjugation controls, credentials and privileges or the unauthorized escalation of privilege to a higher level privilege.	Determine the effectiveness of authorization on authentication, indemnification, and subjugation controls in terms of depth and roles.
D.16	Survivability Validation Service Continuity (HUMSEC)	The determination and measurement of the resistance of the target to excessive or adverse changes where continuity and resilience controls would be impacted.	Determine the effectiveness of continuity and resistance controls through the verification of denial of service and denial of interactivity.
D.17	Alert and Log Review End Survey (HUMSEC)	A review of audit activities performed with the true depth of those activities as recorded by the target or from a third-party as in the control of alarm.	Know what parts of the audit left a usable and reliable trail.

Testing Data Networks

COMSEC

The tests for the Computer Security (COMSEC) channel require interactions with the existing data communication network operational safeguards used to control access to property.

This channel covers the involvement of computer systems, primarily the operating networks within the target scope or framework. While some services consider this simply as "penetration testing", the true compliance objective of security testing in this channel is system interaction and operational quality testing with gap measurements to the required security standard outlined in company policy, industry regulations, and/or regional legislation.

During testing, end operators and artificial intelligence can recognize on-going attacks both by process and signature. For this reason, the auditor will be required to have a sufficient variety of methods to avoid disclosure of the tests or work with the operators to assure that where security fails and where it succeeds is brought to light. Tests which focus only on problems foster fixes and do not leave room to design for future success.

Competent auditors will require adequate networking knowledge, diligent security testing skills, and critical thinking skills to assure factual data collection creates factual results through correlation and analysis.

Considerations

Please note the following considerations to assure a safe, high quality test:

1. Ignorantia legis neminem excusat: auditors who do not do proper posture review for the scope as well as the regions targeted for business or interactions may not escape punishment for violating laws merely because they were unaware of the law; that is, persons have presumed knowledge of the law. Auditors are considered professionals in this subject matter and, therefore, the assumption exists that what may not be common knowledge for a normal person about a foreign region's laws regarding computer systems, professionals make themselves aware of the laws necessary to engage in that undertaking.

2. Property rights: Testing must specifically target only systems which are under direct legal ownership with the scope owner and computer systems on the property of the scope owner.Any personal effect should remain personal and private unless it specifically involves the scope owner through disparagement, false light, competitiveness, or reasons stated in personnel contract agreements. Auditors must make efforts to not invade upon a person's private life where that private life has made efforts to separate itself from the scope. Auditors with special agreements to test systems which are under direct contract but not owned or are owned but not housed at the owner's legal property must take great caution to assure tests have minimum impact on other systems outside the scope or contract.

3. Quality: Tests should not be made where quality is assumed through quantity. Testing against a target by trying a large number of problems is not the same as a quality test. A quality test does not regard the number of exploits or vulnerabilities one has to work with but rather in

recognizing when an infrastructure has limitations and in what way.

11.1 Posture Review

Initial studies of the posture include the laws, ethics, policies, industry regulations, and political culture which influence the security and privacy requirements for the scope. This review forms a matrix of which testing has been mapped but not constrained to due to the ubiquity of the channel endpoints. Therefore, it is important to consider, as some legislation requires, the target market or end users of this channel which must also be added to the scope for this module.

11.1.1 Policy

Review and document appropriate organizational policy regarding security, integrity, and privacy requirements of the scope. Review and document contracts and Service Level Agreements (SLAs) with service providers and other involved third parties.

11.1.2 Legislation and Regulations

Review and document appropriate regional and national legislation and industry regulations regarding the security and privacy requirements of the organization in the scope as well as that which includes the appropriate customers, partners, organizational branches, or resellers outside the scope.

11.1.3 Culture

Review and document appropriate organizational culture in the scope towards security and privacy awareness, required and available personnel training, organizational hierarchy, help desk use, and requirements for reporting security issues.

11.1.4 Age

Review and document the age of systems, software, and service applications required for operations.

11.1.5 Fragile Artifacts

Review and document any systems, software, and service applications which require special care due to high use, instabilities, or a high rate of change.

11.2 Logistics

This is the preparation of the channel test environment needed to prevent false positives and false negatives which lead to inaccurate test results.

11.2.1 Framework

(a) Verify the scope and the owner of the targets outlined for the audit.
(b) Determine the property location and the owner of the property housing the targets.
(c) Verify the owner of the targets from network registration.
(d) Verify the owner of the target domains from domain registration information.
(e) Verify the ISP(s) providing network access and/or redundancy.
(f) Search for other IP blocks and targets from the same owner.
(g) Search for similar domain names or mistyped domain names which can be confused with the target.
(h) Verify which target domain names resolve to systems outside of the owner's control such as caching devices.
(i) Verify which target IP addresses trace back to locations different from the owner's location.
(j) Verify that reverse name look-ups of target system addresses correspond with the scope and the scope owner.
(k) Find and verify the paths of network services which interact outside of target for the paths they follow into and out of the scope.
(l) Determine the physical location of the targets.
(m) Prepare local name resolution to map domain names only to the specific systems to be tested and not any devices outside the target or target ownership.
(n) Use reverse name lookups to determine the existence of all the machines in a network.

11.2.2 Network Quality

(a) Measure the rate of speed and packet loss to the scope for a requested service in TCP, UDP, and ICMP both as a whole service request and as a request/response pair. Repeat each request in succession at least 100 times and record the average for both whole service requests and packet responses for each of the three protocols.
(b) Determine sending and receiving packet rates for a total of 6 averages (per protocol) as requests per second per network segment in the scope.
(c) Record packet loss percentages for the determined packet sending and receiving rates.

11.2.3 Time

(a) Verify time zone, holidays, and work schedules for the various systems within the scope including partners, resellers, and influential customers interacting with the scope.
(b) Identify the TTL distance to the gateway and the targets.
(c) Assure the auditor's time clock is in sync with the time of the targets.

11.3 Active Detection Verification

Determination of active and passive controls to detect intrusion to filter or deny test attempts must be made prior to testing to mitigate the risk of corrupting the test result data as well as changing the alarm status of monitoring personnel or agents. It may be necessary to coordinate these tests with the appropriate persons within the scope.

11.3.1 Filtering

(a) Test whether INCOMING network data or communications over web, instant messaging, chat, web-based forums, or e-mail, are monitored or filtered by an authoritative party for relaying improper materials, code injections, malicious content, and improper conduct and record reaction responses and response time.
(b) Test whether OUTGOING network data or communications over web, instant messaging, chat, web-based forums, or e-mail, are monitored or filtered by an authoritative party for relaying improper materials, code injections, malicious content, and improper conduct and record reaction responses and response time.

11.3.2 Active Detection

(a) Verify active responses to probes from systems and services. This could be human or machine readable notifications, packet responses, silent alarm trips, or the like.
(b) Map any applications, systems, or network segments within the scope which produce logs, alarms, or notifications. This could include Network or Host based Intrusion Detection or Prevention Systems, syslog's, Security Information Management tools (SIMs), application logs, and the like.

11.4 Visibility Audit

Enumeration and indexing of the targets in the scope through direct and indirect interaction with or between live systems.

11.4.1 Network Surveying

(a) Identify the perimeter of the network segment.
(b) Query all name servers and the name servers of the ISP and hosting provider, if available, for corresponding A, PTR, and zone transfer records to determine the existence of all targets in the network and any related redundancies, load balancing, caching, proxying, and virtual hosting.
(c) Verify broadcast requests on responses from all targets.
(d) Verify and examine the use of traffic and routing protocols for all targets.
(e) Verify ICMP responses for ICMP types 0-255 and ICMP codes 0-2 from all targets.
(f) Verify default and likely SNMP community names in use are according to practical deployments of all SNMP versions.
(g) Verify responses from targets to select ports with TTL expiration set to 1 and 2 hops:
    TCP 8, 22, 23, 25, 80, 443, 445, 1433
    UDP 0, 53, 139, 161
    ICMP T00:C00, T13:C00, T15:C00, T17:C00
(h) Trace the route of ICMP packets to all targets.
(i) Trace the route of TCP packets to all targets for ports 22, 25, 80 and 443.
(j) Trace the route of UDP packets to all targets for ports 53 and 161.
(k) Identify TCP ISN sequence number predictability for all targets.
(l) Verify IPID increments from responses for all targets.

(m) Verify the use of Loose Source Routing to the target gateway and outer perimeter systems to route packets to all targets.

11.4.2 Enumeration

(a) Search newsgroups, IRC, IM, P2P, VoIP, and web-based communications for connecting information of the target to determine outgoing gateway systems and internal addressing.
(b) Examine e-mail headers, bounced mails, read receipts, mail failures, and malware rejections to determine outgoing gateway systems and internal addressing.
(c) Examine target web-based application source code and scripts to determine the existence of additional targets in the network.
(d) Search web logs and intrusion logs for system trails from the target network.
(e) Verify responses from UDP packet requests to ports 0-65535.
(f) Verify responses to UDP packet requests FROM SOURCE ports 0, 53, 139, and 161 to 0, 53, 69, 131, and 161.
(g) Verify responses to UDP packet requests with BAD CHECKSUMS to ports 0, 53, 69, 131, and 161.
(h) Verify responses to UDP service requests to common remote access trojan ports. (same as e?)
(i) Verify responses from TCP SYN packet requests to ports 0-65535.
(j) Verify responses from TCP service requests to ports 0, 21, 22, 23, 25, 53, 80, and 443.
(k) Verify responses from a TCP ACK with a SOURCE port of 80 to ports 3100-3150, 10001-10050, 33500-33550, and 50 random ports above 35000.
(l) Verify responses from TCP SYN fragments to ports 0, 21, 22, 23, 25, 53, 80, and 443.
(m) Verify responses from all combinations of TCP flags to ports 0, 21, 22, 23, 25, 53, 80, and 443.
(n) Verify the use of all targets with HTTP or HTTPS based VPNs, proxies, and URL redirectors to redirect requests for targets within the scope.
(o) Verify the use of all targets with sequential IPIDs to enumerate systems within the network.
(p) Map and verify for consistency visible systems and responding ports by TTLs.
(q) Verify the use of Loose Source Routing to the target gateway and outer perimeter systems to route packets to all targets.

11.4.3 Identification

(a) Identify targets' TTL response, system uptime, service, application, application faults, and correspond this with the responses from system and service fingerprinting tools.

11.5 Access Verification

Tests for the enumeration of access points leading within the scope.

11.5.1 Access Process

(a) Request known, common services which utilize UDP for connections from all addresses.
(b) Request known, common VPN services including those which utilize IPSEC and IKE for connections from all addresses.

(c) Request known, common Trojan services which utilize UDP for connections from all addresses.
(d) Request known, common Trojan services which utilize ICMP for connections from all addresses.
(e) Request known, common Trojan services which utilize TCP for connections from all addresses and unfiltered ports which have sent no response to a TCP SYN.

11.5.2 Services

(a) Request all discovered TCP ports for service banners (flags).
(b) Verify service banner (flag) through interactions with the service comprising of both valid and invalid requests.
(c) Match each open port to a daemon (service), application (specific code or product which uses the service, and protocol (the means for interacting with that service or application).
(d) Verify server uptime to latest vulnerabilities and patch releases.
(e) Verify the application to the system and the version.
(f) Identify the components of the listening service.
(g) Verify service and application to TTL and OS fingerprint for all addresses.
(h) Verify HTTP and HTTPS for virtual hosting.
(i) Verify VoIP services.

11.5.3 Authentication

(a) Enumerate accesses requiring authentication and document all privileges discovered which can be used to provide access.
(b) Verify the method of authorization and the identification required.
(c) Verify the method of the authentication.
(d) Verify the strength of the authentication through password cracking and re-applying discovered passwords to all access points requiring authentication.
(e) Verify the process for receiving authentication.
(f) Test for logic errors in the application of the authentication.

11.6 Trust Verification

Tests for trusts between systems within the scope where trust refers to access to information or physical property without the need for identification or authentication.

11.6.1 Spoofing

(a) Test measures to access property within the scope by spoofing your network address as one of the trusted hosts.
(b) Verify if available caching mechanisms can be poisoned.

11.6.2 Phishing

(a) Verify that URLs for submissions and queries on the target are concise, within the same domain, use only the POST method, and use consistent branding.

(b) Verify that target content images/records/data does not exist on sites outside of the target to create a duplicate of the target.
(c) Examine top level domain records for domains similar to those identified with the scope.
(d) Verify that the target uses personalization in websites and mail when interacting with authenticated users.
(e) Verify the control and response of the target to mail bounces where the FROM is spoofed in the header field to be that of the target domain.

11.6.3 Resource Abuse

(a) Test the depth of access to business or confidential information available on web servers without any established, required credentials.
(b) Test the if information is sent to the outside of the scope as padding to network packets.
(c) Verify that continuity measures, specifically load balancing, are seamless outside the scope to prevent users from using, referring, linking, bookmarking, or abusing just one of the resources.

11.7 Controls Verification

Tests to enumerate and verify the operational functionality of safety measures for assets and services.

11.7.1 Non-repudiation

(a) Enumerate and test for use or inadequacies from daemons and systems to properly identify and log access or interactions to property for specific evidence to challenge repudiation.
(b) Document the depth of the recorded interaction and the process of identification.
(c) Verify that all methods of interactions are properly recorded with proper identification.
(d) Identify methods of identification which defeat repudiation.

11.7.2 Confidentiality

(a) Enumerate all interactions with services within the scope for communications or assets transported over the channel using secured lines, encryption, "quieted" or "closed" interactions to protect the confidentiality of the information property between the two parties.
(b) Verify the acceptable methods used for confidentiality.
(c) Test the strength and design of the encryption or obfuscation method.
(d) Verify the outer limits of communication which can be protected via the applied method of confidentiality.

11.7.3 Privacy

(a) Enumerate services within the scope for communications or assets transported using specific, individual signatures, personal identification, or "quieted" or "closed room" personal interactions to protect the privacy of the interaction and the process of providing assets only to those within the proper security clearance for that process, communication, or asset.

(b) Correlate information with non-responsive TCP and UDP ports to determine if availability is dependent upon a private type of contact or private protocol.

11.7.4 Integrity

(a) Enumerate and test for inadequacies of integrity where using a documented process, signatures, encryption, hash, or markings to assure that the asset cannot be changed, continued, redirected, or reversed without it being known to parties involved.

11.8 Process Verification

Tests to examine the maintenance of functional security in established processes and due diligence as defined in the Posture Review.

11.8.1 Maintenance

Examine and document the timeliness, appropriateness, access to, and extent of processes for the notification and security response in regards to network and security monitoring.

11.8.2 Misinformation

Determine the extent to which security notifications and alarms can be expanded or altered with misinformation.

11.8.3 Due Diligence

(a) Map and verify any gaps between practice and requirements as determined in the Posture Review through all channels.

11.8.4 Indemnification

(a) Document and enumerate targets and services which are protected from abuse or circumvention of employee policy, are insured for theft or damages, or use liability and permission disclaimers.
(b) Verify the legality and appropriateness of the language in the disclaimers.
(c) Verify the affect of the disclaimers upon security or safety measures.
(d) Examine the language of the insurance policy for limitations on types of damages or assets.

11.9 Configuration Verification

Tests to gather all information, technical and non-technical, on how assets are intended to work, and to examine the ability to circumvent or disrupt functional security in assets, exploiting improper configuration of access controls, loss controls, and applications.

11.9.1 Configuration Controls

(a) Examine controls to verify baseline configurations for OS's, applications and equipment within the scope to validate secure configurations, ensure proper security and best practices.
(b) Examine controls to verify the configurations and baselines of systems, equipment and applications meet the intent of the organization and reflect a business justification.
(c) Examine Access Control Lists (ACLs) and business roles configured on networks, systems, services and applications within the scope to ensure they meet the intent of the organization and reflect a business justification.

11.9.2 Common Configuration Errors

(a) Verify services available are not unnecessarily redundant match the systems' intended business role.
(b) Verify default settings have been changed. Some devices or applications ship with a default or hidden administrative account. These accounts should be changed, or if possible, disabled or deleted and replaced with a new administrative account.
(c) Verify that Administration is done locally or with controls to limit who or what can access the remote port of the equipment.

11.9.3 Awareness Mapping

(a) Map the limitations discovered in security awareness training for personnel through gap analysis with actual procedures including, but not limited to: the provision of property via any channel, the ability to recognize improper and forged identification or required methods, the method of proper identification among personnel, the use of personal security measures for self and property, the handling of confidential and sensitive property, and the conformity to organizational security policy.

11.9.4 Awareness Hijacking

(a) Discover and examine the extent to which a non-official person provides misinformation regarding security policy in an authoritative manner to purposely circumvent or break security policy.

11.10 Property Validation

Tests to examine information and data available within the scope or provided by personnel which may be illegal or unethical.

11.10.1 Sharing

(a) Verify the extent to which individually licensed, private, faked, reproduced, non-free, or non-open property is shared either intentionally through sharing processes and programs, libraries, and personal caches or unintentionally through mismanagement of licenses and resources, or negligence.

11.10.2 Black Market

(a) Verify the extent to which individually licensed, private, faked, reproduced, non-free, or non-open property is promoted, marketed, or sold between personnel or by the organization.

11.10.3 Sales Channels

(a) Verify whether any public, out of scope businesses, auctions, or property sales provide contact information from targets within the scope.

11.11 Segregation Review

Tests for appropriate separation of private or personal information property from business information. Like a privacy review, it is the focal point of the legal and ethical storage, transmission, and control of personnel, partner, and customer private information property.

11.11.1 Privacy Containment Mapping

(a) Map key locations of private information property within the scope, what information is stored, how and where the information is stored, and over which channels the information is communicated.

11.11.2 Disclosure

(a) Examine and document types of disclosures of private information property for segregation according to policy and regulations as determined in the Posture Review.
(b) Verify that private information and confidential intellectual property, such as documents, service contracts, OS/Software keys, etc. are not available to anyone without proper privileges.

11.11.3 Limitations

(a) Verify that design considerations or channel alternatives exist for people with physical limitations to interact with the target.
(b) Identify any parts of the infrastructure designed to interact with children (under 13 years of age) and verify what and how identifying information is provided from that child.

11.11.4 Discrimination

(a) Verify information requested and privileges granted from gatekeepers in cases where age (specifically minors under 13 years of age), sex, race, custom/culture and religion are factors which may be discriminated against in accordance to the Posture Review.

11.12 Exposure Verification

Tests for uncovering information which provides for or leads to access or allows for access to multiple locations with the same authentication.

11.12.1 Exposure Enumeration

(a) Enumerate information regarding the organization such as organization charts, key personnel titles, job descriptions, personal and work telephone numbers, mobile phone numbers, business cards, shared documents, resumes, organizational affiliations, private and public e-mail addresses, logins, login schemes, passwords, back-up methods, insurers, or any particular organizational information stated implicitly as confidential in regulations and policy.
(b) Enumerate system, service and application exposures detailing the design, type, version, or state on the targets or from resources outside the scope such as from postings or leaks.

11.13 Competitive Intelligence Scouting

Tests for scavenging information that can be analyzed as business intelligence. While competitive intelligence as a field is related to marketing, the process here includes any form of competitive intelligence gathering, including but not limited to economic and industrial espionage. Business information includes but is not limited to business relationships like employees, partners, or resellers, contacts, finances, strategy, and plans.

11.13.1 Business Grinding

(a) Enumerate and evaluate access points (gateways) to business property within the scope: what business information is stored, how it is stored, and where the information is stored.

11.13.2 Profiling

(a) Profile and verify the organization, employee skill requirement types, pay scales, channel and gateway information, technologies, and direction from sources outside the scope.
(b) Profile data network set-ups and configurations from job databases and newspapers hiring data networking positions within the organization relating to hardware and software engineering or administration within the target's default business language(s).

11.13.3 Business Environment

(a) Explore and document from individual gateway personnel business details such as alliances, partners, major customers, vendors, distributors, investors, business relations, production, development, product information, planning, stocks and trading, and any particular business information or property stated implicitly as confidential in regulations and policy.
(b) Review third party web notes, annotations, and social bookmark site content made for

the web presence of the scope.

11.13.4 Organizational Environment

(a) Examine and document types of disclosures of business property from gatekeepers on operations, processes, hierarchy, financial reporting, investment opportunities, mergers, acquisitions, channel investments, channel maintenance, internal social politics, personnel dissatisfaction and turn-over rate, primary vacation times, hirings, firings, and any particular organizational property stated implicitly as confidential in regulations and policy.

11.14 Quarantine Verification

Tests for verifying the proper fielding and containment of aggressive or hostile contacts at the gateway points.

11.14.1 Containment Process Identification

(a) Identify and examine quarantine methods for aggressive and hostile contacts such as sales people, head-hunters, grifters, journalists, competitors, job seekers, job candidates, and disruptive persons.

11.14.2 Containment Levels

(a) Verify the state of containment and length of time for quarantine methods both into and out of the scope. Ensure the completeness and thoroughness of the methods and that they are within legal context and boundaries.

11.15 Privileges Audit

Tests where credentials are supplied to the user and permission is granted for testing with those credentials.

11.15.1 Identification

(a) Examine and document the authorization process for obtaining identification from users through both legitimate and fraudulent means on all channels.

11.15.2 Authorization

(a) Examine and verify the means for gaining fraudulent authorization to gain privileges to that of other personnel.
(b) Enumerate the use of default accounts on targets.
(c) Test access to authenticated access points through the most appropriate and available cracking techniques. Password cracking via dictionary or brute-force may be limited by

the time frame of the audit and therefore not a valid test of the protection from that authentication schema however any successful discoveries do attest to its weakness.

11.15.3 Escalation

(a) Collect information on trusted persons, trusted roles or positions, access gateways for trusted persons, and any required physical access media such as tokens or smart cards.
(b) Verify the boundaries of privileges on the target or across multiple targets and if the means exists to escalate those privileges.

11.16 Survivability Validation

Determining and measuring the resistance of the targets within the scope to excessive or hostile changes designed to cause failure.

Denial of Service (DoS) is a situation where a circumstance, either intentionally or accidentally, prevents the system from functioning as intended. In certain cases, the system may be functioning exactly as designed however it was never intended to handle the load, scope, or parameters being imposed upon it. Survivability tests must be closely monitored as the intent is to cause failure and this may be unacceptable to the target owner.

11.16.1 Resilience

(a) Verify single points of failure (choke points) in the infrastructure where change or failure can cause a service outage.
(b) Verify the impact on target access a system or service failure will cause.
(c) Verify the privileges available from the failure-induced access.
(d) Verify the operational functionality of controls to prevent access or permissions above lowest possible privileges upon failure.

11.16.2 Continuity

(a) Enumerate and test for inadequacies from all targets with regard to access delays and service response times through back-up systems or the switch to alternate channels.
(b) Verify intruder lock-out schemes cannot be used against valid users.

11.16.3 Safety

(a) Map and document the process of gatekeepers shutting down target systems due to evacuation or safety concerns as a gap analysis with regulation and security policy.

11.17 Alert and Log Review

A gap analysis between activities performed with the test and the true depth of those activities as recorded or from third-party perceptions both human and mechanical.

11.17.1 Alarm

(a) Verify and enumerate the use of a localized or scope-wide warning system, log, or message for each access gateway over each channel where a suspect situation is elevated by personnel upon suspicion of circumvention attempts, social engineering, or fraudulent activity.

11.17.2 Storage and Retrieval

(a) Document and verify unprivileged access to alarm, log, and notification storage locations and property.
(b) Verify the quality and the length of time of the document storage to assure the data will maintain integrity on that storage medium for the required duration.

Security Test Audit Report (STAR)

The STAR is a document which is to be included with a security test report to show the specifics of what was conducted within the test. The STAR can provide security metrics, comparability with other tests, and third party certification from ISECOM of the client's security rating.

The STAR must be filled out, signed, and included with each security test report in order to provide an OSSTMM test. This document may be used in addition to an Executive Summary or it may be provided as an additional document.

OSSTMM Security Test Audit Report

OSSTMM.ORG – ISECOM.ORG

REPORT ID		**DATE**	
LEAD AUDITOR		**TEST DATE DURATION**	
SCOPE AND INDEX		**VECTORS**	
		TEST TYPES	
CHANNELS		**TERM**	

I am responsible for the information within this report and have personally verified that all information herein this OSSTMM Audit Report is factual and true.

SIGNATURE

COMPANY STAMP/SEAL

OPST CERTIFICATION NUMBERS		**OPSA CERTIFICATION NUMBERS**	

OPERATIONAL SECURITY VALUES

VISIBILITY	
ACCESS	
TRUST	
POROSITY	

LIMITATIONS VALUES

	VERIFIED
Vulnerability	
Weakness	
Concern	
Exposure	
Anomaly	

RAV OPSEC	
RAV CONTROLS	
RAV LIMITATIONS	

CONTROLS VALUES

AUTHENTICATION	
INDEMNIFICATION	
SUBJUGATION	
CONTINUITY	
RESILIENCE	
NON-REPUDIATION	
CONFIDENTIALITY	
PRIVACY	
INTEGRITY	
ALARM	
WHOLE COVERAGE	
TRUE COVERAGE	

The RAV Score is the Actual Security Value as based on Operational Security, Controls, and Limitations.

RAV SCORE

OVERVIEW

This Open Source Security Testing Methodology Manual provides a methodology for a thorough security test. A security test is an accurate measurement of security at an operational level, void of assumptions and anecdotal evidence. A proper methodology makes for a valid security measurement which is consistent and repeatable.

RELATED TERMS AND DEFINITIONS

This report may refer to words and terms that may be construed with other intents or meanings. This is especially true within international translations. This report attempts to use standard terms and definitions as found in international testing vocabulary and based on NCSC-TG-004 (Teal Green Book) from the US. Department of Defense where applicable and generally accepted terms and definitions as outlined in the OSSTMM glossary.

PURPOSE

The primary purpose of this Audit Report is to provide a standard reporting scheme based on a scientific methodology for the accurate characterization of security through examination and correlation in a consistent and reliable way. The secondary purpose is to provide guidelines which when followed will allow the auditor to provide a certified OSSTMM audit.

PROCESS

This Audit Report must accompany the full security test report document which provides evidence of the test and the results as defined in the statement of work between the testing organization and the client.

For this OSSTMM Audit Report to be valid, it must be filled out clearly, properly, and completely. The OSSTMM Audit Report must be signed by the lead or responsible tester or analyst and accompany include the stamp of the company which holds the contract or sub-contract of the test. This audit report must show under COMPLETION STATUS which Channel and the associated Modules and Tasks have been tested to completion, not tested to completion, and which tests were not applicable and why. A report which documents that only specific parts of the Channel test have been completed due to time constraints, project problems, or customer refusal may still be recognized as an official OSSTMM audit if accompanied by this report clearly showing the deficiencies and the reasons for those deficiencies.

CERTIFICATION

OSSTMM certification is the assurance of an organization's security according to the thorough tests within the OSSTMM standard and is available per vector and channel for organizations or parts of organizations which maintain a quarterly RAV level of a minimum of 90% validated yearly from an independent third-party auditor. Validation of security tests or quarterly metrics are subject to the ISECOM validation requirements to assure consistency and integrity.

ABOUT ISECOM

ISECOM is an independent, non-profit security research organization and certification authority defined by the principles of open collaboration and transparency. ISECOM provides assurance for this OSSTMM Audit Report according to the guidelines defined in the above process. Recipients of this report may direct all OSSTMM and OSSTMM Audit Report questions directly back to ISECOM at info@isecom.org.

1. POSTURE REVIEW

TASK	COMMENTS	COMPLETION STATUS
Identified business objectives and markets.		
Identified legislation and regulations applicable to the targets in the scope.		
Identified business policies.		
Identified business and industry ethics policies.		
Identified operation cultures and norms.		
Identified operation times and flow applicable to the targets in the scope.		
Identified all necessary Channels for this scope.		
Identified all Vectors for this scope.		

2. LOGISTICS

TASK	COMMENTS	COMPLETION STATUS
Applied testing safety measures.		
Determined and accounted for test instabilities.		
Determined and accounted for downtime in scope.		
Determined and accounted for test pace according to the test environment and the security presence.		

3. ACTIVE DETECTION VERIFICATION

TASK	COMMENTS	COMPLETION STATUS
Determined and accounted for interferences.		
Tested with both interferences active and inactive.		
Determined restrictions imposed on tests.		
Verified detection rules and predictability.		

4. VISIBILITY AUDIT

TASK	COMMENTS	COMPLETION STATUS
Determined targets through all enumeration tasks.		
Determined new targets by researching known targets.		

5. CONTROLS VERIFICATION

TASK	COMMENTS	COMPLETION STATUS
Verified controls for Non-Repudiation functioning according to all tasks.		
Verified controls for Confidentiality functioning according to all tasks.		
Verified controls for Privacy functioning according to all tasks.		
Verified controls for Integrity functioning according to all tasks.		
Verified controls for Alarm functioning according to all tasks.		
Verified known security limitations of all controls Class B categories.		
Searched for novel circumvention techniques and security limitations of all controls Class B categories.		

6. TRUST VERIFICATION

TASK	COMMENTS	COMPLETION STATUS
Determined interactions which rely on other interactions to complete the test interaction according to the tasks.		
Determined targets with trust relationships to other targets in the scope to complete interactions.		
Determined targets with trust relationships to other targets outside the scope to complete interactions.		
Verified known security limitations of discovered trusts between the trusts.		
Verified known security limitations of discovered trusts between targets in the scope and the trusted interactions.		
Searched for novel circumvention techniques and security limitations of discovered trusts.		

7. ACCESS VERIFICATION

TASK	COMMENTS	COMPLETION STATUS
Verified interactions with access points to all targets in the scope.		
Determined type of interaction for all access points.		
Determined source of interaction defined as a service or process.		
Verified depth of access.		
Verified known security limitations of discovered access points.		
Searched for novel circumvention techniques and security limitations of discovered access points.		

8. PROCESS VERIFICATION

TASK	COMMENTS	COMPLETION STATUS
Determined all processes controlling the action of interactivity with each access.		
Verified the interaction operates within the confines of the determined process.		
Verified the interaction operates within the confines of the security policy for such interactions.		
Determined the gap between the operations of interactions and the requirements of posture from the Posture Review.		
Verified known security limitations of discovered processes.		
Searched for novel circumvention techniques and security limitations of discovered processes.		

9. CONFIGURATION/TRAINING VERIFICATION

TASK	COMMENTS	COMPLETION STATUS
Verified configuration/training requirements according to the posture in the Posture Review.		
Verified the application of appropriate security mechanisms as defined in the Posture Review.		
Verified the functionality and security limitations within the configurations/training for the targets in the scope.		
Searched for novel circumvention techniques and security limitations within configurations/training.		

10. PROPERTY VALIDATION

TASK	COMMENTS	COMPLETION STATUS
Determined the amount and type of unlicensed intellectual property distributed within the scope.		
Verify the amount and type of unlicensed intellectual property available for sale/trade with the seller originating within the scope.		

11. SEGREGATION REVIEW

TASK	COMMENTS	COMPLETION STATUS
Determined the amount and location of private information as defined in the Posture Review available through the targets.		
Determined the type of private information as defined in the Posture Review available within the scope.		
Verified the relationship between publicly accessible information outside the target detailing private or confidential information defined in the Posture Review and the scope.		
Verified the accessibility of public accesses within the target to people with disabilities.		

12. EXPOSURE VERIFICATION

TASK	COMMENTS	COMPLETION STATUS
Searched for available targets through publicly available sources outside of the scope.		
Searched for available organizational assets as defined in the Posture Review through publicly available sources outside of the scope.		
Determined access, visibility, trust, and controls information available publicly within the targets.		
Determined a profile of the organization's channel infrastructure for all channels tested through publicly available information within the targets.		
Determined a profile of the organization's channel infrastructure for all channels tested through publicly available information outside the scope.		

13. COMPETITIVE INTELLIGENCE SCOUTING

TASK	COMMENTS	COMPLETION STATUS
Determined the business environment of partners, suppliers, workers, and market through publicly available information on targets within the scope.		
Determined the business environment of partners, vendors, distributors, suppliers, workers, and market through publicly available information outside the scope.		
Determined the organizational environment through publicly available information on targets within the scope.		
Determined the organizational environment through publicly available information outside the scope.		

14. QUARANTINE VERIFICATION

TASK	COMMENTS	COMPLETION STATUS
Verified quarantine methods for interactions to the targets in the scope.		
Verified quarantine methods for interactions from the targets to other targets outside the scope.		
Verified length of time of quarantine.		
Verified quarantine process from receive to release.		
Verified known security limitations of discovered quarantines.		
Searched for novel circumvention techniques and security limitations of discovered quarantines.		

15. PRIVILEGES AUDIT

TASK	COMMENTS	COMPLETION STATUS
Verified the means of legitimately obtaining privileges for all authenticated interactions.		
Verified the use of fraudulent identification to obtain privileges.		
Verified the means of circumventing authentication requirements.		
Verified the means of taking non-public authentication privileges.		
Verified the means hijacking other authentication privileges.		
Verified known security limitations of discovered authentication mechanisms to escalate privileges.		
Searched for novel circumvention techniques and security limitations of discovered authentication mechanisms to escalate privileges.		
Determined depth of all discovered authentication privileges.		
Determined re-usability of all discovered authentication privileges on the authentication mechanisms on all targets.		

Verified requirements towards obtaining authentication privileges for discriminatory practices according to the Posture Review.		
Verified means towards obtaining authentication privileges for discriminatory practices for people with disabilities.		

16. SURVIVABILITY VALIDATION/SERVICE CONTINUITY

TASK	COMMENTS	COMPLETION STATUS
Determined measures applicable to disrupt or stop service continuity to and from the targets.		
Verified continuity processes and safety mechanisms active for the targets.		
Verified known security limitations of discovered safety and service continuity processes and mechanisms.		
Searched for novel circumvention techniques and security limitations of discovered safety and service continuity processes and mechanisms.		

17. ALERT AND LOG REVIEW/END SURVEY

TASK	COMMENTS	COMPLETION STATUS
Verified methods for recording and alerting interactions to the targets in the scope.		
Verified methods for recording and alerting interactions from the targets to other targets outside the scope.		
Verified speed of recording and alerting.		
Verified persistence of recording and alerting.		
Verified integrity of recording and alerting.		
Verified distribution process of recording and alerting.		
Verified known security limitations of discovered recording and alerting methods.		
Searched for novel circumvention techniques and security limitations of discovered recording and alerting methods.		

License

The Open Methodology License 3.0

This license is Copyright under the Creative Commons 2.5 Attribution, 2007, ISECOM.

PREAMBLE

This license is to protect a methodology as a complex set of methods, processes, or procedures to be applied within a discipline. The key requirements of this license is that 1) the methodology has value as intellectual property which through application thereof can produce value which is quantifiable and 2) that the methodology is available publicly and an appropriate effort is made for the methodology to be transparent to anyone.

With respect the GNU General Public License (GPL), this license is similar with the exception that it gives the right to software developers to include this open methodology license (OML) to software which is closed and distributed commercially.

The main concern covered by this license is that open methodology developers receive proper credit for contribution and development.

Special considerations to the Free Software Foundation and the GNU General Public License for legal concepts and wording.

TERMS AND CONDITIONS

1. The license applies to any methodology or other intellectual tool (ie. matrix, checklist, etc.) which contains a notice placed by the creator saying it is protected under the terms of this Open Methodology License 3.0.

2. The Methodology refers to any such methodology, intellectual tool or any such work based on the Methodology. A "work based on the Methodology" means either the Methodology or any derivative work by Trade Secret law which applies to a work containing the Methodology or a portion of it, either verbatim or with modifications and/or translated into another language.

3. All persons may use, distribute, teach, and promote the Methodology exactly as it has been received, in any medium, provided that they conspicuously and appropriately publish on each copy the appropriate Open Methodology License notice and the creator or creators of the Methodology; keep intact all the notices that refer to this License and to the absence of any warranty; give any other recipients of the Methodology a copy of this License along with the Methodology, and the location as to where they can receive an original copy of the Methodology from the Methodology creator.

4. Any persons who sell training, products, or services of the Methodology must clearly display the name of the creators of this Methodology in addition to the terms of this license.

5. All persons may include this Methodology in part or in whole in commercial service offerings, private or internal (non-commercial) use, or for educational purposes without explicit consent from the creator providing points 3 and 4 are complied with.

6. No persons may distribute an adaption, modification, or change of this Methodology without explicit consent from the creator.

7. All persons may utilize the Methodology or any portion of it to create or enhance commercial or free software, and copy and distribute such software under any terms, provided that they also meet all of these

conditions:

a) Points 3, 4, 5, and 6 of this License are strictly adhered to.

b) Any reduction to or incomplete usage of the Methodology in software must strictly and explicitly state which parts of the Methodology were utilized in the software and which parts were not.

c) When the software is run, all software using the Methodology must either cause the software, when started running, to print or display an announcement of use of the Methodology including a notice of warranty how to view a copy of this License or make clear provisions in another form such as in documentation or delivered open source code.

8. If, as a consequence of a court judgment or allegation of Patent infringement, Trade Secret law infringement, or for any other legal reason, where conditions are imposed on any person (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse said person from the conditions of this License. If said person cannot satisfy simultaneously the obligations under this License and any other pertinent obligations, then as a consequence said person may not use, copy, apply, use, distribute, or promote, the Methodology at all. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

9. If the distribution and/or use of the Methodology is restricted in certain countries either by patents or by Trade Secret interfaces, the original creator who places the Methodology under this License may add an explicit geographical distribution limitation excluding those countries, so that application, use, or distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

10. ISECOM may publish revised and/or new versions of the Open Methodology License. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

NO WARRANTY

11. Because the methodology is licensed free of charge, there is no warranty for the methodology, to the extent permitted by applicable law. except when otherwise stated in writing the creator and/or other parties provides the methodology "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the quality and performance in use of the methodology is with the persons accepting this license. Should the methodology prove incomplete or incompatible said person assumes the cost of all necessary servicing, repair or correction.

12. In no event unless required by applicable law or agreed to in writing will the creator, or any other party who may use, apply, or teach the methodology unmodified as permitted herein, be liable to any persons for damages, including any general, special, incidental or consequential damages arising out of the use or inability to use the methodology (including but not limited to loss, inaccuracies, or failure of the methodology to operate with any other methodologies), even if such holder or other party has been advised of the possibility of such damages.

ISECOM's security certifications are for you, your work, and those waiting for you at home.

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES
Making Sense of Security

Find out more at www.isecom.org/training