# OSSTMM 3

## The Open Source Security Testing Methodology Manual

### Contemporary Security Testing and Analysis

Created by Pete Herzog

Developed by ISECOM

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

**Designed for e-book readers or double-sided printing.**

**This manual provides test cases that result in verified facts. These facts provide actionable information that can measurably improve your operational security. By using the OSSTMM you no longer have to rely on general best practices, anecdotal evidence, or superstitions because you will have verified information specific to your needs on which to base your security decisions.**

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

# Instructions

This is a methodology to test the operational security of physical locations, human interactions, and all forms of communications such as wireless, wired, analog, and digital. 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 them (the parts of the targets tested and not the tools or techniques used), the types of controls discovered, 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. The STAR gives the specific test information on the state of the scope for the benefits of having a clear statement of the security metrics and details for comparisons with previous security tests or industry test averages. More details on the required information for 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 standard test and the formalization of the report. It has been reported that this methodology actually reduces testing and reporting time due to the efficiencies introduced into the process. There should be no time or financial reason to avoid using the OSSTMM and no unreasonable restrictions are made to the tester.

## Upgrading from Older Versions

If you are familiar with the OSSTMM 2.x series then you will find that the methodology has completely changed. The new rav provides a factual attack surface metric that is much more accurate for measuring the susceptibility to attacks. 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: Human, Physical, Wireless, Telecommunications, and Data Networks.

The rav information from 2.x to 3.0 is incompatible. Those with early 3.0 draft rav (prior to RC 12) will require that the values be re-calculated using this final attack surface calculation which is available as a spreadsheet calculator at http://www.isecom.org/ravs. Previous OSSTMM security metrics 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. Our intention is to eventually eliminate the use of risk in areas of security which have no set price value of an asset (like with people, personal privacy, and even fluctuating markets) in favor of trust metrics which are based completely on facts.

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 thorough and proper security tests, systems, and processes are available through ISECOM and will help you get the most of the OSSTMM.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## Version Information

The current version of the Open Source Security Testing Methodology Manual (OSSTMM) is 3.02. This version of the OSSTMM ends the 2.x series. All OSSTMM versions prior to 3.0 including 3.0 release candidates (RC versions) are now obsolete.

The original version was published on Monday, December 18, 2000. This current version is published on Tuesday, December 14, 2010.

## 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 a registered non-profit organization and established in New York, USA and in Catalonia, Spain.

### *Local Support*

Regional ISECOM offices may be available in your area for language and business support. Find the ISECOM Partner in your area at http://www.isecom.org/tp.

### *Community Support*

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

### *Print Edition*

The print edition of this manual is available for purchase at the ISECOM website.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

## Restrictions

Any information contained within this document may not be modified or sold without the express consent of ISECOM. Commercial selling of this document or the information within this document, including the methodology applied within a tool, software, or checklist may NOT be provided without explicit permission from ISECOM.

This research document is free to read, free to re-distribute non-commercially, and free to quote or apply in academic or commercial research, and free to use or apply in the following commercial engagements: testing, education, consulting, and research.

This manual is licensed to ISECOM under Creative Commons 3.0 Attribution-NonCommercial-NoDerivs and the Open Methodology License 3.0.

The ISECOM logo is an official Trademark and may not be used or reproduced commercially without consent from ISECOM. The OSSTMM hummingbird graphic is copyright Marta Barceló Jordan, licensed to ISECOM and may not be used or reproduced commercially without permission.

As a collaborative, open project, the OSSTMM is not to be distributed by any means for which there is commercial gain either by itself or as part of a collection. As a standard, there may be only one, official version of the OSSTMM at any time and that version is not to be altered or forked in any way which will cause confusion as to the purpose of the original methodology. Therefore, no derivation of the OSSTMM is allowed.

As a methodology, the OSSTMM is protected under the Open Methodology License 3.0 which applies the protection as that granted to Trade Secrets. However, where a Trade Secret requires sufficient effort requirements to retain a secret, the OML requires that the user make sufficient effort to be as transparent as possible about the application of the methodology. Therefore, use and application of the OSSTMM is considered as acceptance of the responsibility of the user to meet the requirements in the OML. There are no commercial restrictions on the use or application of the methodology within the OSSTMM. The OML is available at the end of this manual and at http://www.isecom.org/oml.

**Any and all licensing questions or requests should be directed to ISECOM.**



## Primary Developers

- ISECOM
  - **Marta Barceló, Director, ISECOM Board Member**
  - **Pete Herzog, Director, OSSTMM Project Lead, ISECOM Board Member**

## Primary Contributors

The following people are listed alphabetically by company. Each has been a substantial influence to the development of this OSSTMM.

@Mediaservice.net, Italy
**Raoul Chiesa, ISECOM Board Member**
**Marco Ivaldi**
**Fabio Guasconi**
**Fabrizio Sensibile**

adMERITia GmbH, Germany
**Heiko Rudolph, ISECOM Board Member**
**Aaron Brown**

Bell Canada, Canada
**Rick Mitchell**

Blue Secure Limited, New Zealand
**Richard Feist, ISECOM Board Member**

Dreamlab Technologies Ltd., Switzerland
**Nick Mayencourt, ISECOM Board Member**
**Urs B. Weber**
**Adrian Gschwend**
**Thomas Bader**

ISECOM, USA
**Robert E. Lee, ISECOM Board Member**

GCP Global, Mexico
**Francisco Puente**

KCT Data, Inc., USA
**Kim Truett, ISECOM Board Member**

La Salle URL, Spain
**Jaume Abella, ISECOM Board Member**

Lab106 & Outpost24, Netherlands
**Cor Rosielle**

OneConsult GmbH, Switzerland
**Christoph Baumgartner, ISECOM Board Member**

Outpost24, Sweden
**Jack C. Louis**

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## Contributors, Reviewers, and Assistants

A huge and sincere thanks to all those who have applied their efforts to making this OSSTMM version happen. Without you, there would not have been the no-nonsense discussions that made this manual.

*A special thanks to Jack C. Louis (Jan 5, 1977 - March 15, 2009), a brilliant security researcher, an amazing person, and among the first ISECOM certified OPST and OPSA Trainers. We at ISECOM greatly appreciate all your efforts and hereby let them live on as a benchmark we hope inspire other security professionals to attain. Your contributions to the OSSTMM shall never be forgotten. Thank you!*

### Contributions

Alberto Perrone, @Mediaservice.net, Italy
Martin Dion, Above Security, Canada
Lars Heidelberg, adMERITia GmbH, Germany
Martin Pajonk, adMERITia GmbH, Germany
Dru Lavigne, Carleton University, Canada
Todd A. Jacobs, Codegnome, USA
Phil Robinson, Digital Assurance, UK
Philipp Egli, Dreamlab Technologies Ltd., Switzerland
Daniel Hulliger, Dreamlab Technologies Ltd., Switzerland
Simon Nussbaum, Dreamlab Technologies Ltd., Switzerland
Sven Vetsch, Dreamlab Technologies Ltd., Switzerland
Colby Clark, Guidance Software, USA
Andy Moore, Hereford InfoSec, UK
Peter Klee, IBM, Germany
Daniel Fernandez Bleda, Internet Security Auditors, Spain
Jay Abbott, Outpost24 / Lab106, Netherlands
Steve Armstrong, Logically Secure, UK
Simon Wepfer, OneConsult GmbH, Switzerland
Manuel Krucker, OneConsult GmbH, Switzerland
Jan Alsenz, OneConsult GmbH, Switzerland
Tobias Ellenberger, OneConsult GmbH, Switzerland
Shaun Copplestone, The Watchers Inc., Canada
Ian Latter, Pure Hacking, Australia
Ty Miller, Pure Hacking, Australia
Jordi André i Vallverdú, La Caixa, Spain
Jim Brown, Thrupoint, USA
Chris Griffin, ISECOM, USA
Charles Le Grand, USA
Dave Lauer, USA
John Hoffoss, Minnesota State Colleges and Universities, USA
Mike Mooney, USA
Pablo Endres, Venezuela / Germany
Jeremy Wilde, compliancetutorial.com, UK / France
Rob J. Meijer, Netherlands
Mike Simpson, USA / Germany

### Review and Assistance

Gunnar Peterson, Arctec Group, USA
Dieter Sarrazyn, Ascure nv., Belgium
Bob Davies, Bell Canada, Canada
Josep Ruano, Capside, Spain
Adrien de Beaupre, Canada
Clement Dupuis, CCCure, Canada
Armand Puccetti, CEA, France
Jose Luis Martin Mas, davinci Consulting, Spain
Sylvie Reinhard, Dreamlab Technologies Ltd., Switzerland
Raphaël Haberer-Proust, Dreamlab Technologies Ltd., Switzerland
Josh Zelonis, Dyad Security, USA
Bora Turan, Ernst and Young, Turkey
Luis Ramon Garcia Solano, GCP Global, Mexico
John Thomas Regney, Gedas, Spain
Mike Aiello, Goldman Sachs, USA
Dirk Kuhlmann, HP, UK
John Rittinghouse, Hypersecurity LLC, USA
Massimiliano Graziani, IISFA, Italy
Jose Navarro, Indiseg, Spain
Timothy Phillips, Information Assurance Solutions, USA
Joan Ruiz, La Salle URL, Spain
Víktu Pons i Colomer, La Salle URL, Spain
Roman Drahtmueller, Novell, Germany
Hernán Marcelo Racciatti, SICLABS, Argentina
Tom Brown, RWE Shared Services IS, UK
Marcel Gerardino, Sentinel, Dominican Republic
Manuel Atug, SRC Security Research & Consulting GmbH, Germany
Torsten Duwe, SUSE, Germany
Alexander J. Herzog, USA
Drexx Laggui, L&A Inc, Philippines
Ruud van der Meulen, Netherlands
Chris Gatford, HackLabs, Australia
Wim Remes, Belgium
Gary Axten, UK / Spain
Alan Tang, UK
Jason Woloz, USA
John R. Moser, USA
Tom O'Connor, Ireland
Mike Vasquez, City of Mesa, USA

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org


# Foreword

Security verification used to require a cross-disciplinary specialist 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, tool kits, and many other ways to make security testing easy enough that anyone can do it. 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 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. 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 the ISECOM certified 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 Training Partners, ISECOM Licensed Auditors, 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

Director, ISECOM

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

# Table of Contents

**Instructions** ..... **2**
Quick Start ..... 2
Upgrading from Older Versions ..... 2
Version Information ..... 3
About this Project ..... 3
Restrictions ..... 4
Primary Developers ..... 5
Primary Contributors ..... 5
Contributors, Reviewers, and Assistants ..... 6
**Foreword** ..... **7**
**Introduction** ..... **11**
Purpose ..... 13
Document Scope ..... 13
Liability ..... 13
Certification and Accreditation ..... 14
Related Projects ..... 17
**Chapter 1 – What You Need to Know** ..... **20**
1.1 Security ..... 23
1.2 Controls ..... 24
1.3 Information Assurance Objectives ..... 27
1.4 Limitations ..... 28
1.5 Actual Security ..... 31
1.6 Compliance ..... 31
**Chapter 2 – What You Need to Do** ..... **33**
2.1 Defining a Security Test ..... 33
2.2 Scope ..... 34
2.3 Common Test Types ..... 36
2.4 Rules Of Engagement ..... 38
2.5 The Operational Security Testing Process ..... 41
2.6 Four Point Process ..... 43
2.7 The Trifecta ..... 44
2.8 Error Handling ..... 46
2.9 Disclosure ..... 51
**Chapter 3 – Security Analysis** ..... **53**
3.1 Critical Security Thinking ..... 54
3.2 Recognize the OpSec Model ..... 56
3.3 Look for Pattern Matching as a Sign of Errors ..... 57
3.4 Characterize the Results ..... 57
3.5 Look for Signs of Intuition ..... 58
3.6 Transparent Reporting ..... 59
**Chapter 4 – Operational Security Metrics** ..... **62**
4.1 Getting to Know the Rav ..... 63
4.2 How to Make a Rav ..... 67
4.3 Turning Test Results into an Attack Surface Measurement ..... 70
4.4 The Operational Security Formula ..... 79
4.5 The Controls Formula ..... 80
4.6 The Limitations Formula ..... 83
4.7 The Actual Security Formula ..... 85

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

**Chapter 5 – Trust Analysis** ..... **87**
5.1 Understanding Trust ..... 87
5.2 Fallacies in Trust ..... 89
5.3 The Ten Trust Properties ..... 90
5.4 The Trust Rules ..... 91
5.5 Applying Trust Rules to Security Testing ..... 94
**Chapter 6 – Work Flow** ..... **96**
6.1 Methodology Flow ..... 97
6.2 The Test Modules ..... 99
6.3 One Methodology ..... 103
**Chapter 7 - Human Security Testing** ..... **105**
**Chapter 8 - Physical Security Testing** ..... **120**
**Chapter 9 - Wireless Security Testing** ..... **138**
**Chapter 10 - Telecommunications Security Testing** ..... **151**
**Chapter 11 - Data Networks Security Testing** ..... **167**
**Chapter 12 - Compliance** ..... **185**
Regulations ..... 186
**Chapter 13 – Reporting with the STAR** ..... **192**
**Chapter 14 – What You Get** ..... **204**
The Möbius Defense ..... 205
Get What We Need ..... 206
**Chapter 15 – Open Methodology License** ..... **208**
The OML 3 ..... 208

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

**In art, the end result is a thing of beauty, whereas in science, the means of reaching the end result is a thing of beauty. When a security test is an art then the result is unverifiable and that undermines the value of a test. One way to assure a security test has value is to know the test has been properly conducted. For that you need to use a formal methodology. The OSSTMM aims to be it.**

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org



# Introduction

The Open Source Security Testing Methodology Manual (OSSTMM) provides a methodology for a thorough security test, herein referred to as an OSSTMM audit. An OSSTMM audit is an accurate measurement of security at an operational level that is void of assumptions and anecdotal evidence. As a methodology it is designed to be consistent and repeatable. As an open source project, it allows for any security tester to contribute ideas for performing more accurate, actionable, and efficient security tests. Further it allows for the 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 a best practices framework. It had become a methodology to assure security was being done right at the operational level. As security 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.

Since environments are significantly more complex than in years past due such things as remote operations, virtualization, cloud computing, and other new infrastructure types, we can no longer think in simplistic tests meant only for desktops, servers, or routing equipment. Therefore, with version 3, the OSSTMM encompasses tests from all channels - Human, Physical, Wireless, Telecommunications, and Data Networks. This also makes it a perfectly suited for testing cloud computing, virtual infrastructures, messaging middleware, mobile communication infrastructures, high-security locations, human resources, trusted computing, and any logical processes which all cover multiple channels and require a different kind of security test. A set of attack surface metrics, called ravs, provide a powerful and highly flexible 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 however you will find the proposed trust management here to be superior to risk management. 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.

Legal and industry specific regulations also commonly require a security audit as a component of becoming compliant. An OSSTMM audit is well suited for most all of these cases. Specific OSSTMM tests can therefore be connected with particular security standard requirements, making the OSSTMM itself a way to gain compliance to those requirements. This applies to regulations and policies from physical security like the US Federal Energy Reserve Commission's ruling to pure data security efforts such as the latest PCI-DSS and including cross-channel requirements as found in many NIST recommendations and information security management specifications like ISO/IEC 27001:2005, ISO/IEC 27002:2005, and ISO/IEC 27005:2008.

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.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *A Short Note About Language in the OSSTMM*

*What is an audit? Some of the words used in this document may stray from the definition you are familiar with. New research often requires updating, enhancing, or retracting information from the world as we thought we have known it. This is a normal occurrence and to assist you with the changes, this document does try to define these words properly in their new context. In this document, an OSSTMM audit or "audit" is the result of the analysis performed after an OSSTMM test. The person who performs this function of test and analysis is referred to as the Security Analyst or just "Analyst".*

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## Purpose

The primary purpose of this manual is to provide a scientific methodology for the accurate characterization of operational security (OpSec) 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 analyst 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 operational channels, which include Human, Physical, Wireless, Telecommunications, and Data Networks, over any vector, and the description of derived metrics. This manual only focuses on OpSec and the use of the words safety and security are within this context.

## Liability

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

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 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 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 ISECOM 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 show what was and was not tested to be applicable for certification. (See Chapter 16, Making the STAR for details and an example of a STAR.)

A certified OSSTMM audit provides the following benefits:

- Serves as proof of a factual test
- Holds Analyst responsible for the test
- Provides a clear result to the client
- Provides a more comprehensive overview than an executive summary
- Provides understandable metrics

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

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *Certifications for Professionals*

Anyone who uses this methodology for security testing and analysis and completes a valid STAR is said to have performed an OSSTMM audit. However, individual certification is also available through ISECOM for the applied skills in professional security testing, analysis, methodical process, and professional standards as outlined in the OSSTMM Rules of Engagement. ISECOM is the authority for a variety of skill and applied knowledge certification exams based on OSSTMM research. Classes and the official exams are provided by certified training partners in various regions around the world. The current certification exams available are:


#### *OPST*

The OSSTMM Professional Security Tester proves a candidate has the skill and knowledge to perform accurate & efficient security tests on data networks.

http://www.opst.org


#### *OPSA*

The OSSTMM Professional Security Analyst proves a candidate can apply the principles of security analysis and attack surface metrics accurately & efficiently.

http://www.opsa.org


#### *OPSE*

The OSSTMM Professional Security Expert proves a candidate has learned all the security concepts within the most current, publicly available OSSTMM and the background to the research.

http://www.opse.org


#### *OWSE*

The OSSTMM Wireless Security Expert proves a candidate has the skill and knowledge to analyze and test the operational security of wireless technologies across the electromagnetic spectrum accurately & efficiently.

http://www.owse.org


#### *CTA*

The Certified Trust Analyst proves a candidate has the skills and knowledge to efficiently evaluate the trust properties of any person, place, thing, system, or process and make accurate and efficient trust decisions.

http://www.trustanalyst.org

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

### *Certifications for Organizations*

Certifications for organizations, infrastructure, and products is also available through ISECOM. The following certifications are available:


#### *Security Test Audit Report*

OSSTMM certification is available for organizations or parts of organizations that validate their security with the STAR from ISECOM. Validation of security tests and quarterly metrics are subject to the ISECOM validation requirements to assure a high level of trustworthiness in an organization.


#### *ISECOM Licensed Auditors*

ILAs have proven to ISECOM to have the competence and capacity to perform OSSTMM audits for themselves and for others. This provides for an easy and efficient way to maintain Security Test Audit Reports and have those reports certified by ISECOM.


#### *OSSTMM Seal of Approval*

OSSTMM evaluation seals are available for products, services, and business processes. This seal defines an operational state of security, safety, trust, and privacy. 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 guesswork from procurement and allows one to find and compare alternative solutions.


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## Related Projects

To properly test the security of anything, you first need to know how that thing operates, what it's comprised of, and what is the environment it exists in. This is how the OSSTMM itself had been approached as a means of understanding the best, most efficient, and most thorough way to test security. Therefore, we needed to understand security. This research seeking the "security particle" as it turns out has brought about the application and design of more projects beyond the OSSTMM.

While not all applications of the OSSTMM to areas outside of security testing are worthy of being projects. However, some do provide a testament to the fact that we are now only limited by our own imaginations. The OSSTMM has become a tool with which we can take new approaches to many new means of protection.

### *Source Code Analysis Risk Evaluation (SCARE)*

The SCARE project applies the OSSTMM ravs to source code analysis. The end result is a SCARE value which is the amount of the source code with unprotected operations.
**http://www.isecom.org/scare**

### *Home Security Methodology and Vacation Guide (HSM)*

The HSM project applies the OSSTMM ravs, Four Point Process, Trust Metrics, and analysis process to protecting and fortifying a home. The end result is to create a home that is safer and more secure without restricting the freedoms of the occupants.
**http://www.isecom.org/hsm**

### *Hacker Highschool (HHS)*

HHS is a different kind of security awareness program for teens. It uses the OSSTMM testing and analysis research to provide knowledge and skills through hands-on lessons and access to an Internet-based test network. However while doing so, it reinforces resourcefulness and critical thinking skills.
**http://www.hackerhighschool.org**

### *The Bad People Project (BPP)*

The BPP is a different kind of security and safety awareness program for children and parents. It uses OSSTMM ravs and Trust Metrics to create better rules for children about safety and security to be explained through games, stories, and role play. The rules are easier to remember and free of contradictions and cultural biases. The parents can visit and contribute to the gallery of children's drawings which examines what children think what a bad person looks like. These drawings are the further used to find new ways to reach children and improve the rules taught to them.
**http://www.badpeopleproject.org**

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *Security Operations Maturity Architecture (SOMA)*

The SOMA project aims to provide the OSSTMM operational processes at the strategic level. This project applies ravs and Trust Metrics to determining security maturity by how well protection strategy and tactics work and not just how they should work according to policy.
**http://www.isecom.org/soma**

### *Business Integrity Testing (BIT)*

The BIT project extends the OSSTMM operational testing and analysis to business processes and transactions. This adds new strategic insight to the security of business conduct by employees and in the development of new business plans.
**http://www.isecom.org/bit**

### *Smarter Safer Better*

This project provides the safety and security tools and skills people need every day to combat fraud, lies, and deception. The tools are based on the OSSTMM research which is focused on avoiding persuasive tricks and manipulation techniques. The project is unique in how it utilizes support groups for people to discuss issues they have encountered and work together to analyze the problems.
**http://www.smartersaferbetter.org**

### *Mastering Trust*

This project is to create seminar materials and workbooks on how to use the OSSTMM Trust Metrics in every day life to make better decisions. This project addresses why our gut instincts are broken and how we can fix and improve them. Whether its in business or private relationships, knowing who you can trust and how much is more than protecting yourself from being hurt, it´s a competitive edge.
**http://www.isecom.org/seminars**

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

**Security doesn't have to last forever; just longer than everything else that might notice it's gone.**

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

# Chapter 1 – What You Need to Know

This manual is about operational security (OpSec). It is about measuring how well security works. While this may seem plain and obvious: "Don't we all do operational security?" it is a distinction which must be made because most compliance objectives require no more than matching processes and configurations to a set of best practices. This manual and the testing process it outlines requires that you make no assumptions that a security solution, product, or process will behave during operational use as it has been designated to do on paper. More simply, this methodology will tell you if what you have does what you want it to do and not just what it was told to do.

OpSec is a combination of separation and controls. Under OpSec, for a threat to be effective, it must interact either directly or indirectly with the asset. To separate the threat from the asset is to avoid a possible interaction. Therefore it is possible to have total (100%) security if the threat and the asset are completely separated from each other. Otherwise what you have is safety of the asset which is provided by the controls you put on the asset or the degree to which you lessen the impact of the threat.

For example, to be *secure* from lightning, one must move to where lightning can't reach such as deep in a mountain. Threats which can't be separated from the assets must be made safer so that their interactions and any effects from interactions do little or no harm. In this same example, to be *safe* from lightning, one must stay indoors during storms, avoid windows or other openings, and use lightning rods on the roof. Therefore, under the context of operational security, we call *security* the separation of an asset and a threat and *safety* the control of a threat or its effects.

To have true safety of the assets different types of controls are required. However, controls also may increase the number of interactions within the scope which means more controls are not necessarily better. Therefore it is recommended to use different types of operational controls rather than just more controls. More controls of the same type of operational controls do not provide a defense in depth as access through one is often access through all of that type. This is why it is so important to be able to categorize controls by what they do in operations to be certain of the level of protection provided by them.

To better understand how OpSec can work within an operational environment, it must be reduced to its elements. These elements allow one to quantify the **Attack Surface**, which is the lack of specific separations and functional controls that exist for that **Vector**, the direction of the interaction. The reductionist approach resolves to us needing to see security and safety in a new way, one that allows for them to exist independent of risk and fully capable of creating **Perfect Security**, the exact balance of security and controls with operations and limitations. However, to see security in a new way requires new terminology as well.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

| Term | Definition |
|---|---|
| | |
| Attack Surface | The lack of specific separations and functional controls that exist for that vector. |
| Attack Vector | A sub-scope of a vector created in order to approach the security testing of a complex scope in an organized manner. It is based on the divide and conquer algorithm design paradigm that consists in recursively breaking down a problem into two or more sub-problems of the same (or related) type, until these become simple enough to be solved directly. |
| Controls | Impact and loss reduction controls. The assurance that the physical and information assets as well as the channels themselves are protected from various types of invalid interactions as defined by the channel. For example, insuring the store in the case of fire is a control that does not prevent the inventory from getting damaged or stolen but will pay out equivalent value for the loss. Ten controls have been defined. The first five controls are Class A and control interactions. The five Class B controls are relevant to controlling procedures. See section 1.2 below for further information regarding controls. |
| Limitations | This is the current state of perceived and known limits for channels, operations, and controls as verified within the audit. Limitation types are classified by how they interact with security and safety on an operational level. Therefore, opinions as to impact, availability in the wild, difficulty to perform, and complexity are not used to classify them. For example, an old rusted lock used to secure the gates of the store at closing time has an imposed security limitation providing a fraction of the protection strength necessary to delay or withstand an attack. Determining that the lock is old and weak through visual verification is referred to as an identified limitation. Determining it is old and weak by breaking it using 100 kg of force when a successful deterrent requires 1000 kg of force shows a verified limitation. One of its limitations is then classified based on the consequence of the operational action, which in this case is Access. |
| Operations | Operations are the lack of security one must have to be interactive, useful, public, open, or available. For example, limiting how a person buys goods or services from a store over a particular channel, such as one door for going in and out, is a method of security within the store's operations. |
| Perfect Security | The exact balance of security and controls with operations and limitations. |
| Porosity | All interactive points, operations, which are categorized as a Visibility, Access, or Trust. |

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

| Term | Definition |
|---|---|
| | |
| Safety | A form of protection where the threat or its effects are controlled. In order to be safe, the controls must be in place to assure the threat itself or the effects of the threat are minimized to an acceptable level by the asset owner or manager. This manual covers safety as "controls" which are the means to mitigate attacks in an operational or live environment. |
| Security | A form of protection where a separation is created between the assets and the threat. This includes but is not limited to the elimination of either the asset or the threat. In order to be secure, the asset is removed from the threat or the threat is removed from the asset. This manual covers security from an operational perspective, verifying security measures in an operating or live environment. |
| Rav | The rav is a scale measurement of an attack surface, the amount of uncontrolled interactions with a target, which is calculated by the quantitative balance between porosity, limitations, and controls. In this scale, 100 rav (also sometimes shown as 100% rav) is perfect balance and anything less is too few controls and therefore a greater attack surface. More than 100 rav shows more controls than are necessary which itself may be a problem as controls often add interactions within a scope as well as complexity and maintenance issues. |
| Target | That within the scope that you are attacking, which is comprised of the asset and any protections the asset may have. |
| Vector | The direction of an interaction. |
| Vulnerability | One classification of Limitation where a person or process can access, deny access to others, or hide itself or assets within the scope. More details and examples are available in the Limitations table in 4.2. |


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 1.1 Security

Security is a function of a separation. Either the separation between an asset and any threats exists or it does not. There are 3 logical and proactive ways to create this separation:

1. Move the asset to create a physical or logical barrier between it and the threats.
2. Change the threat to a harmless state.
3. Destroy the threat.

When analyzing the state of security we can see where there is the possibility for interaction and where there is not. We know some, all, or even none of these interactions may be required for operations. Like doors into a building, some of the doors are needed for customers and others for workers. However, each door is an interactive point which can increase both necessary operations and unwanted ones, like theft. Since the security tester may not know at this point the business justification for all these interactive points, we refer to this as the **porosity**. The porosity reduces the separation between a threat and an access. It is further categorized as one of 3 elements, visibility, access, or trust which describes its function in operations which further allows the proper controls to be added during the remediation phase of improving protection.

So consider that if the separation exists properly from the threats, such as a man inside a mountain avoiding lightning, then that security is true; it is 100%. For every hole in the mountain, every means for lightning to cause harm to that man, the porosity increases as an Access. Each point of interaction reduces the security below 100%, where 100% represents a full separation. Therefore, the increase in porosity is the decrease in security and each *pore* is either a Visibility, Access, or Trust.

| Term | Definition |
|---|---|
| | |
| Visibility | Police science places "opportunity" as one of the three elements which encourage theft, along with "benefit", and "diminished risk". Visibility is a means of calculating opportunity. It is each target's asset known to exist within the scope. Unknown assets are only in danger of being discovered as opposed to being in danger of being targeted. |
| Access | Since security is the separation of a threat and an asset then the ability to interact with the asset directly is to access it. Access is calculated by the number of different places where the interaction can occur. Removing direct interaction with an asset will halve the number of ways it can be taken away. |
| Trust | We measure trust as part of OpSec as each relationship that exists where the target accepts interaction freely from another target within the scope. While a trust may be a security hole, it is a common replacement for authentication and a means for evaluating relationships in a rational and repeatable manner. Therefore, the use of trust metrics is encouraged which will allow for one to measure how valid a trust is by calculating the amount of reliability in the trust. |

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 1.2 Controls

When the threat is all around then it is controls which will provide safety in operations. Controls are a means to influence the impact of threats and their effects when interaction is required.

> *Just because you can't directly control it doesn't mean it can't be controlled. Control the environment and you control everything in it.*

While there are many different names and types of operation controls, there are only 12 main categories which contain all possible controls. Two of the categories however, **Identification**, the verification of an existing identity, and **Authorization**, the granting of permissions from the rightful authority, cannot stand alone in an operational environment and instead, in operations, combine and are added to the Authentication control. This leaves OpSec with ten possible controls an Analyst will need to identify and understand.

The reason why Identification and Authorization cannot be expressed operationally is because neither can be transferred. Identity exists as is and while the means of identification, as a process, is an operational aspect, the actual process is to verify a previously provided identity from another source or from the latest in a chain of sources. Even under circumstances where a government agency officially changes the identity of a person, they are still the same person from identifying marks to their DNA and only their documentation changes. Therefore, a security process can attempt to identify someone by verifying their identity but nothing in this case is granted or provided. There is no true "granting" of identity just as there can be no true "theft" of identity. Furthermore, identity is a collection of thoughts, emotions, experiences, relationships, and intentions, as well as physical shape or marks. You are who you are because you exist not because someone granted that to you. A perfect duplicate or clone of you is still not you because from origin your experiences will differ. While this may sound more like philosophy than security, it is very important that Analysts understand this. Identification processes only verify against a former identification process. If that process has been corrupted or can be circumvented, then the entire security foundation that requires proper identification is flawed.

Authorization, like Identification, is another operations control which cannot be transferred. It is the control to grant permissions. An employee authorized to enter a room may hold the door open for another person to enter. This does not authorize the new person. Authorization did not get transferred. This new person is trespassing in a restricted area and the employee who held open the door actually was part of a limitation in the Authentication process to grant Access.

Another property of Authorization is that it requires identification to work. Without identification, authorization is a blanket "permit all" without even knowing what all is. However in operations this is itself a paradox because to authorize all without scrutiny means that there is no authorization. Therefore to not authorize you do not use authorization.

The Authentication control combines both identification and authorization to map Access. The process is simply knowing who (or what) it is and what, where, when, and how they can access before they are granted access. Because authentication is a control for interactivity, it is one of the five Class A controls, also known as the "Interactive Controls".

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *Interactive Controls*

The Class A Interactive Controls make up exactly half of all the operation controls. These controls directly influence visibility, access, or trust interactions. The Class A categories are Authentication, Indemnification, Subjugation, Continuity, and Resilience.

1. **Authentication** is a control through the challenge of credentials based on identification and authorization.
2. **Indemnification** is a control through a contract between the asset owner and the interacting party. This contract may be in the form of a visible warning as a precursor to legal action if posted rules are not followed, specific, public legislative protection, or with a third-party assurance provider in case of damages like an insurance company.
3. **Resilience** is a control over all interactions to maintain the *protection* of assets in the event of corruption or failure.
4. **Subjugation** is a control assuring that interactions occur only according to defined processes. The asset owner defines how the interaction occurs which removes the freedom of choice but also the liability of loss from the interacting party.
5. **Continuity** is a control over all interactions to maintain *interactivity* with assets in the event of corruption or failure.

### *Process Controls*

The other half of operation controls are the Class B controls which are used to create defensive processes. These controls do not directly influence interactions rather they protect the assets once the threat is present. These are also known as Process Controls and include Non-repudiation, Confidentiality, Privacy, Integrity, and Alarm.

6. **Non-repudiation** is a control which prevents the interacting party from denying its role in any interactivity.
7. **Confidentiality** is a control for assuring an asset displayed or exchanged between interacting parties cannot be known outside of those parties.
8. **Privacy** is a control for assuring the means of how an asset is accessed, displayed, or exchanged between parties cannot be known outside of those parties.
9. **Integrity** is a control to assure that interacting parties know when assets and processes have changed.
10. **Alarm** is a control to notify that an interaction is occurring or has occurred.

While controls are a positive influence in OpSec, minimizing the attack surface, they can themselves add to the attack surface if they themselves have limitations. Often times this effect is not noticed and if the protection mechanisms aren't tested thoroughly as to how they work under all conditions, this may not become apparent. Therefore the use of controls must assure that they do not insinuate new attack vectors into the target. Therefore, sometimes no controls are better than bad controls.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *The Bad Lock Example*

Is a bad lock on a door better than no lock at all? An Analyst must use critical security thinking, a form of logic skills to overcome the innate sense of security we carry to understand why bad controls can increase the attack surface to greater than no control at all.

Common thought is that adding controls with limitations are better than having none at all. Is it not better to have a poor lock than to have no lock at all? After all, as conventional wisdom suggests, a wisdom borne of emotion rather than verification, some "security" is better than none. This is why the analogy of the lock is such a good example and actually does better to answer the question then any other because it shows so well how we misunderstand controls that are so common around us.

Ask anyone who has had to break open a locked door where they kick or hit the door to open it? That answer differs whether it is a key lock opened from the outside as opposed to a bolt lock on the inside. There's a reason for this.

When a lock (which is considered the authentication control) is added to a door, the heavy, solid door needs to have a space hollowed out and the lock inserted. That creates a limitation, a weak spot in the door. So does adding a handle. Doors with no handles or internal locks do not have this limitation. However they require the door to be opened from the inside in another means. So to open a door with that kind of lock, you kick or hit the door at the handle or lock mechanism.

If there is a bolt lock, that limitation does not exist because the door remains solid. Those doors often require a force to open that will sooner break the door than the lock. Doors made to withstand high pressures have the bolts on the outside and the opening mechanism in the center of the door as a small hole, like doors on a boat or submarine, to avoid the weaknesses of hollowing out part of the door.

Now to more directly answer the question: if it is better to have a weak lock than no lock. This question refers to a door with the minimum, a cheap or simple key lock (authentication) that can be bypassed by someone who wants to enter. So if we know the authentication is weak, then we know somebody can get in and even worse, they can do it without damaging the lock or the door which means we may have no knowledge of the intrusion. If you think, well, that's okay because our problem isn't the real crooks, it's the opportunists looking for the low-hanging fruit then you're making a risk decision and that does not affect your attack surface which is made from what you have and not what you want. Furthermore, by having a lock at all implies, most of all to the opportunists, that there is something of value inside.

If you add a control, any control, you increase the attack surface of anything. If that new thing you add brings a new attack vector then you were probably better off without. In some cases, the new attack vector is smaller than the actual amount of safety the new control gives you. However, a good control will have no limitations and can shrink the attack surface.

A lock in a door should not be easily subverted or add to the attack surface in a significant way. Such a lock requires force to open and that adds another control then which the lock provides, alarm. A broken lock is also a good notification of a break-in.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 1.3 Information Assurance Objectives

To facilitate understanding of operation controls, they can be matched back to the three Information Assurance Objectives of Confidentiality, Availability, and Integrity. These objectives are used across the information security industry although due in part to their over-simplification, they are more for the benefit of managing it rather than creating it or testing it. The mapping is not a perfect 1:1 however it is sufficient to demonstrate operation controls according to the basic CIA Triad. Because the definitions used for CIA are very broad the mappings appear to be as such:

| Information Assurance Objectives | Operation Controls |
|---|---|
| Confidentiality | Confidentiality<br>Privacy<br>Authentication<br>Resilience |
| Integrity | Integrity<br>Non-repudiation<br>Subjugation |
| Availability | Continuity<br>Indemnification<br>Alarm |

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 1.4 Limitations

The inability of protection mechanisms to work are their limitations. Therefore the state of security in regard to known flaws and restrictions within the operations scope is called Limitation. It is the holes, vulnerabilities, weaknesses, and problems in keeping that separation between an asset and a threat or in assuring controls continue working correctly.

Limitations have been classified into five categories and these categories define the type of vulnerability, mistake, misconfiguration, or deficiency by operation. This is different from how limitations are classified under most security management frameworks and best practices which is why we use the term Limitation rather than more common terms to avoid confusion. Those other terms refer to vulnerabilities or deficiencies because they are categorized by the type of attack or often the threat itself. There is a focus on the risk from the attack. However, to remove bias from security metrics and provide a more fair assessment we removed the use of risk. Risk itself is heavily biased and often highly variable depending on the environment, assets, threats, and many more factors. Therefore, under OpSec, we use the term Limitations to express the difference of categorizing how OpSec fails rather than by the type of threat. Since the number and type of threats cannot be known it makes more sense to understand a security or safety mechanism based on when it will fail. This allows the Analyst to test for the conditions in which it will no longer sustain the necessary level of protection. Only once we have this knowledge can we begin to play the what-if game of threats and risks. Then we can also invest in the appropriate type of separation or controls required and create precise plans for disasters and contingencies.

Although the Limitations are categorized here as 1 through 5 this does not mean they are in a hierarchical format of severity. Rather they are numbered only to differentiate them both for operational planning and metrics. This also means it is possible that more than one type of Limitation can be applied to a single problem. Furthermore, the weight (value) of a particular Limitation is based on the other available and corresponding controls and interactive areas to the scope, there can be no specific hierarchy since the value of each is specific to the protective measures in the scope being audited.

Within the OSSTMM the five Limitation classifications are:

1. **Vulnerability** is the flaw or error that: (a) denies access to assets for authorized people or processes, (b) allows for privileged access to assets to unauthorized people or processes, or (c) allows unauthorized people or processes to hide assets or themselves within the scope.
2. **Weakness** is the flaw or error that disrupts, reduces, abuses, or nullifies specifically the effects of the five interactivity controls: authentication, indemnification, resilience, subjugation, and continuity.
3. **Concern** is the flaw or error that disrupts, reduces, abuses, or nullifies the effects of the flow or execution of the five process controls: non-repudiation, confidentiality, privacy, integrity, and alarm.
4. **Exposure** is an unjustifiable action, flaw, or error that provides direct or indirect visibility of targets or assets within the chosen scope channel.
5. **Anomaly** is any unidentifiable or unknown element which has not been controlled and cannot be accounted for in normal operations.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *Limitations Mapping*

To better understand how Limitations fit into the OpSec framework, it can be seen mapping back to security and safety:

| Category | | OpSec | Limitations |
|---|---|---|---|
| | | | |
| Operations | | Visibility | Exposure |
| | | Access | Vulnerability |
| | | Trust | |
| Controls | Class A - Interactive | Authentication | Weakness |
| | | Indemnification | |
| | | Resilience | |
| | | Subjugation | |
| | | Continuity | |
| | Class B - Process | Non-Repudiation | Concern |
| | | Confidentiality | |
| | | Privacy | |
| | | Integrity | |
| | | Alarm | |
| | | | Anomalies |

This mapping shows how Limitations effect security and how there values are determined.

A *vulnerability* is the flaw or error that: (a) denies access to assets for authorized people or processes (b) allows for privileged access to assets to unauthorized people or processes, or (c) allows unauthorized people or processes to hide assets or themselves within the scope. This means that Vulnerability must be mapped to all points of interaction or OpSec and because Vulnerability can circumnavigate or nullify the Controls, these must also be considered in the weighting of Vulnerability.

A *weakness* is a flaw in Class A Controls however can impact OpSec therefore it is mapped to all OpSec parameters as well as being mapped to this interactive class of controls.

A *concern* can only be found in Class B Controls however can impact OpSec therefore it is mapped to all OpSec parameters as well as being mapped to this process class of controls.

An *exposure* gives us intelligence about the interaction with a target and thus maps directly to Visibility and Access. This intelligence can also help an attacker navigate around some or all controls and so Exposure is also mapped to both Control classes. Finally, Exposure has no value itself unless there is a way to use this intelligence to exploit the asset or a Control and so Vulnerabilities, Weaknesses and Concerns also play a role in the weighting of Exposure's value.

An *anomaly* is any unidentifiable or unknown element which has not been controlled and cannot be accounted for in normal operations. The fact that it has not been controlled and cannot be accounted for signifies a direct link with Trust. This Limitation can also cause anomalies in the way Controls function and so they are also included in the weighting. Finally, as with an Exposure, an Anomaly alone does not affect OpSec without the existence of either a Vulnerability, Weakness or Concern which can exploit this unusual behavior.

Additionally, more than one category can apply to a limitation when the flaw breaks OpSec in more than

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

one place. For example, an Authentication control which allows a person to hijack another person's credentials has a Weakness and should the credentials allow Access then it also has a Vulnerability.

In another example, an Authentication control uses a common list of names corresponding to e-mail addresses. Every address which can be found or guessed and used as a log-in is an Exposure while the control itself has a Weakness for its inability to identify the correct user of the Authentication mechanism of the log-in. If any of those credentials allow Access then we include this as a Vulnerability as well.

### *Justification for Limitations*

The concept that limitations are only limitations if they have no business justification is false. A limitation is a limitation if it behaves in one of the limiting factors as described here. A justification for a limitation is a risk decision that is met with either a control of some kind or merely acceptance of the limitation. Risk decisions that accept the limitations as they are often come down to: the damage a limitation can cause does not justify the cost to fix or control the limitation, the limitation must remain according to legislation, contracts, or policy, or a conclusion that the threat does not exist or is unlikely for this particular limitation. Since risk justifications are not a part of calculating an attack surface, all limitations discovered must still be counted within the attack surface regardless if best practice, common practice, or legal practice denotes it as not a risk. If it is not then the audit will not show a true representation of the operational security of the scope.

### *Managing Limitations*

Another concept that must be taken into consideration is one of managing flaws and errors in an audit. The three most straightforward ways to manage limitations is to remove the problem area providing the interactive point altogether, fix them, or accept them as part of doing business known as the business justification.

An audit will often uncover more than one problem per target. The Analyst is to report the limitations per target and not just which are the weak targets. These limitations may be in the protection measures and controls themselves, thus diminishing OpSec. Each limitation is to be rated as to what occurs when the problem is invoked, even if that invocation is theoretical or the verification is of limited execution to restrict actual damages. Theoretical categorization, where no verification could be made, is a slippery slope and should be limited to cases where verification would reduce the quality of operations. Then, when categorizing the problems, each limitation should be examined and calculated in specific terms of operation at its most basic components. However, the Analyst should be sure never to report a "flaw within a flaw" where the flaws share the same component and same operational effect. An example of this would be a door broken open with a broken window. The door opening is an Access even if the broken window is also but both are for the same component, the door way, and same operational effect, an opening. An example from Data Networks would be a computer system which sends a kernel reply, such as an ICMP "closed port" T03C03 packet for a particular port. This interaction is not counted for all such ports since the Access comes from the same component, the kernel, and has the same operational effect, sending a T03C03 packet per port queried.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 1.5 Actual Security

The role of the Controls is to control the porosity in OpSec. It's like having ten ways of controlling threats that come through a hole in a wall. For each hole, a maximum of ten different controls can be applied which bring security back up towards and sometimes above 100%. Limitations then reduce the effectiveness of OpSec and Controls. The result of an audit which discovers and shows the Security, Controls, and Limitations is effectively demonstrating Actual Security.

Actual Security is a term for a snapshot of an attack surface in an operational environment. It is a logarithmic representation of the Controls, Limitations, and OpSec at a particular moment in time. It is logarithmic because it represents the reality of size where a larger scope will have a larger attack surface even if mathematically the Controls will balance the OpSec. Using this as building blocks to better understand how security works, the visualization that we create from this is the effective balance created between where an attack can occur, where the Controls are in place to manage an attack, and the limitations of the protective measures.

Another benefit of mathematical representation of an attack surface as Actual Security is that besides just showing where protection measures are lacking it can also show the opposite. Since it is possible to have more controls than one needs this can be mathematically represented as more than 100% rav. Whether a risk assessment may make this point seem impossible, the mathematical representation is useful for showing waste. It can be used to prove when money is being overspent on the wrong types of controls or redundant controls.

## 1.6 Compliance

Compliance is a different thing than security and exists separate from security. It is possible to be compliant yet not secure and it is possible to be relatively secure but non-compliant and therefore of low trustworthiness.

Compliance projects are not the time to redefine operational security requirements as a result of an OSSTMM test, they may however be the time to specify the use of OSSTMM testing, on a periodic basis, to fulfill a control requirement drafted as a result of a trust assessment that has scoped the minimum number of controls required to achieve a compliant (but not necessarily secure) state.

The big problem with compliance is it requires a lot of documentation that has to be versioned and updated. This documentation can be of business processes, narratives, trust assessments, risk assessments, signed off design tests, operational audits, attestations, and so on and on. This documentation is scrutinized by internal and external auditors and has to logically fulfill its existence in the world of a compliant state.

Most recent compliance efforts have been driven by the short term requirements of imposed regulations with short term implementation requirements. This has created a lot of resource requirements and cost. Given time to think about it we try to build compliance and evidence production into a process and manage this resource requirement and cost.

Compliance is a broad brush approach to the application of best practice from, as far as Information Technology is concerned, the likes of COBIT and ITIL; an OSSTMM test should provide documentation that provides an understandable, verifiable level of quality. The use of the OSSTMM, however, is designed to allow the Analyst to view and understand security and safety. Therefore, with the use of this methodology, any compliance is, at least, the production of evidence of governance within the business process of security.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

**Fact does not come from the grand leaps of discovery but rather from the small, careful steps of verification.**

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org



# Chapter 2 – What You Need to Do

Where do you start? Testing is a complicated affair and with anything complicated, you approach it in small, comprehensible pieces to be sure you don't make mistakes.

Conventional wisdom says complexity is an enemy of security. However, it is only at odds with human nature. Anything which is made more complex is not inherently insecure. Consider a computer managing complex tasks. The problem as we know it is not that the computer will make mistakes, confuse the tasks, or forget to complete some. As more tasks are added to the computer, it gets slower and slower, taking more time to complete all the tasks. People, however, do make mistakes, forget tasks, and purposely abandon tasks which are either not important or required at the moment. So when testing security, what you need to do is properly manage any complexity. This is done by properly defining the security test.

## 2.1 Defining a Security Test

These 7 steps will take you to the start of a properly defined security test.

1. Define what you want to protect. These are the assets. The protection mechanisms for these assets are the **Controls** you will test to identify **Limitations**.
2. Identify the area around the assets which includes the protection mechanisms and the processes or services built around the assets. This is where interaction with assets will take place. This is your **engagement zone**.
3. Define everything outside the engagement zone that you need to keep your assets operational. This may include things you may not be able to directly influence like electricity, food, water, air, stable ground, information, legislation, regulations and things you may be able to work with like dryness, warmth, coolness, clarity, contractors, colleagues, branding, partnerships, and so on. Also count that which keeps the infrastructure operational like processes, protocols, and continued resources. This is your test **scope**.
4. Define how your scope interacts within itself and with the outside. Logically compartmentalize the assets within the scope through the direction of interactions such as inside to outside, outside to inside, inside to inside, department A to department B, etc. These are your **vectors**. Each vector should ideally be a separate test to keep each compartmentalized test duration short before too much change can occur within the environment.
5. Identify what equipment will be needed for each test. Inside each vector, interactions may occur on various levels. These levels may be classified in many ways, however here they have been classified by function as five **channels**. The channels are Human, Physical, Wireless, Telecommunications, and Data Networks. Each channel must be separately tested for each vector.
6. Determine what information you want to learn from the test. Will you be testing interactions with the assets or also the response from active security measures? The **test type** must be individually defined for each test, however there are six common types identified here as Blind, Double Blind, Gray Box, Double Gray Box, Tandem, and Reversal.
7. Assure the security test you have defined is in compliance to the **Rules of Engagement**, a guideline to assure the process for a proper security test without creating misunderstandings, misconceptions, or false expectations.

The end result will be a measurement of your **Attack Surface**. The attack surface is the unprotected part of the Scope from a defined Vector.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 2.2 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 classes of which there are five channels: Telecommunications and Data Networks security Channels of the COMSEC class, Physical and Human Security Channels of the PHYSSEC class, and the full spectrum Wireless Security Channel of the SPECSEC class. Classes are from official designations currently in use in the security industry, government, and the military. Classes are used to define an area of study, investigation, or operation. However, Channels are the specific means of interacting with assets. An asset can be anything that 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. Often, the scope extends far beyond the reach of the asset owner as dependencies are beyond the asset owner's ability to provide independently. The scope requires that all threats be considered possible, even if not probable. Although, it must be made clear that a security analysis must be restricted to that which is within a type of certainty (not to be confused with risk which is not a certainty but a probability). These restrictions include:

1. Non-events such as a volcano eruption where no volcano exists,
2. Non-impact like moonlight through data center window, or
3. Global-impacting such as a catastrophic meteor impact.

While a thorough security audit requires testing all five channels, realistically, tests are conducted and categorized by the required expertise of the Analyst and the required equipment for the audit.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *Channels*

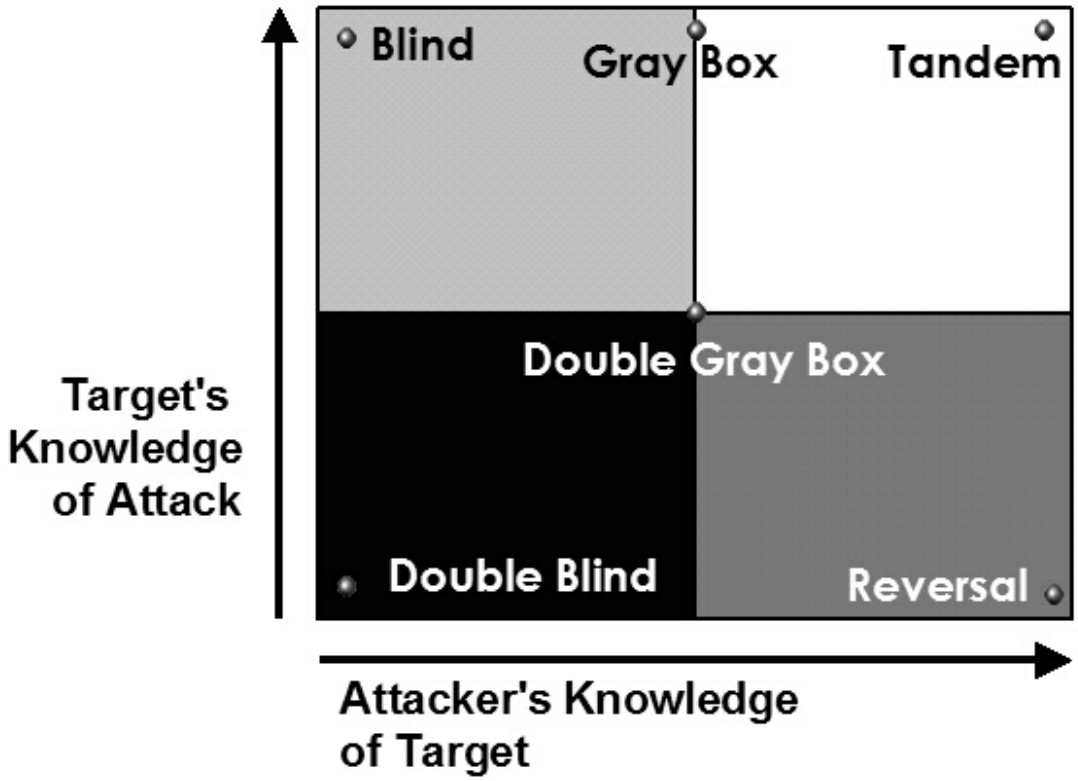
| Class | Channel | Description |
|---|---|---|
| Physical Security (PHYSSEC) | Human | Comprises the human element of communication where interaction is either physical or psychological. |
| | Physical | Physical security testing where the channel is both physical and non-electronic in nature. Comprises the tangible element of security where interaction requires physical effort or an energy transmitter to manipulate. |
| Spectrum Security (SPECSEC) | Wireless | 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. |
| Communications Security (COMSEC) | Telecommunications | Comprises all telecommunication networks, digital or analog, where interaction takes place over established telephone or telephone-like network lines. |
| | Data Networks | Comprises all electronic systems and data networks where interaction takes place over established cable and wired network lines.<br>Data Networks |

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.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 2.3 Common Test Types

These six types differ based on the amount of information the tester knows about the targets, what the target knows about the tester or expects from the test, and the legitimacy of the test. Some tests will test the tester's skill more than actually testing the security of a target.




Do note when reporting the audit, there is often a requirement to identify exactly the type of audit performed. Too often, audits based on 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.


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

| Type | | Description |
|---|---|---|
| 1 | Blind | The Analyst 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 Analyst. The breadth and depth of a blind audit can only be as vast as the Analyst's applicable knowledge and efficiency allows. In COMSEC and SPECSEC, this is often referred to as Ethical Hacking and in the PHYSSEC class, this is generally scripted as **War Gaming** or **Role Playing**. |
| 2 | Double Blind | The Analyst 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 Analyst and the preparedness of the target to unknown variables of agitation. The breadth and depth of any blind audit can only be as vast as the Analyst's applicable knowledge and efficiency allows. This is also known as a **Black Box test** or **Penetration test**. |
| 3 | Gray Box | The Analyst 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 Analyst. The nature of the test is efficiency. The breadth and depth depends upon the quality of the information provided to the Analyst before the test as well as the Analyst'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 Analyst 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 Analyst and the target's preparedness to unknown variables of agitation. The breadth and depth depends upon the quality of the information provided to the Analyst and the target before the test as well as the Analyst's applicable knowledge. This is also known as a **White Box** test. |
| 5 | Tandem | The Analyst 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 Analyst does have full view of all tests and their responses. The breadth and depth depends upon the quality of the information provided to the Analyst before the test (transparency) as well as the Analyst's applicable knowledge. This is often known as an In-House Audit or a **Crystal Box** test and the Analyst is often part of the security process. |
| 6 | Reversal | The Analyst engages the target with full knowledge of its processes and operational security, but the target knows nothing of what, how, or when the Analyst 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 Analyst and the Analyst's applicable knowledge and creativity. This is also often called a **Red Team exercise**. |

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 2.4 Rules Of Engagement

These rules define the operational guidelines of acceptable practices in marketing and selling testing, performing testing work, and handling the results of testing engagements.

### *A. Sales and Marketing*

1. The use of fear, uncertainty, doubt, and deception may not be used in the sales or marketing presentations, websites, supporting materials, reports, or discussion of security testing for the purpose of selling or providing security tests. This includes but is not limited to highlighting crimes, facts, glorified criminal or hacker profiles, and statistics to motivate sales.
2. The offering of free services for failure to penetrate the target is forbidden.
3. Public cracking, hacking, and trespass contests to promote security assurance for sales or marketing of security testing or security products are forbidden.
4. To name past or present clients in the marketing or sales for potential customers is only allowed if the work for the client was specifically the same as being marketed or sold and the named client has provided written permission to do so.
5. It is required that clients are advised truthfully and factually in regards to their security and security measures. Ignorance is not an excuse for dishonest consultancy.

### *B. Assessment / Estimate Delivery*

6. Performing security tests against any scope without explicit written permission from the target owner or appropriate authority is strictly forbidden.
7. The security testing of obviously highly insecure and unstable systems, locations, and processes is forbidden until the proper security infrastructure has been put in place.

### *C. Contracts and Negotiations*

8. With or without a Non-Disclosure Agreement contract, the security Analyst is required to provide confidentiality and non-disclosure of customer information and test results.
9. Contracts should limit liability to the cost of the job, unless malicious activity has been proven.
10. Contracts must clearly explain the limits and dangers of the security test as part of the statement of work.
11. In the case of remote testing, the contract must include the origin of the Analysts by address, telephone number or IP address.
12. The client must provide a signed statement which provides testing permission exempting the Analysts from trespass within the scope, and damages liability to the cost of the audit service with the exception where malicious activity has been proven.
13. Contracts must contain emergency contact names and phone numbers.
14. The contract must include clear, specific permissions for tests involving survivability failures, denial of service, process testing, and social engineering.
15. Contracts must contain the process for future contract and statement of work (SOW) changes.
16. Contracts must contain verified conflicts of interest for a factual security test and report.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *D. Scope Definition*

17. The scope must be clearly defined contractually before verifying vulnerable services.
18. The audit must clearly explain the limits of any security tests according to the scope.

### *E. Test Plan*

19. The test plan may not contain plans, processes, techniques, or procedures which are outside the area of expertise or competence level of the Analyst.

### *F. Test Process*

20. The Analyst must respect and maintain the safety, health, welfare, and privacy of the public both within and outside the scope.
21. The Analyst must always operate within the law of the physical location(s) of the targets in addition to rules or laws governing the Analyst's test location.
22. To prevent temporary raises in security for the duration of the test, only notify key people about the testing. It is the client's judgment which discerns who the key people are; however, it is assumed that they will be information and policy gatekeepers, managers of security processes, incident response personnel, and security operations staff.
23. If necessary for privileged testing, the client must provide two, separate, access tokens whether they be passwords, certificates, secure ID numbers, badges, etc. and they should be typical to the users of the privileges being tested rather than especially empty or secure accesses.
24. When testing includes known privileges, the Analyst must first test without privileges (such as in a black box environment) prior to testing again with privileges.
25. The Analysts are required to know their tools, where the tools came from, how the tools work, and have them tested in a restricted test area before using the tools on the client organization.
26. The conduct of tests which are explicitly meant to test the denial of a service or process or survivability may only be done with explicit permission and only to the scope where no damage is done outside of the scope or the community in which the scope resides.
27. Tests involving people may only be performed on those identified in the scope and may not include private persons, customers, partners, associates, or other external entities without written permission from those entities.
28. Verified limitations, such as discovered breaches, vulnerabilities with known or high exploitation rates, vulnerabilities which are exploitable for full, unmonitored or untraceable access, or which may immediately endanger lives, discovered during testing must be reported to the customer with a practical solution as soon as they are found.
29. Any form of flood testing where a scope is overwhelmed from a larger and stronger source is forbidden over non-privately owned channels.
30. The Analyst may not leave the scope in a position of less actual security than it was when provided.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *G. Reporting*

31. The Analyst must respect the privacy of all individuals and maintain their privacy for all results.
32. Results involving people untrained in security or non-security personnel may only be reported via non-identifying or statistical means.
33. The Analyst may not sign test results and audit reports in which they were not directly involved.
34. Reports must remain objective and without untruths or any personally directed malice.
35. Client notifications are required whenever the Analyst changes the testing plan, changes the source test venue, has low trust findings, or any testing problems have occurred. Notifications must be provided previous to running new, dangerous, or high traffic tests, and regular progress updates are required.
36. Where solutions and recommendations are included in the report, they must be valid and practical.
37. Reports must clearly mark all unknowns and anomalies.
38. Reports must clearly state both discovered successful and failed security measures and loss controls.
39. Reports must use only quantitative metrics for measuring security. These metrics must be based on facts and void of subjective interpretations.
40. The client must be notified when the report is being sent as to expect its arrival and to confirm receipt of delivery.
41. All communication channels for delivery of the report must be end to end confidential.
42. Results and reports may never be used for commercial gain beyond that of the interaction with the client.


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 2.5 The Operational Security Testing Process

Why test operations? Unfortunately, not everything works as configured. Not everyone behaves as trained. Therefore the truth of configuration and training is in the resulting operations. That's why we need to test operations.

The OpSec testing process is a discrete event test of a dynamic, stochastic system. This means that you will be making a chronological sequence of tests on a system that changes and does not always give the same output for the input provided. The target is a system, a collection of interacting and co-dependent processes which is also influenced by the stochastic environment it exists in. Being stochastic means the behavior of events in a system cannot be determined because the next environmental state can only be partially but not fully determined by the previous state. The system contains a finite but possibly extremely large number of variables and each change in variables may present an event and a change in state. Since the environment is stochastic, there is an element of randomness and there is no means for predetermining with certainty how all the variables will affect the system state.

Most of what people understand of OpSec comes from the defensive aspect which is understandable since security is generally considered a defensive strategy. Aggressive testing of OpSec is then relegated to the same class as the exploitation and circumvention of the current design or configuration. However, the fundamental problem with this technique is that a design or configuration does not equate to operation.

We encounter many instances in life where operation does not conform to configuration. A simple example is a typical job description. It is more common than not that the policy which dictates one's job, also known as a job description, falls short from actually reflecting what we do on the job. Another example is the TV channel. Because a channel is set to a particular frequency (configured) it does not mean we will receive the show broadcast on that channel or only that show.

This security testing methodology is designed on the principle of verifying the security of operations. While it may not always test processes and policy directly, a successful test of operations will allow for analysis of both direct and indirect data to study the gap between operations and processes. This will show the size of the rift between what management expects of operations from the processes they developed and what is really happening. More simply put, the Analyst's goal is to answer: "how do current operations work and how do they work differently from how management thinks they work?"

A point of note is the extensive research available on change control for processes to limit the amount of indeterminable events in a stochastic system. The Analyst will often attempt to exceed the constraints of change control and present "what if" scenarios which the change control implementers may not have considered. A thorough understanding of change control is essential for any Analyst.

An operational security test therefore requires thorough understanding of the testing process, choosing the correct type of test, recognizing the test channels and vectors, defining the scope according to the correct index, and applying the methodology properly.

Strangely, nowhere, besides in security testing is the echo process considered the defacto test. Like yelling into a cavernous area and awaiting the response, the echo process requires interacting and then monitoring emanations from the target for indicators of a particular state such as secure or insecure, vulnerable or protected, on or off, and left or right. The echo process is of a cause and effect type of verification. The Analyst makes the cause and analyzes the effect on the target. It is strange that this is the primary means of testing something as critical as security because although it makes for a very fast test, it is also highly prone to errors, some of which may be devastating to the target. Consider that in a security test using the echo process, a target that does not respond is considered secure. Following that logic, a

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

target needs only to be non-responsive to a particular type of request to give the appearance of security however still be fully interactive with other types of requests which shows there has been no separation.

If hospitals used the echo process to determine the health of an individual, it would rarely help people, but at least the waiting room time would be very short. Hospitals however, like most other scientific industries, apply the Four Point Process which includes a function of the echo process called the "interaction" as one of the four tests. The other three tests are: the "inquest" of reading emanations from the patient such as pulse, blood pressure, and brain waves; the "intervention" of changing and stressing operating conditions such as the patient's homeostasis, behavior, routine, or comfort level; and the "induction" of examining the environment and how it may have affected the target such analyzing what the patient has interacted with, touched, eaten, drank, or breathed in. However, in security testing, the majority of tests are based on the echo process alone. There is so much information lost in such one-dimensional testing we should be thankful that the health care industry has evolved past just the "Does it hurt if I do this?" manner of diagnosis.

The security test process in this methodology does not recommend the echo process alone for reliable results. While the echo process may be used for certain, particular tests where the error margin is small and the increased efficiency allows for time to be moved to other time-intensive techniques, it is not recommended for tests outside of a deterministic environment. The Analyst must choose carefully when and under what conditions to apply the echo process.

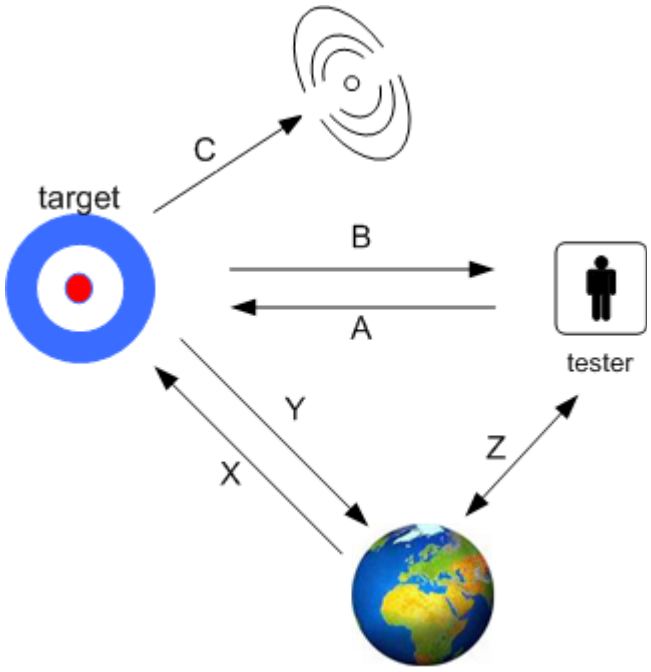
While many testing processes exist, the Four Point Process for security testing is designed for optimum efficiency, accuracy, and thoroughness to assure test validity and minimize errors in uncontrolled and stochastic environments. It is optimized for real-world test scenarios outside of the lab. While it also uses agitation, it differs from the echo process in that it allows for determining more than one cause per effect and more than one effect per cause.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 2.6 Four Point Process

The Four Point Process (4PP) breaks down a test from start to conclusion. These are things that an experienced testing group already does. Don't confuse the formality in the dissection of the process with the formality of the reporting. You don't have to show every step being done but you should understand how you got from A to C. It is like giving people driving directions. You tell them the steps on where they turn and relative proximity to things that they will see to know they are going the right way but you don't tell them every street they drive down and every traffic signal they must obey to get to the end. Well, the 4PP is the specific directions and the means and reporting are actually the relativistic ones.




*Interactions within the 4 Point Process*

1. **Induction:** (Z) establishing principle truths about the target from environmental laws and facts. The Analyst determines factual principles regarding the target from the environment where the target resides. As the target will be influenced by its environment, its behavior will be determinable within this influence. Where the target is not influenced by its environment, there exists an anomaly to be understood.

2. **Inquest:** (C) investigating target emanations. The Analyst investigates the emanations from the target and any tracks or indicators of those emanations. A system or process will generally leave a signature of its existence through interactions with its environment.

3. **Interaction:** (A/B) like echo tests, standard and non-standard interactions with the target to trigger responses. The Analyst will inquire or agitate the target to trigger responses for analysis.

4. **Intervention:** (X/Y/Z) changing resource interactions with the target or between targets. The Analyst will intervene with the resources the target requires from its environment or from its interactions with other targets to understand the extremes under which it can continue operating adequately.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 2.7 The Trifecta

This security testing methodology has a solid base which may seem quite involved, but it is actually simple in practice. It is designed as a flowchart; however, unlike the standard flowchart, the flow, represented by the arrows, may go backward as well as forward. In this way, it is more integrated and while the beginning and the end are clear, the audit has greater flexibility. The Analyst creates a unique path through the methodology based on the target, the type of test, the time allotted for the audit, and the resources applied to the test. For an orchestra, the composer writes the sheet music to designate the order and duration of notes, but only the conductor can control the execution of the performance. This methodology is like the sheet music, designating the necessary tests, but the Analyst controls the order, the duration, as well as the execution. The main reason for requiring this level of flexibility in the OSSTMM is because no methodology can accurately presume the justifications for the operations of channel gateways in a target and their adequate level of security. More directly, this methodology cannot presume a best practice for conducting all audits, as best practice is based on a specific configuration of operations.

Best practice is only best for some; generally the originator of the practice. Operations dictate how services should be offered, and those services dictate the requirements for operational security. Therefore, a methodology that is invoked differently for each audit and by each Analyst can still have the same end result if the Analyst completes the methodology. For this reason one of the foundations of the OSSTMM is to record precisely what was not tested. By comparing what was tested and the depth of the testing with other tests, it is possible to measure operational security (OpSec) based on the test results.

Applying this methodology will therefore meet the Analyst's goal to answer the following three questions which make up the **Trifecta**, the answer to OpSec needs.

### *1. How do current operations work?*

The derived metrics can be applied to determine the problem areas within the scope and which problems must be addressed. The metrics in this methodology are designed to map the problems in different ways so as to show if the problem is a general one or more specific, like an overlook or a mistake.

### *2. How do they work differently from how management thinks they work?*

Access to policies or a trust (or even a risk) assessment will map back to the different categories of the metrics. The categories provide the current state values where a comparison can be made with both an optimum state according to the policies and one according to assessed threats.

### *3. How do they need to work?*

Where the metrics show no gap between policy or trust (or risk) assessment's optimum values yet the security test shows that there is indeed a protection problem regardless of controls as implemented in policy, it is possible to clearly denote a problem. Often, without even mapping to policy, a discrepancy between the implemented controls and the loss of protection is simply evident.

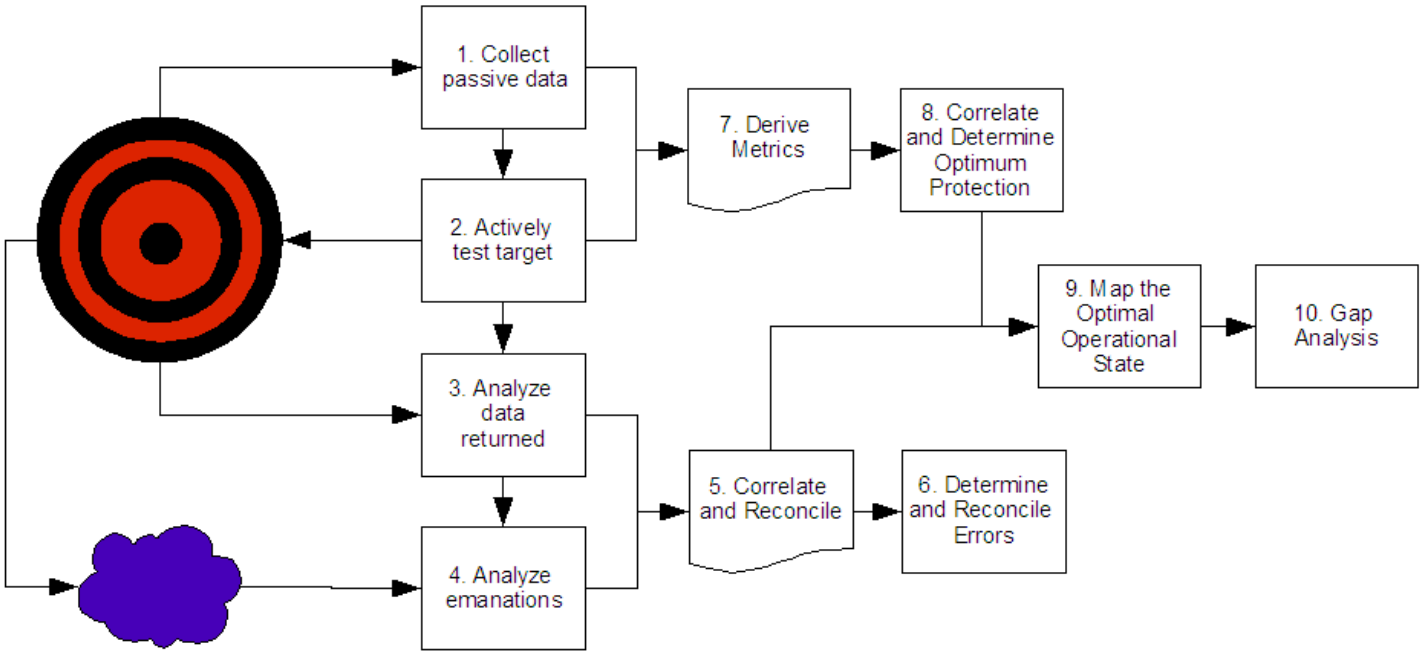
Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *Combining the Trifecta and the 4 Point Process*

The Trifecta combined with the Four Point Process provide a substantially thorough application of this methodology. The steps in this application can be summarized as follows:

1. Passively collect data of normal operations to comprehend the target.
2. Actively test operations by agitating operations beyond the normal baseline.
3. Analyze data received directly from the operations tested.
4. Analyze indirect data from resources and operators (i.e. workers, programs).
5. Correlate and reconcile intelligence from direct (step 3) and indirect (step 4) data test results to determine operational security processes.
6. Determine and reconcile errors.
7. Derive metrics from both normal and agitated operations.
8. Correlate and reconcile intelligence between normal and agitated (steps 1 and 2) operations to determine the optimal level of protection and control which would best be implemented.
9. Map the optimal state of operations (step 8) to processes (step 5).
10. Create a gap analysis to determine what enhancements are needed for processes governing necessary protection and controls (step 5) to achieve the optimal operational state (step 8) from the current one.




*Combining the Trifecta and the 4 Point Process*

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 2.8 Error Handling

The veracity in a security test is not in the sum of its errors, but rather in the accounting for its errors. Since errors may not be the fault of the Analyst, the understanding of how and where errors can exist within a test is much more reasonable than expecting an Analyst to test without error. Furthermore, it is the Analyst who attempts what should not be possible that is most likely to encounter errors; therefore, denoting errors as a negative thing discounts the practice of thorough testing.

| Error Type | | Description |
|---|---|---|
| | | |
| 1 | False Positive | *Something determined as true is actually revealed false.*<br><br>The target response indicates a particular state as true although in reality the state is not true. A false positive often occurs when the Analyst's expectations or assumptions of what indicates a particular state do not hold to real-world conditions which are rarely black and white. |
| 2 | False Negative | *Something determined as false is actually revealed as true.*<br><br>The target response indicates a particular state as not true although in reality the state is true. A false negative often occurs when the Analyst's expectations or assumptions about the target do not hold to real-world conditions, the tools are not adequate for the test, the tools are misused, or the Analyst lacks experience. A false negative can be dangerous as it is a misdiagnosis of a secure state when it does not exist. |
| 3 | Gray Positive | *Something answers true to everything even if false.*<br><br>The target response indicates a particular state as true, however the target is designed to respond to any cause with this state whether it is true or not. This type of security through obscurity may be dangerous, as the illusion cannot be guaranteed to work the same for all stimuli. |
| 4 | Gray Negative | *Something answers false to everything even if true.*<br><br>The target response indicates a particular state as not true, however the target is designed to respond to any cause with this state whether it is true or not. This type of security through obscurity may be dangerous, as the illusion cannot be guaranteed to work the same for all stimuli. |

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

| Error Type | | Description |
|---|---|---|
| | | |
| 5 | Specter | *Something answers either true or false but the real state is revealed as unknown.*<br><br>The target response indicates a particular state as either true or false although in reality the state cannot be known. A specter often occurs when the Analyst receives a response from an external stimulus that is perceived to be from the target. A specter may be intentional, an anomaly from within the channel, or the result of carelessness or inexperience from the Analyst. One of the most common problems in the echo process is the assumption that the response is a result of the test. Cause and effect testing in the real world cannot achieve consistently reliable results since neither the cause nor the effect can be properly isolated. |
| 6 | Indiscretion | *Something answers either true or false depending when it's asked.*<br><br>The target response indicates a particular state as either true or false but only during a particular time, which may or may not follow a pattern. If the response cannot be verified at a time when the state changes, it may prevent the Analyst from comprehending the other state. An Analyst may also determine that this is an anomaly or a problem with testing equipment, especially if the Analyst failed to calibrate the equipment prior to the test or perform appropriate logistics and controls. An indiscretion can be dangerous as it may lead to a false reporting of the state of security. |
| 7 | Entropy Error | *The answer is lost or confused in signal noise.*<br><br>The target response cannot accurately indicate a particular state as either true or false due to a high noise to signal ratio. Akin to the idea of losing a flashlight beam in the sunlight, the Analyst cannot properly determine state until the noise is reduced. This type of environmentally caused error rarely exists in a lab, however it is a normal occurrence in an uncontrolled environment. Entropy can be dangerous, if its effects cannot be countered. |
| 8 | Falsification | *The answer changes depending on how and where the question is asked.*<br><br>The target response indicates a particular state as either true or false although in reality the state is dependent upon largely unknown variables due to target bias. This type of security through obscurity may be dangerous, as the bias will shift when tests come from different vectors or employ different techniques. It is also likely that the target is not aware of the bias. |

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

| Error Type | | Description |
|---|---|---|
| | | |
| 9 | Sampling Error | *The answer cannot represent the whole because the scope has been altered.*<br><br>The target is a biased sample of a larger system or a larger number of possible states. This error normally occurs when an authority influences the operational state of the target for the duration of the test. This may be through specific time constraints on the test or a bias of testing only components designated as "important" within a system. This type of error will cause a misrepresentation of the overall operational security. |
| 10 | Constraint | *The answer changes depending on the limitations of the tools used.*<br><br>The limitations of human senses or equipment capabilities indicate a particular state as either true or false although the actual state is unknown. This error is not caused by poor judgment or wrong equipment choices rather it is a failure to recognize imposed constraints or limitations. |
| 11 | Propagation | *The answer is presumed to be of one state or the other although no test was made.*<br><br>The Analyst does not make a particular test or has a bias to ignore a particular result due to a presumed outcome. This is often a blinding from experience or a confirmation bias. The test may be repeated many times or the tools and equipment may be modified to have the desired outcome. As the name implies, a process that receives no feedback where the errors remain unknown or ignored will propagate further errors as the testing continues. Propagation errors may be dangerous because the errors propagated from early in testing may not be visible during an analysis of conclusions. Furthermore, a study of the entire test process is required to discover propagation errors. |
| 12 | Human Error | *The answer changes depending on the skill of the Analyst.*<br><br>An error caused by lack of ability, experience, or comprehension is not one of bias and is always a factor that is present, regardless of methodology or technique. While an experienced Analyst may make propagation errors, one without experience is more likely to not recognize human error, something that experience teaches to recognize and compensate for. Statistically, there is an indirect relationship between experience and human error. The less experience an Analyst has, the greater the amount of human error an audit may contain. |

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *Working with Test Errors*

During the analysis phase, an Analyst can keep track of the quantity and severity of operation errors from the test. A simple self-assessment can create a margin of operation errors caused during the test which the Analyst can use to either frame the thoroughness of the current audit or other audits of similar systems.

Since it is a self assessment it will have a tendency to be biased. The Analyst should take great care for it to be as factual as possible as a form of quality assurance of the test and the test process. Although some may try to dismiss test errors which were on the fault of the Analyst, keeping track of all errors can only improve future tests and is not something to hide. Errors will happen and are no more than the Analyst's attempt to interact with an ever-changing system. Regardless of the number and severity of errors, the tracking of test errors will serve as a record of the difficulty and complexity of the audit and the competency of the Analyst to deduce the errors.

A record of test errors from the scope will also help sum up the environment in a simplistic way. It is a straight-forward reduction of the Executive Summary which often describes the Analyst's opinion about the state of security wherein few to no errors will show a fairly static target and environment. Many errors show a chaotic environment and one that may lack controls for managing change or loss.

Overall, test error records are useful for understanding the complexity of the audit and change control between audits of regular intervals.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *Test 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 Analyst 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 Analyst 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 within this manual or at the ISECOM website. STAR requires the following information:

1. Date and time of test
2. Duration of test
3. Names of responsible Analysts
4. Test type
5. Scope of test
6. Index (method of target enumeration)
7. Channel tested
8. Test Vector
9. Attack surface metric
10. Which tests have been completed, not completed, or partially completed, and to what extent
11. Any issues regarding the test and the validity of the results
12. Any processes which influence the security limitations
13. Any unknowns or anomalies

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

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 2.9 Disclosure

During a security test the advent of previously unknown or non-publicized security limitations may come to light. What an Analyst does with these is first and foremost a result of the legal regulations of the Analyst's region and the region where the work is being performed.

### *Disclosure Rights*

What you do have to do is make sure that your access to and use of the product or solution did not require any sort of provisions, Non-Disclosure contract, or End User License Agreement (EULA) that denies you the right to claim, announce, or distribute any vulnerabilities discovered. If it did and you or the client accepted this contract then you can't disclose to anyone, perhaps even the manufacturer, without potential legal repercussions. Furthermore if you work for the company making that product or are a legal client of theirs then you may not be able to legally disclose anything either. Furthermore, your rights in any case may be challenged according to the process of law in your region rather than existing legal precedent.

### *Responsibilities*

However, if those cases do not apply then you effectively own that vulnerability and the sooner you make it public the more rights you have as the owner. In many countries, processes and information can be protected by law and often the legal process requires publication or legally filing such with attribution. If your disclosure can do no PHYSICAL harm (like yelling fire in a crowded movie theater), it is yours to make and no legal posturing need shake you when you're right. However, to be safest, you should also promote, with the disclosed vulnerability, the controls which one can apply to fix the problem. For example, if it's a problem with how one authenticates with a solution then suggest an alternative authentication scheme and how it can be successfully integrated. You do not need to wait for the manufacturer to release a fix or a recall to let people fix the problem. However, should you choose to work within the context of notifying the manufacturer, you will need to give them ample time to address the problem before making it public. There is a valid argument that the vulnerability may already be known in criminal circles and need immediate attention. Therefore should you choose to publish without the manufacturer's assistance, do note that including a fix will also show legally that you had good intentions and much of the legal system focuses on implied intent.

Your choice depends on whether frivolous lawsuits are accepted or prevalent in your region. Remember, it is not you the Analyst who is required to do the quality assurance testing for the manufacturer therefore you do not owe them any information from work you've done even if it includes their product.

Full disclosure is helpful as long as it can do no human, physical harm. Furthermore, consumers should not have to wait on manufacturer fixes for their products to be secure. If the product is not sold as a security specific solution then it's up to the consumers to make it secure and safe, or not use it. If it is sold as secure and safe then it is up to the manufacturer to fix it however, the consumer may not want to wait until the manufacturer can do so. Full disclosure allows for this choice.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

**The weakness is not found by analyzing what it is but rather in analyzing what it does.**

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org



# Chapter 3 – Security Analysis

Security analysis here refers to the skill to turn information into security intelligence. This requires understanding more than just the information but also where it came from, how and when it was collected, and any constraints of the collection process. The final part of the analysis process is to create actionable intelligence, information derived from fact that can be used to make decisions. This is the clear distinction between security and risk analysis. In security analysis, you produce facts even if that fact states something can't be known from the information provided. In risk analysis, you speculate and derive opinions based on information. Risk analysis can use security analysis to come up with better, more accurate answers however security analysis cannot use risk analysis to improve accuracy. For this reason we recommend trust analysis.

### *Analyzing the Security of Everything*

The fundamental difference between doing a risk analysis versus a security analysis is that in security analysis you never analyze the threat. This is because assuming you know what threats exist, when they may hit, how they will come, and where they will go is something reserved for risk analysis. In security analysis, you study and measure the attack surface of and around a target. This will allow you then to understand where the threats, any threats, can attack if they do attack. For example, consider a long, high wall. The risk analysis will consider what can get through the wall but the security analysis will focus on where the cracks are, if the foundation is solid, and if the wall is thick or tall enough to prevent Access long enough for help to arrive and respond to the attack. A security analysis will also allow you to assure the right controls exist, work the way they should, and properly cover the interactive points of the various accessible vectors and channels.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 3.1 Critical Security Thinking

Critical security thinking as used here is a term for the practice of using logic and facts to form an idea about security. That idea may be an answer, a conclusion, or a characterization of something or someone so that verification tests can be well defined. As an answer or a conclusion, critical security thinking will provide that which makes the most sense. As a characterization, it will show you what you need to verify, according to what you need to verify, according to what vector, how, and what the targets will be. It will also help you respect different opinions or viewpoints beyond security itself to the interconnectedness security makes with people, places, processes, and money. It will help you address contradictory conclusions and explore alternate consequences. So even if the critical security thinking model can't provide an answer it should tell you what facts are still missing and from where you need to get them.

The process of critical security thinking is dependent on the Analyst being able to discern true statements or at least recognize the degree of possible falsity or dynamic properties in a statement. One way to do this is to recognize the amount of trust you can have in a fact through the use of trust metrics. Another way is to be able to deconstruct a statement, separating out fallacious arguments. In practice, an Analyst will need to do both. The Analyst will need to have a good understanding of what is being analyzed and a good understanding of logical fallacies used to make qualifiers, statements based on fallacious concepts usually in the form of axioms or best practices.

### *The Six Step Analysis Technique*

Unfortunately, the world is not prescriptive. Not every question has a right answer. The correctness of an answer is dependent on many things including, most importantly, how it is asked. This is a problem affecting all industries but none so obviously as security which is why critical security thinking is so important. As a technique for analysis it can be reduced to 6 simple steps to ascertain factual results with a high trust level for correctness even when solutions are not linear like when there is no connection from point A to point B. Therefore the ability to validate sources and measure trust is crucial for making proper, actionable intelligence out of tests. In these steps, "target" refers to whatever you are analyzing in preparation of a test, be it people, computers, buildings, or processes.

1. Build your knowledge of the target from a variety of the most contemporary, factual resources while avoiding commercially biased and speculative information.
2. Determine the global level of experience for the type of target and the amount of information possibly known about it.
3. Determine any bias or ulterior motives in the information sources.
4. Translate jargon from information sources to similar or known words for comparison because what may sound new or complicated may just be a trick to differentiate something common.
5. Be sure the test equipment has been properly calibrated and the test environment verified to assure the results are not contaminated by the test itself.
6. Assure that the translation state of tools or test processes has been removed as much as possible so that the results do not come from the indirect sources in a process or the pre-analysis from some tools.

What's most important to understand here is when making a characterization don't worry about being right. It's more important to be right about being wrong or right which means the right tests were made to verify the characterization. Then if the characterization is wrong we at least know for sure it is wrong and can re-characterize. That's how the scientific method works. It's not about believing or relying on your experience, no matter how vast, but on knowing facts we can build upon.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *Fallacies as Qualifiers*

An additional problem of the humanization of testing into an art form rather than handled as a science is that it introduces all sorts of new errors. Understanding our own limitations as humans and how we think influences how security can be perceived and defined. This leads many security professionals to provide qualifiers for what they don't understand or can't deliver. Most often though they are just repeated as axioms without further thought, eventually accepted as truths of security. This further hurts our ability to provide proper security because our analysis is perverted by catch phrases and best practices that may have no basis in fact now or ever.

For example, some common axioms still in use will seem much less like golden rules and more like excuses when put to the light of critical security thing. These axioms are so common because there is a general inability to think critically about security or separate it from risk as a concept. Security is not about risk. It is about protection and controls. Risk is about risk. Risk is speculated, contrived, derived, and correlated. Risk is also subjective. Security should not be. To better understand how these qualifiers taint our ability to make good security analysis, we can examine the fallacies in the common qualifiers:

1. **There is no such thing as 100% secure.**
   The statement fails to provide conditions such as time and the metric for which percentages can be used as the scale. As a risk statement, it could hold true- "There is no such thing as always being 100% risk free." because under the definition of risk, even our own bodies are subject to time and self-inflicted injuries. However as a security statement it can have far too many exceptions to be true.

2. **Even if you are secure, if an attacker wants in badly enough they'll get in.**
   The statement fails to provide the condition of time, which for any human attacker would be finite, and includes a form of the equivocation fallacy which qualifies the attacker's desire. Therefore, if no attacker has entered then they apparently didn't want in "badly enough". Furthermore, the statement makes a use of the phrase "get in" too broadly so that the idea is gaining entry but could be further applied to any number of potential, harmful attacks.

3. **There is no perfect security.**
   The statement fails to provide the condition of time implying the axiom means "ever" which is itself an absolute and difficult to prove. This short statement also falls into the categories of two logical fallacies, the Nirvana fallacy and the Perfect Solution fallacy. In the Nirvana fallacy, we are mislead to reject something because it cannot be perfect. However, it can be good enough for one's needs. In the Perfect Solution fallacy, the argument assumes a perfect solution even exists. This assumption is easy to argue in terms of products for those who only understand security concepts in terms of products. In reality, "perfect" is a subjective concept and what may not be perfect for one person may indeed be perfect for another. Within the context of this manual, "perfect" means a perfectly balanced equation when calculating the attack surface consisting of OpSec and Limitations against Controls.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

4. **Security is a process not a product.**
   While this statement is meant to inform those who think of security in terms of products, this catchphrase actually uses the fallacies of False Dilemma and Presumption to persuade. As a False Dilemma, it states that there are only two choices, a product and a process and therefore security must be one or the other. As a Presumption, the conclusion of the statement is already presumed as a process being the means to security. Together, these fallacies do not allow for products and processes to combine in the formation of security nor does it allow for something else entirely different. In reality, the public definition of security is ill defined and not actually achievable, which is the likely reason for all these axioms in the first place. This leaves room for many interpretations of what security can be and the main reason why the Analyst must commit to an achievable, measurable definition of security. To state then that security is one thing or another is false especially when security itself is undefined and lends itself to standard, dictionary interpretations. It is also why this manual clearly defines security as something measurable.

An Analyst is required to apply critical security thinking skills to information as it is provided as well as to statements which are made about the analyzed information to form factual intelligence. Intelligence created in such a manner will provide accurate and unbiased metrics as well as a clear understanding of how security is deficient without the need for qualifiers.

## 3.2 Recognize the OpSec Model

There are two problems with security analysis in practical use on operations. The first is that technology is often far ahead of every Analyst's ability to understand how all of it works, if this know-how is even possible to obtain under the current closed-box status of most commercial technology products. The second problem is that ironically, the deconstruction of how something works, including business processes, may be illegal in order to protect the financial risk and privacy of the manufacturer from the buyer even though as a user of the product, the buyer may actually need that information to protect themselves from real threats which are probably not their customers. However, even in cases where a technology or process cannot be analyzed directly, the product can be analyzed within the environment with which it interacts.

For each vector and channel that is analyzed, the Analyst will be putting an overlay of the OpSec model over the targets. To apply the OpSec model is simply to count the controls for each interactive point of Access or Trust as well as the discovery of opportunity in the form of Visibility. Where a target is an unknown like a black box which can't be opened, the Analyst needs to address the controls over the system's interactions in its environment. The process will look like this:

1. What is visible in the scope? What is of possible value that is known? What targets can be determined?
2. What are the interactive Access points to those targets and from what vector or channel?
3. What are the Trusts within the scope and over what vector or channel?
4. Which are the controls for those Accesses and Trusts?
5. Are the controls complete or do they have limitations?

Even a quick application of the OpSec model will tell you if an Access or a Trust is balanced with controls. This will tell you the size of the attack surface and which interactive points are open without any controls to govern them.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 3.3 Look for Pattern Matching as a Sign of Errors

If you begin by looking for exactly what you seek then you may only find what you expect to find. This is adequate when looking for matching socks but not so good when looking at the big picture of an attack surface. It is the major problem known as pattern matching, the human trait to skip over steps, sometimes unknowingly, which are considered unnecessary due to an "obvious" outcome. It also makes people see cause and effect where there may be none. It is a blind spot which Analysts will develop after years of doing initial, basic, or redundant tasks. These tasks are made more efficient through short-cuts which affect the quality of the verification tests and ultimately the analysis.

For actionable intelligence, a result is only as good as the methods used to get them. Not knowing how you got a particular result will severely limit the action you can take to fix it. When an Analyst uses pattern matching to skip steps, the method cannot be properly known. Still, the desire to "cut to the chase" to get to the meat of a problem while presuming a state which is actually unknown is a problem in many areas of science. Security is no exception. Therefore an Analyst must recognize when tests have been skipped or the data fudged to provide unverified results.

To detect pattern matching, examine the test methods and result data for the following:

1. Tests using specific threats instead of a thorough interaction with the attack surface.
2. The lack of details on resulting processes behind interactions with the target.
3. Little or no information about controls for various targets.
4. Only some of the targets are reported for certain tests and those have completely negative results.
5. Targets not tested for reasons which are anecdotal (notes where a person has said there is nothing there to test or has been secured).
6. Tests of targets which have obviously not been secured.

## 3.4 Characterize the Results

The scientific method is not a checklist. It is a process which allows for intelligence and imagination. A hypothesis is made and then data is collected through testing and observation to evaluate that hypothesis. In a security test, a hypothesis is essentially made whenever a verification is made against a direct or indirect interactive point in the scope. The Analyst has the empirical data from those tests and must consider if the tests actually verified the hypothesis. Were the right tests made? Were enough tests made? Were the right channels or vectors tested? Were new interactions created that were also then tested? To do this, we characterize the results.

To characterize a security test using the scientific method is to discover the properties of the scope to assure the correct tests were made for it. The tester makes a hypothesis as to the interactivity of a point in the attack surface. The test will return that the point is interactive and adds to the attack surface or not interactive and whether it still adds to the attack surface, controls in place, any limitations in those controls, any limitations in the defined security, and any anomalies. At this point the Analyst may be wrong about the function of the process in operation however the Analyst may not be wrong in which tests should be used to verify what the function actually is. This is why both knowledge of the process and creatively imagining the indirect interaction are necessary.

For example, the Analyst may characterize a process as including the interaction between a visitor and the network via the access card. So while this visitor does not have the credentials to access the network, because the card reader is tied into the computer system, that visitor does access the network by swiping the card. The Analyst must consider how to test what happens when the visitor interacts with the card reader to gain access as well as the side effects of having the card read. However, even if the tests show that the card reader is connected to a stand-alone computer system and is not attached to the network,

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

the Analyst has properly verified that the right tests were made against the right targets to get that answer.

Therefore, the Analyst will examine the scope for where an interaction might occur as well as where operations show interactions do occur. This will allow a characterization of the points of interaction, any possible indirect interactions, and all side effects from such interactions. This characterization must be then matched with the tests made to determine if all the correct tests were made.

## 3.5 Look for Signs of Intuition

One thing that machines are clearly better than humans at is consistency. Humans generally get bored, confused, or careless. When a machine counts coins, it doesn't lose count and need to start over. It doesn't doubt itself and start over. It also won't use intuition. Also called "gut instinct" the power of intuition is incredible. It allows people to imagine, apply creativity to a job, and know when something feels wrong. It's part of the human condition to subconsciously detect problems and prepare accordingly. However it's exactly this that sometimes leads us to make mistakes. This is never more obvious than when we count large amounts of similar-looking objects. Without total concentration, we may begin to feel uneasy about the tally and eventually we may feel compelled to either start over or just accept a particular correct-sounding number where we think we left off and continue from there.

There is a time when a test requires precise concentration; during a large number of repetitive sequences. Generally, we tend to create tools to handle this type of repetition however it may not always be possible due to the dynamic nature of the test like when interacting with people instead of inanimate objects or machines. So as the test progresses, the tester may use intuition to make the presumption that the test will be unnecessary. The Analyst must pay special attention to these tests and look for signs of intuition in part of the tester.

Signs of trouble from intuition in tests are:

1. Inconsistencies of types of tests performed across multiple, similar targets.
2. The number of tests decrease between targets.
3. The length of time for tests decrease between targets.
4. The same target tested more than once with the same tests.

Detection of intuition in tests will show an inadequate testing process and the quality of the results should be regarded with suspicion. Re-testing may be necessary.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 3.6 Transparent Reporting

Rarely will a security analysis end with all the answers. Since the tests will depend on the OpSec and controls of a particular channel and vector there will be unknowns. There may be a visible target which provides no interaction and no further information about that target can be determined from this vector and this channel. This is correct. The Analyst should report what has been found with certainty and not merely what could be. There is no place for guessing when measuring an attack surface.

In addition to information about the test itself as to how it was made, the Analyst will need to report the following 7 test results:

**1. Unknowns**
As more vectors and channels are analyzed, more information will be available and that which is reported will change and provide actionable intelligence. Conversely, maybe more results are inconclusive or the correlation of results provide conflicting answers, the resulting actionable intelligence is unknown. Unknown is a valid answer to report. What cannot be known is as valid and as important in security as what is discovered. What is unknown shows what is difficult to test or analyze. The unknown need not be seen as a failure of the tester rather it may be caused by superior protection or an attack that uses a large cost of time or resources not possible in a test. No Analyst should fear reporting something is unknown. It is a powerful result to base further risk analysis upon.

**2. Untested Targets**
Additionally, the Analyst needs to report another type of unknown - targets in the scope which have not been tested in a particular vector or channel. If a test cannot be completed because of time constraints, tool limitations, targets being unstable, the test environment being too dynamic or too noisy to collect proper results, or because the tests were not wanted by the target owner then this needs to be known. By reporting what was not tested, it is possible to do proper test comparisons with future tests. It will also help avoid cheating by only testing the well protected segment of a scope and ignoring the rest to create the illusion of a small attack surface.

**3. Identified and Verified Limitations**
Besides unknowns, the Analyst must also report any identified and verified limitations such as vulnerabilities in the targets. An identified limitation is one which has been determined through knowledge and correlation. This is useful when the tests themselves are dangerous or very costly. Sometimes a test can be damaging to a target or cause unacceptable or even criminal collateral damage. A verified limitation is one where the problem has been specifically tested to determine if it exists.

**4. False Positives and the Means to Generate Them**
During tests, some identified limitations will not be vulnerable to those particular attacks during verification. This, however does not conclude that the target does not have those limitations. It only means that particular test at that particular time and from that particular tester did not expose the vulnerability as identified. It could also mean the target is vulnerable but is protected by a particular control. Such determined false positives should be reported so that during further development of protective and defensive techniques, the problem can be looked at more closely, particularly from a different vector.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

**5. Failed Security Processes and Procedures**
During analysis, test results will show more than just the OpSec, types of controls, and number of limitations. It will show a bigger picture, one of processes and procedures that are in use to formalize protective measures. These can be about anything that are designed to get the protection measures to their current state. This includes but is not limited to maintenance, procurement, identification, authorization, housekeeping, disaster recovery, partner relations, policy generation, climate control, and human resources. When a target has a limitation often times there is a failed process or procedure behind it. The Analyst should be able to determine exactly what it is from the aggregate test results.

**6. Good Practices**
The term "Best Practices" is used to explain the best way for a person or organization to do something. Unfortunately, this has been abused to the point where it now means that it's best for everyone. This itself has caused problems and wasted resources. One way to counter this problem is to use the aggregate test results to show practices which are successful. This will show what can be repeated for equivalent success in other areas of the organization and defining a customized "Best Practice" for them. It will also lessen their reliance on industry-wide Best Practices in favor of what works best for them.

**7. Compliance**
Should specific compliance objectives need to be reached, the Analyst needs to use the correlated test results to determine if these objectives have been met. This may need to be provided in a special format as determined by the auditor however the Analyst is best equipped to show which test results provide the necessary information.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

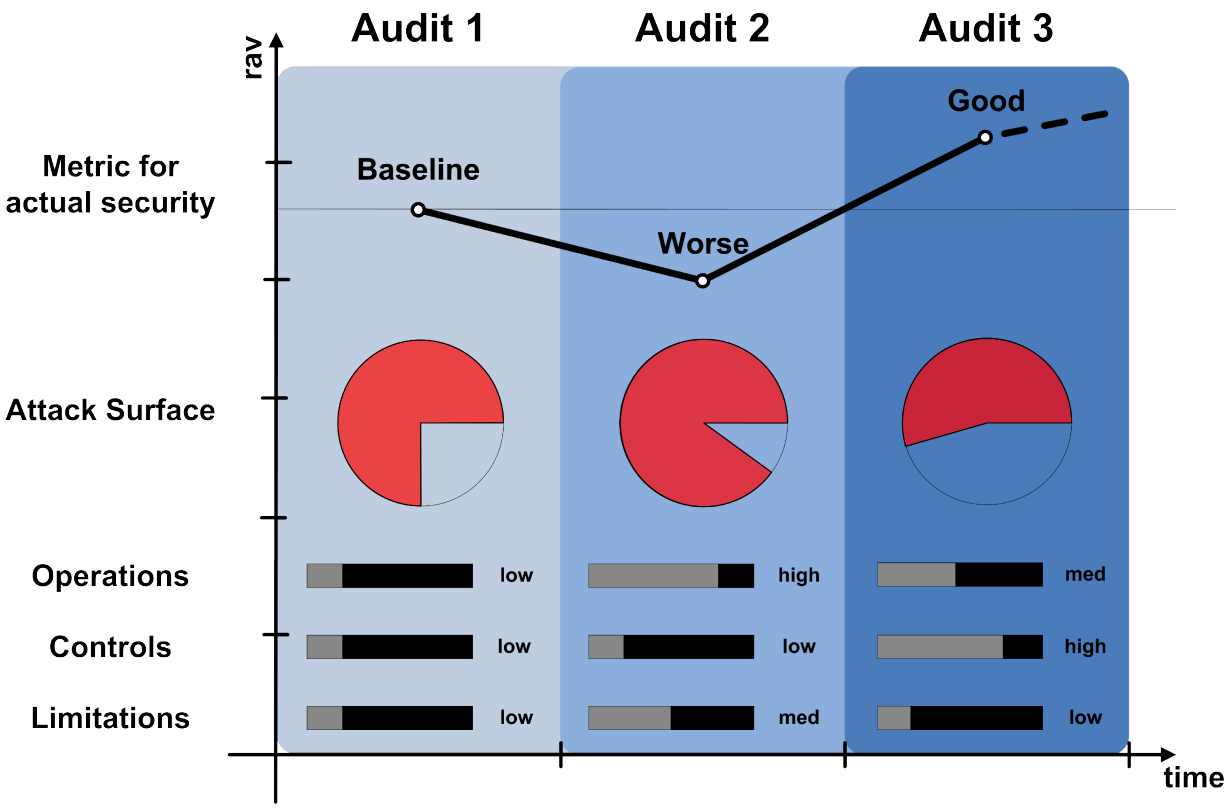
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

**Risk assessment is a concept for selecting security and controls based on presumed risk. It works for defining strategy. Security testing however is verifying to what completeness that security or those controls exist. It works for defining operations. To test you don't make a risk assessment because doing so would restrict your potential and your findings. After all, you shouldn't be making the same guesses they are.**

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

# Chapter 4 – Operational Security Metrics

Operational security metrics are the metrics we are most familiar with in our lives. When we measure the height, width, or length of an object we are using an operational metric. When we write the date, have a birthday, or ask the score of a game we are using operational metrics. An operational metric is a constant measurement that informs us of a factual count in relation to the physical world we live in. They are operational because they are numbers we can work with consistently from day to day and person to person. It is difficult to work with relative or inconsistent measurements like choosing a specific hue of yellow to paint a room, starting work at sunrise, having the right flavor of strawberry for a milkshake, or preparing for the next threat to affect your organization's profits because the factors have many variables which are biased or frequently changing between people, regions, customs, and locations. For this reason, many professions attempt to standardize such things like flavors, colors, and work hours. This is done through reductionism, a process of finding the elements of such things and building them up from there by quantifying those elements. This way, colors become frequencies, work hours become hours and minutes, flavors become chemical compounds, and an attack surface becomes porosity, controls, and limitations. The only real problem with operational metrics is the requirement for knowing how to properly apply the metric for it to be useful.




*Using ravs to measure and track the security of anything over time.*

The completion of a thorough security test has the advantage of providing accurate metrics on the state of security. As with the use of any metric. the less thorough the test, the less accurate the overall metric. Less skilled or less experienced Analysts will also adversely affect the quality of the metric just as people who can't tell time can't build clocks, designers without the right tools can't match colors exactly, and

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

brew masters who can't measure the ingredients in beer can't make similar batches repeatedly for market. Therefore a successful security metric requires a test which can be described as measuring the appropriate vectors while accounting for inaccuracies and misrepresentations in the collected test data as well as the skills or experience of the security professionals performing the test. Faults in these requirements result in lower quality measurements and false security determinations therefore the metric must also be simple enough to use without making it so simple that it tells nothing. Furthermore, a proper security metric must avoid the biases inherent in risk assessments by assuring measurements have integrity. These qualities have been combined to create the ravs, an unbiased, factual description of an attack surface.

## 4.1 Getting to Know the Rav

The rav is a scale measurement of the attack surface, the amount of uncontrolled interactions with a target, which is calculated by the quantitative balance between operations, limitations, and controls. Having the ravs is to understand how much of the attack surface is exposed. In this scale, 100 rav (also shown as 100% rav for simplicity of understanding although not precisely a percentage) is perfect balance and anything less is too few controls and therefore a greater attack surface. More than 100 rav shows more controls than are necessary which itself may be a problem as controls often add interactions within a scope as well as complexity and maintenance issues.

The rav does not measure risk for an attack surface, rather it enables the measurement of it. It cannot say if a particular target will be attacked however it can say where on a target it will be attacked, what types of attacks the target can successfully defend against, how deep an attacker can get, and how much damage can be done. With that information it is then possible to assess the trusts (and risks) much more accurately.

The rav is actually multiple separate calculations of Porosity, Controls, and Limitations, that when combined will show the size of an attack surface in two practical ways. The first way is in a straight calculation. It is the calculation of the Delta, a number that describes the specific exposure of that target. This is useful for determining how a new person, thing, or process will change the operational security of a new scope or as a comparison between multiple, single targets. This is also the easiest way to see Perfect Security, the perfect balance between Porosity, Controls, and Limitations. The rav is displayed as a positive or negative number which shows how far away the target is from a perfect security balance. A positive delta shows too much is spent on controls in general or even if the overspending is on too much of one type of control. A negative delta shows a lack of controls or controls themselves with limitations which cannot protect the target adequately. This is a powerful tool for knowing exactly where and how resources are being spent to protect a particular target. However this is not how the rav is most useful; that is done best the second way.

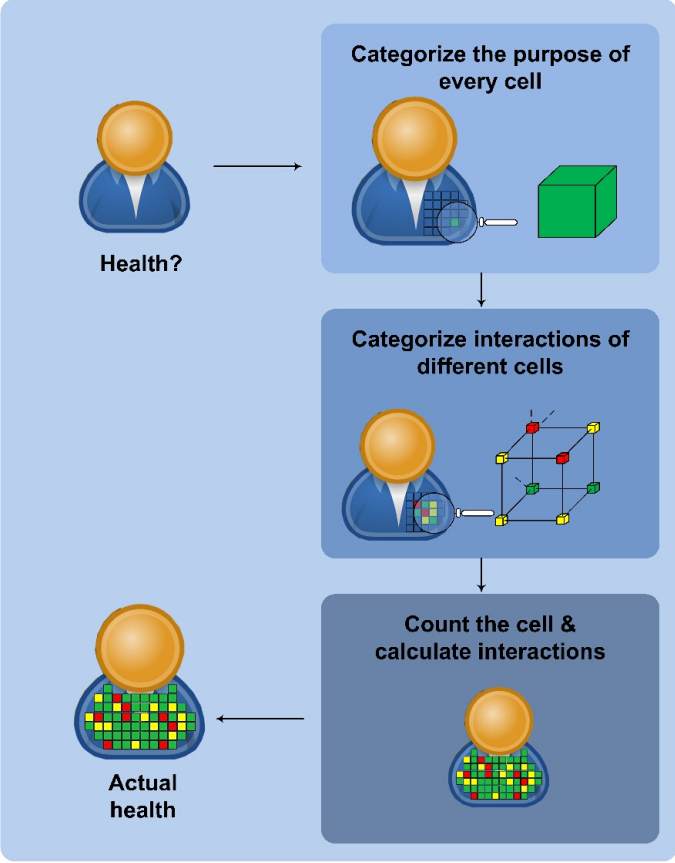
The second practical way to display the attack surface is for understanding the big picture. This is represented as Actual Security. Where the Delta calculation is based on perfect balance, the Actual Security calculation uses the Delta but also includes additional and redundant controls to provide a metric more people friendly and familiar. Here the rav representation is similar to how people use percentages. The rav is calculated with a base 10 logarithm, which makes a more comprehensible representation. While the rav is still a balance, perfect balance is set at 100 and calculations are made in respect to that. This will allow most people to have a quick and easy overview of all the targets in a scope or of just a single target in relation to other targets. It is extremely flexible so multiple attack surfaces can be compared by Actual Security even if the scope or the targets are very different: 95% rav of a scope with 1000 computer systems is comparable to 95% rav with just 10 systems, which can be again compared to a building with a 95% rav. All three will provide the same information to a person that the protection of the target is 5% deficient and therefore exposed to attack. With this knowledge, one can begin to assess risk and determine what is exposed, what is left uncontrolled, and if that 5% is acceptable. So for whatever threat there is, it can only occur where the openings are and that will sharpen the exactness of a risk analysis from broad sword to scalpel.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *What Is a Rav Like?*

A rav is a little different from other security measurements because the count is unique from the scope. That is like determining the overall size of a person by counting all the cells in them and categorizing them by what they do to determine the person's overall health. For a rav, both the count and the operation are required. This is why the rav can only be derived from operational security testing.

Imagine a machine exists that can audit all the cells in a human body. This machine works by monitoring the cells in their environment and even prodding each cell in a way it can react to better categorize its purpose. We could then see what various cells do and how they contribute to the overall make-up of the human body. Some cells make up tissue walls like skin cells do. Some, like white blood cells, provide authentication and attack other cells which are on its "bad" list. Then some cells are foreigners, like bacteria which have entered at some point and thrived. The machine would classify all the cells that make up the person, a defined scope, rather than say which are "bad" or "good".




*The ravs are like counting cells and classifying them by what they do to determine how well the organism fits into an environment.*

By counting the cells the machine can tell mostly how well the person as an organism works (health) and how well they fit into their current environment. It can also determine which cells are broken, which are superfluous, and of which type more might be required for the person to be more efficient, prepared for the unexpected, or for any number of specific requirements. Since the cells are dividing and dying all the time, the machine must also make regular tests and chart the person's ability to improve or at least maintain homeostasis.

Now in addition to counting cells and seeing how they work, the machine will also see with which other cells or under what conditions they interact and how well. In each operation of the cell's duties the machine can determine what the cells limitations are. So if it was possible for the machine to also repair a problem in faulty cells directly, fortify the body by changing the process of the cells, or removing the unnecessary cells, we would be able to directly affect the health of the body as a whole with each change. Or perhaps we might change the environment that the body is exposed to instead of the cells to make more global changes. By subjecting the person to better nutrition, diet, or exercise we will also change the body on a cellular level. All this is possible by knowing how things work inside the body and what's there in these operations.

Unfortunately there is no such machine for counting all cells in a human body. However it does exist for security. Analysts can count and verify the operations of targets in a scope as if it is a super-organism. They record its interactions and the controls surrounding those interactions. They classify them by operation, resources, processes, and limitations. Those numbers the Analysts generate are combined so that controls add to operational security and limitations take away from it. Even the value of the limitations, how badly each type of problem hurts, is also not arbitrary because it's based on the combination of security and controls within that particular scope. So a bad problem in a protective environment will provide less over-all exposure than one in a less controlled environment.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *Eight Fundamental Security Answers*

The rav does not represent risk where risk is known as Risk = Threat x Vulnerability x Asset. In that equation, risk is the result of an informed, however highly biased, equation. If we can remove most of the bias by knowing the level of protection and therefore the level of vulnerability impact, we can reduce the bias in that equation and give a much better risk assessment. Therefore, the rav is actually the factual foundation for a risk assessment where an Analyst has facts to work with. The real power of the rav however is how it can provide answers to the following eight fundamental security questions with great accuracy.

1. *How much money should be spent on security?*

   The rav will show the current amount of protection to make security projections and define milestones even before buying a particular solution or implementing some new process. From these projections and milestones, financial restrictions can be created to meet the goals and get the most specific results from the investment. By knowing exactly what is controlled based on the current expenditure, you can also see what is not being controlled for that money. "More" then becomes that which is missing. It is then possible to forecast the cost of filling in the missing controls to achieve a perfect balance or at least a decidedly acceptable level of coverage.

2. *What should be protected first?*

   The rav can be used to see security as part of the big picture and as a macro lens on a particular part of a target, or any combination thereof. After analysis, the rav will show which particular part of the scope has the greatest porosity and the weakest controls. Comparing that to one's needs and asset worth, a ratio of protection strength to value can be generated to decide exactly where to start.

3. *What protection solutions do we need and how should we set them up for maximum effectiveness?*

   A fully completed rav will show the 10 possible operational controls applied for each target and the limitations of those controls. You can then choose solutions based on which types of controls you want to put in place. The difference now is that you no longer need to look at a solution in terms of what it is rather than as the protection or controls it can provide. This allows you to view products for the controls you need to provide in the areas where controls are currently deficient.

4. *How much improvement is gained by specific security procurements and processes?*

   A key feature of the rav is that you can make a "Delta" by mapping out the benefits and limitations of a particular solution for comparison prior to procurement. This means you can see what changes that solution will make to the scope to compare with other solutions. Combining that map to a rav of the scope where the solution would be placed, the amount of improvement can be gauged even prior to purchase. You can even predict the value of that protection by dividing the price of the solution by the rav delta.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

5. *How do we measure the periodic security efforts and improvements?*

   With regular audits, the rav can be recalculated and compared to the older value. Thereby the cost of new solutions and processes can be justified regularly as well as the cost of maintaining the current security level.

6. *How do we know if we are reducing our exposure to our threats?*

   With specific knowledge of your controls, you can easily tell what part or vector of the scope is weak to specific and most unknown threats. In rav terminology, an unknown threat is just one that can appear where interactions exist but controls do not. Therefore a map can be drawn between the threats determined by the Risk Assessors and the controls in place. Regular metric reviews will show any change in this map and can be done so regularly. Then it is possible to gauge the cost each of those threats has on security by the expenditure on controls.

7. *Can the rav tell us how well something resists attacks?*

   Technically, yes. The more you can balance controls with interactions, the smaller the attack surface will be and the more capable the target will have to control known and unknown types of interactions.

8. *Can the rav help me with regulatory compliance?*

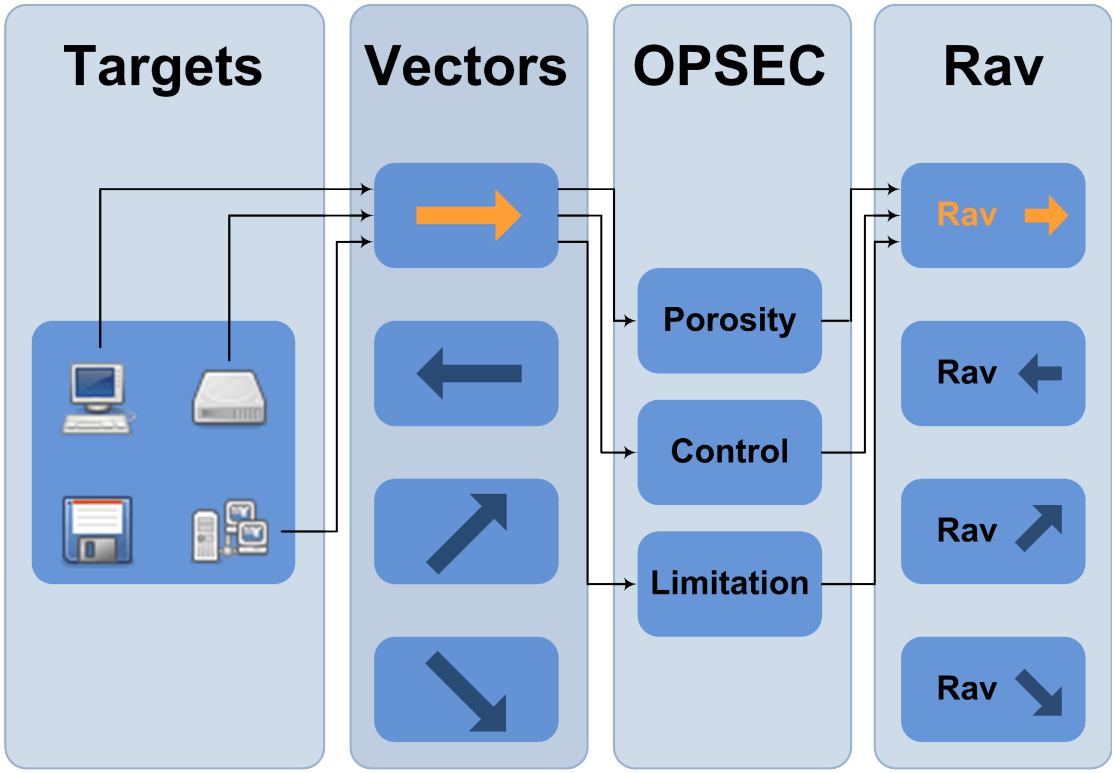
   Anything that helps you classify all controls and Access points in a scope will help you with compliance audits. The rav helps you do such a good job of getting your security under control that you may even find the major flaws in compliance regulations. While there is no particular compliance right now that asks you to have a particular rav score, showing the OSSTMM STAR with its rav score will help you meet various compliance requirements for a third-party audit and documentation.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 4.2 How to Make a Rav

The rav requires a security test in order to have the right things counted and the right operations analyzed. Any security test can be used but the more thorough and accurate the test the more the conclusive the results will be. The rav was originally designed for operations tests, like the OSSTMM, where the auditor focuses on the behavior of the target rather than the configuration. However experiments show it is possible to apply the rav to non-operational tests as well such as in static code analysis to determine the level of software security and complexity or in physical security checklist audits to determine the level of protection a physical space will provide. The SCARE (Source Code Analysis Risk Evaluation) project does exactly this by applying the ravs to C source code.




*The simplicity of making a rav from a security test.*

The minimum rav is made by the calculation of porosity which are the holes in the scope. The problem with security metrics is generally in the determination of the assessors to count what they can't possibly really know. This problem does not exist in the rav. You get what you know from what is there for a particular vector and you make no assumptions surrounding what is not there. You count all that which is visible and interactive outside of the scope and allows for unauthenticated interaction between other targets in the scope. That becomes the porosity. This porosity value makes the first of 3 parts of the final rav value. The next part is to account for the controls in place per target. This means going target by target and determining where any of the 10 controls are in place such as Authentication, Subjugation, Non-repudiation, etc. Each control is valued as 10% of a pore since each provides 1/10$^{th}$ of the total controls needed to prevent all attack types. This is because having all 10 controls for each pore is functionally the same as closing the pore provided the controls have no limitations. The third part of the rav is accounting for the limitations found in the protection and the controls. These are also known as "vulnerabilities". The value of these limitations comes from the porosity and established controls themselves. With all counts completed, the rav is basically subtracting porosity and limitations from the controls. This is most easily done with the rav spreadsheet calculator.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

Unfortunately, an unskilled analyst can provide the wrong information which will translate into a bad rav. This is a possibility, just like it's possible a carpenter doesn't measure a board right or a mechanic fails to read the gauges right. The world is full of what-if scenarios. Therefore the rav is designed to be minimally influenced by bad auditing or cheating by eliminating the direct scope size from the metric calculation. However, no metric can be immune from fudging and the only way to assure the most accurate rav is to have multiple tests over time to make the counts and to be sure the auditor will take responsibility over the accuracy of the test.

It is possible to take a short-cut in testing and still make a representative rav. If you don't mind the error margin because you only want to make a quick comparison, you can just calculate the Porosity which means counting the visible and accessible targets. For example, those who run vulnerability scanners can count porosity and limitations relatively easily and assign default controls for discovered services. Analysts can also create a checklist which offers default controls for different common solutions found. These are all shortcuts to reduce the time to calculation but will affect the overall rav with an unknown, but perhaps acceptable, error margin.

The end result is a calculation for Actual Security. It applies multiple controls of the same type to satisfy double-enforcement requirements like 2-factor Authentication. It also uses Log10 to reduce large numbers into human-manageable form. People generally like to work with smaller numbers and especially as percentages which are easier to visualize. For a small scope, the accuracy of using Log10 as a reduction technique is negligible. However, if you have a very large scope with many targets you may want to work with the very large numbers for greater accuracy. Additionally if you want to see the true balance where multiple controls of the same type are not measured, that calculation can be found under the heading of True Protection.

### *Combining Channels and Vectors*

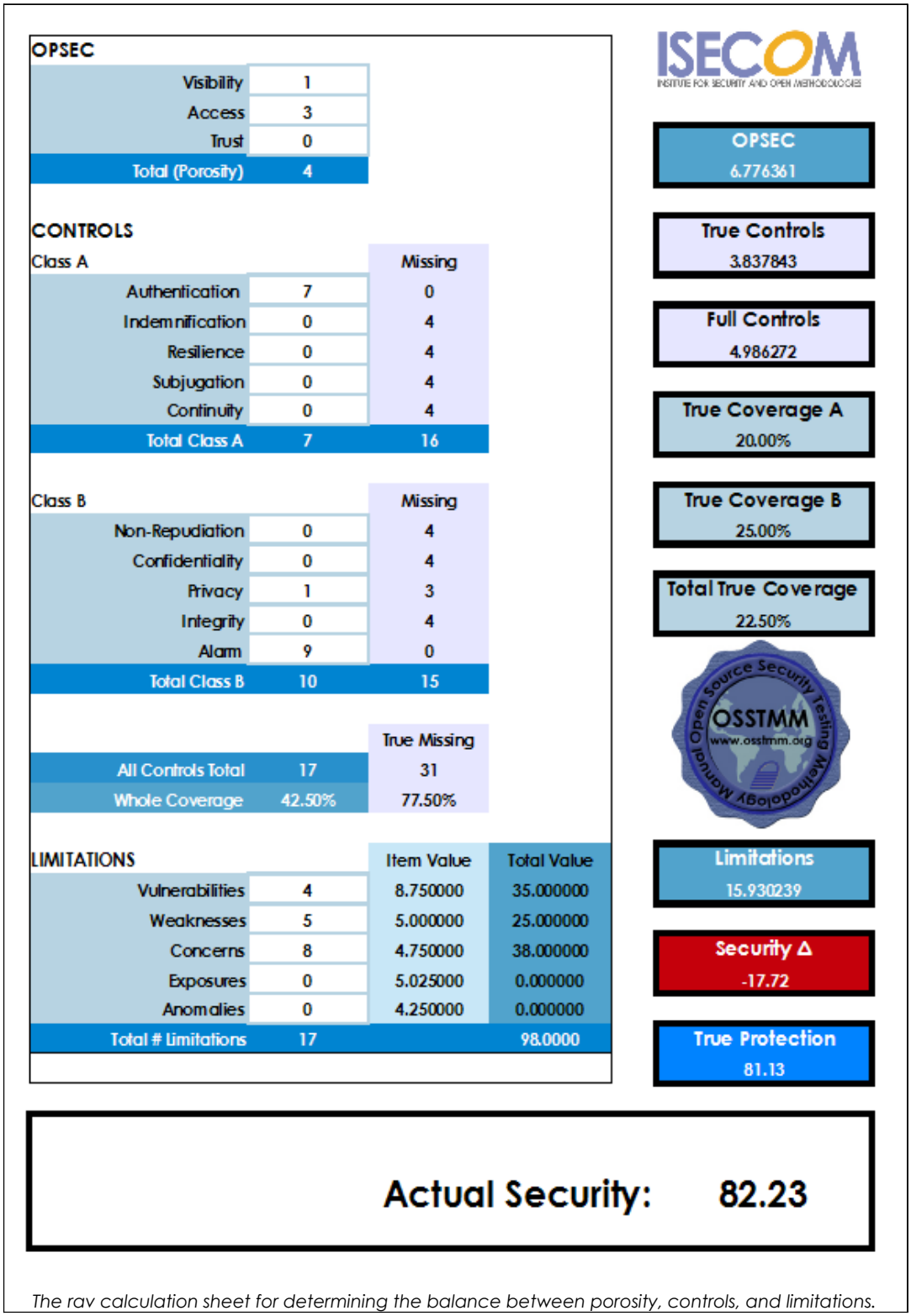
One important requirement in applying the rav is that Actual Security can only be calculated per scope. A change in channel, vector, or index is a new scope and a new calculation for Actual Security. However, once calculated, multiple scopes can be combined together in aggregate to create one Actual Security that represents a fuller vision of the operational security all scopes. For example, a test can be made of Internet-facing servers from both the Internet side and from within the perimeter network where the servers reside. That is 2 vectors. Assume that, the Internet vector is indexed by IP address and contains 50 targets. The intranet vector is indexed by MAC address and is made of 100 targets because less controls exist internally to allow for more collaborative interaction between systems. Once each test is completed and the rav is counted they can be combined into one calculation of 150 targets as well as the sums of each limitations and controls. This will give a final Actual Security metric which is more complete for that perimeter network than either test would provide alone. It would also be possible to add the analysis from physical security, wireless, telecommunications, and human security tests in the same way. Such combinations are possible to create a better understanding of the total security in a holistic way.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *Rav Calculator*

A straight-forward and simpler way to make ravs is to use the specifically created spreadsheets to calculate the Attack Surface and various, popular required metrics from the test data. This spreadsheet is available at the ISECOM website. The Analyst need only enter the values into the empty, white boxes and the rest of the calculations will be handled automatically.



| OPSEC | |
|---|---|
| Visibility | 1 |
| Access | 3 |
| Trust | 0 |
| Total (Porosity) | 4 |

| CONTROLS | | |
|---|---|---|
| Class A | | Missing |
| Authentication | 7 | 0 |
| Indemnification | 0 | 4 |
| Resilience | 0 | 4 |
| Subjugation | 0 | 4 |
| Continuity | 0 | 4 |
| Total Class A | 7 | 16 |
| Class B | | Missing |
| Non-Repudiation | 0 | 4 |
| Confidentiality | 0 | 4 |
| Privacy | 1 | 3 |
| Integrity | 0 | 4 |
| Alarm | 9 | 0 |
| Total Class B | 10 | 15 |
| | | True Missing |
| All Controls Total | 17 | 31 |
| Whole Coverage | 42.50% | 77.50% |

| LIMITATIONS | | Item Value | Total Value |
|---|---|---|---|
| Vulnerabilities | 4 | 8.750000 | 35.000000 |
| Weaknesses | 5 | 5.000000 | 25.000000 |
| Concerns | 8 | 4.750000 | 38.000000 |
| Exposures | 0 | 5.025000 | 0.000000 |
| Anomalies | 0 | 4.250000 | 0.000000 |
| Total # Limitations | 17 | | 98.0000 |



*The rav calculation sheet for determining the balance between porosity, controls, and limitations.*

## 4.3 Turning Test Results into an Attack Surface Measurement

### *Operational Security*

The measurement of the Attack Surface requires the measurements of Visibility, Trust, and Access relative to the scope. The number of targets in the scope that can be determined to exist by direct interaction, indirect interaction, or passive emanations is its visibility. As visibility is determined, its value represents the number of targets in the scope. Trust is any non-authenticated interaction to any of the targets. Access is the number of interaction points with each target.

| Category | | Description |
|---|---|---|
| | | |
| 1 | ***Visibility*** | The number of targets in the scope. Count all targets by index only once and maintain the index consistently for all targets. It is generally unrealistic to have more targets visible than there are targets in the defined scope; however, it may be possible due to vector bleeds where a target which is normally not visible from one vector is visible due to a misconfiguration or anomaly.<br><br>A HUMSEC audit employs 50 people; however, only 38 of them are interactive from the test vector and channel. This would make a visibility of 38. |
| 2 | ***Access*** | This differs from visibility where one is determining the number of existing targets. Here, the auditor must count each Access per unique interaction point per unique probe.<br><br>In a PHYSSEC audit, a building with 2 doors and 5 windows which all open has an Access of 7. If all the doors and windows are sealed, then it is an Access of 0 as these are not points where one can gain entry.<br><br>For a COMSEC audit of data networks, the auditor counts each port response as an Access regardless of how many different ways the auditor can probe that port. However, if a service is not hosted at that port (daemon or an application), then all replies instead come from the IP Stack. Therefore, a server that responds with a SYN/ACK and service interactivity to only one of the TCP ports scanned and with a RST to the rest does not have an Access count of 65536 (including port 0) since 66535 of the ports respond with the same response of RST from the kernel. To simplify, count only ports with service responses and only one IP Stack response regardless of the number of ports which can initiate this kind of interactivity.<br><br>With HUMSEC audits, this is much more simplified. A person who responds to a query counts as an Access with all types of queries (all the different questions you may ask or statements made count as the same type of response on the same channel). Therefore, a person can only be an Access of 1 per channel and vector. Only a person who completely ignores the request by not acknowledging the channel is not counted. |


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

| Category | | | Description |
|---|---|---|---|
| | | | |
| 3 | | ***Trust*** | This differs from visibility where one is determining the number of existing targets. Here, the auditor must count each Trust per unique interaction point per unique probe.<br><br>In a PHYSSEC audit, a building with 2 internal doors separating rooms which open has a Trust of 2. If those doors are sealed then it is a Trust of 0 as these are not points where one can pass.<br><br>For a COMSEC audit of data networks, the auditor counts each type of service forward or port forward as a Trust.<br><br>With HUMSEC audits, a person who acts as a gateway to interact with other people or to access property is a trust per channel. Therefore, a person can only be a Trust of 1 per channel and vector. Only a person who does not comply to the Trust request is not counted. |

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *Controls*

The next step in calculating the rav is to define the Controls; the security mechanisms put in place to provide assurance and protection during interactions.

| Category | | | Description |
|---|---|---|---|
| | | | |
| 1 | | ***Authentication*** | Count each instance of authentication required to gain access. This requires that authorization and identification make up the process for the proper use of the authentication mechanism.<br><br>In a PHYSSEC audit, if both a special ID card and a thumb print scan is required to gain access, then add two for authentication. However, if Access just requires one or the other, then only count one. |
| 2 | | ***Indemnification*** | Count each instance of methods used to exact liability and insure compensation for all assets within the scope.<br><br>A basic PHYSSEC example is a warning sign threatening to prosecute trespassers. Another common example is property insurance. In a scope of 200 computers, a blanket insurance policy against theft applies to all 200 and therefore is a count of 200. However, do not confuse the method with the flaw in the method. A threat to prosecute without the ability or will to prosecute is still an indemnification method-- however, it is with a limitation. |
| 3 | | ***Subjugation*** | Count each instance for Access or Trust in the scope which strictly does not allow for controls to follow user discretion or originate outside of itself. This differs from being a security limitation in the target since it applies to the design or implementation of controls.<br><br>In a COMSEC data networks audit, if a log-in can be made in HTTP as well as HTTPS but requires the user to make that distinction, then it fails to count toward Subjugation. However, if the implementation requires the secured mode by default, such as a PKI internal messaging system, then it does meet the requirement of the Subjugation control for that scope.<br><br>More simply, in HUMSEC, a non-repudiation process where the person must sign a register and provide an identification number to receive a document is under Subjugation controls when the provider of the document records the identification number, rather than having the receiver do so, to eliminate the recording of a false number with a false name. |


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

| Category | | | Description |
|---|---|---|---|
| | | | |
| 4 | | ***Continuity*** | Count each instance for Access or Trust in the scope which assures that no interruption in interaction over the channel and vector can be caused, even under situations of total failure. Continuity is the umbrella term for characteristics such as survivability, load balancing, and redundancy.<br><br>In a PHYSSEC audit, if it is discovered that an entry way into a store becomes blocked such that no alternate entry way is possible and customers cannot enter, that Access does not have Continuity.<br><br>In a COMSEC data networks audit, if a web server service fails from high-load and an alternate web server provides redundancy so no interactions are lost, this Access has Continuity. |
| 5 | | ***Resilience*** | Count each instance for Access or Trust in the scope that does not fail open or provide new accesses upon security failure. In common language, to "fail securely".<br><br>In a PHYSSEC audit where 2 guards control Access to a door, if one is removed and the door cannot be opened by the remaining guard, then it has resilience.<br><br>In a COMSEC data networks audit, if a web service requiring a log-in or password loses communication with its authentication database, then all Access should be denied rather than permitted in order to have resilience. |
| 6 | | ***Non-repudiation*** | Count each instance for the Access or Trust that provides a non-repudiation mechanism for each interaction to provide assurance that the particular interaction did occur at a particular time between the identified parties. Non-repudiation depends upon identification and authorization to be properly established for it to be properly applied without limitations.<br><br>In a PHYSSEC audit, the Non-repudiation control exists if the entrance to a building requires a camera with a biometric face scan to gain entry and each time it is used, the time of entry is recorded with the ID. However, if a key-card is used instead, the Non-repudiation control requires a synchronized, time-coded camera to assure the record of the card-user's identity to avoid being a flawed implementation. If the door is tried without the key card, not having the synchronized camera monitoring the door would mean that not all interactions with the entryway have the Non-repudiation control and therefore does not count for this control.<br><br>In a COMSEC data networks audit, there may be multiple log files for non-repudiation. A port scan interacting at the IP Stack is recorded in one log while interaction with the web service is recorded to another log file. However, as the web service may not log the interactions from the POST method, the control is still counted; however, so is the security limitation. |

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

| Category | | | Description |
|---|---|---|---|
| | | | |
| 7 | | ***Confidentiality*** | Count each instance for Access or Trust in the scope that provides the means to maintain the content of undisclosed interactions between the interacting parties.<br><br>A typical tool for Confidentiality is encryption. Additionally, obfuscation of the content of an interaction is also a type of confidentiality, albeit a flawed one.<br><br>In HUMSEC, however, a method of Confidentiality may include whispering or using hand signals. |
| 8 | | ***Privacy*** | Count each instance for Access or Trust in the scope that provides the means to maintain the method of undisclosed interactions between the interacting parties. While "being private" is a common expression, the phrase is a bad example of privacy as a loss control because it includes elements of confidentiality. As a loss control, when something is done "in private" it means that only "the doing" is private but the content of the interaction may not be.<br><br>A typical tool for Privacy is obscuring the interaction, that is, having the interaction take place outside of the visibility of third parties. Confusion of the means of interaction as obfuscation is another method of applying the Privacy control.<br><br>In HUMSEC, a method of Privacy may be simply taking the interaction into a closed room away from other people. In movies, we see techniques to create the Privacy control by setting two identical suitcases side by side, some type of incident to create confusion takes place, and the two people switch the suitcases in seemingly plain view. |
| 9 | | ***Integrity*** | Count each instance for Access or Trust in the scope which can assure that the interaction process and Access to assets has finality and cannot be corrupted, stopped, continued, redirected, or reversed without it being known to the parties involved. Integrity is a change control process.<br><br>In COMSEC data networks, encryption or a file hash can provide the Integrity control over the change of the file in transit.<br><br>In HUMSEC, segregation of duties and other corruption-reduction mechanisms provide Integrity control. Assuring integrity in personnel requires that two or more people are required for a single process to assure oversight of that process. This includes that no master Access to the whole process exists. There can be no person with full access and no master key to all doors. |


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

| Category | | | Description |
|---|---|---|---|
| | | | |
| 10 | | ***Alarm*** | Count each instance for Access or Trust which has a record or makes a notification when unauthorized and unintended porosity increases for the vector or restrictions and controls are compromised or corrupted.<br><br>In COMSEC data networks, count each server and service which a network-based intrusion detection system monitors. Or, count each service that maintains a monitored log of interaction. access logs count, even if they are not used to send a notification alert immediately, unless they are never monitored. However, logs which are not designed to be used for such notifications, such as a counter of packets sent and received, do not classify as an alarm as there is too little data stored. |

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *Limitations*

Finally, the limitations are verified where possible. The values of each Limitation are dependent on Porosity and Controls. This is different from the more common risk perspective where a vulnerability may be assigned a risk level based on what damage it can do, how easy it is to do, and the distance in range for the attack. Therefore the Limitation values are calculated based on the Porosity and Controls of the target they can be found on.

| Category | | | Description |
|---|---|---|---|
| | | | |
| 1 | | ***Vulnerability*** | Count separately each flaw or error that defies protections whereby a person or process can access, deny access to others, or hide itself or assets within the scope.<br><br>In PHYSSEC, a vulnerability can be as simple as a glass door, a metal gate corroded by the weather, a door that can be sealed by wedging coins into the gap between it and its frame, electronic equipment not sealed from pests such as ants or mice, a bootable CD drive on a PC, or a process that allows an employee to take a trashcan large enough to hide or transport assets out of the scope.<br><br>In HUMSEC, a vulnerability can be a cultural bias that does not allow an employee to question others who look out of place or a lack of training which leaves a new secretary to give out business information classified for internal use only.<br><br>In COMSEC data security, a vulnerability can be a flaw in software that allows an attacker to overwrite memory space to gain access, a computation flaw that allows an attacker to lock the CPU into 100% usage, or an operating system that allows enough data to be copied onto the disk until it cannot operate anymore.<br><br>In COMSEC telecommunications, a vulnerability can be a flaw in the pay phone system that allows sounds through the receiver to mimic coin drops, a telephone box that allows anyone to access anyone else's phone line, a voice mail system that provides messages from any phone anywhere, or a FAX machine that can be polled remotely to resend the last thing in memory to the caller's number.<br><br>In SPECSEC, a vulnerability can be hardware which can be overloaded and burnt out by higher powered versions of the same frequency or a near frequency, a standard receiver without special configurations which can access the data in the signal, a receiver which can be forced to accept a third-party signal in place of the intended one, or a wireless access point dropping connections near a microwave oven. |


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

| Category | | | Description |
|---|---|---|---|
| | | | |
| 2 | | ***Weakness*** | Count each flaw or error in the controls for interactivity: authentication, indemnification, resilience, subjugation, and continuity.<br><br>In PHYSSEC, a weakness can be a door lock that opens when a card is wedged between it and the door frame, a back-up generator with no fuel, or insurance that doesn't cover flood damage in a flood zone.<br><br>In HUMSEC, a weakness can be a process failure of a second guard to take the post of the guard who runs after an intruder or a cultural climate within a company for allowing friends into posted restricted spaces.<br><br>In COMSEC data security, a weakness can be a log-in that allows unlimited attempts or a web farm with round-robin DNS for load balancing yet each system also has a unique name for direct linking.<br><br>In COMSEC telecommunications, a weakness can be a PBX that still has the default administration passwords or a modem bank for remote access dial-in which does not log the caller numbers, time, and duration.<br><br>In SPECSEC, a weakness can be a wireless access point authenticating users based on MAC addresses (which can be spoofed) or an RFID security tag that no longer receives signals and therefore fails "open" after receiving a signal from a high power source. |
| 3 | | ***Concern*** | Count each flaw or error in process controls: non-repudiation, confidentiality, privacy, integrity, and alarm.<br><br>In PHYSSEC, a concern can be a door lock mechanism whose operation controls and key types are public, a back-up generator with no power meter or fuel gauge, an equipment process that does not require the employee to sign-out materials when received, or a fire alarm not loud enough to be heard by machine workers with ear plugs.<br><br>In HUMSEC, a concern can be a process failure of a guard who maintains the same schedule and routine or a cultural climate within a company that allows employees to use public meeting rooms for internal business.<br><br>In COMSEC data security, a concern can be the use of locally generated web server certificates for HTTPS or log files which record only the transaction participants and not the correct date and time of the transaction.<br><br>In COMSEC telecommunications, a concern can be the use of a FAX machine for sending private information or a voice mail system that uses touch tones for entering a PIN or password.<br><br>In SPECSEC, a concern can be a wireless access point using weak data encryption or an infrared door opener that cannot read the sender in the rain. |

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

| Category | | | Description |
|---|---|---|---|
| | | | |
| 4 | | ***Exposure*** | Count each unjustifiable action, flaw, or error that provides direct or indirect visibility of targets or assets within the chosen scope channel.<br><br>In PHYSSEC, an exposure can be a window which allows one to view assets and processes or a power meter that shows how much energy a building uses and its fluctuation over time.<br><br>In HUMSEC, an exposure can be a guard who allows all visitors to view the list of names on the sign-in sheet or a company operator who informs callers that a particular person is out sick or on vacation.<br><br>In COMSEC data security, an exposure can be a descriptive and valid banner about a service (disinformation banners are not exposures) or an ICMP echo reply from a host.<br><br>In COMSEC telecommunications, an exposure can be an automated company directory sorted alphabetically, allowing anyone to cycle through all persons and numbers, or a FAX machine that stores the last dialed numbers.<br><br>In SPECSEC, an exposure can be a signal that disrupts other machinery or an infrared device whose operation is visible by standard video cameras with night capability. |
| 5 | | ***Anomaly*** | Count each unidentifiable or unknown element which cannot be accounted for in normal operations, generally when the source or destination of the element cannot be understood. An anomaly may be an early sign of a security problem. Since unknowns are elements which cannot be controlled, a proper audit requires noting any and all anomalies.<br><br>In PHYSSEC, an anomaly can be dead birds discovered on the roof a building around communications equipment.<br><br>In HUMSEC, an anomaly can be questions a guard asks which may seem irrelevant to either the job or standard small talk.<br><br>In COMSEC data security, an anomaly can be correct responses to a probe from a different IP address than was probed or expected.<br><br>In COMSEC telecommunications, an anomaly can be a modem response from a number that has no modem.<br><br>In SPECSEC, an anomaly can be a local signal that cannot be properly located nor does it do any known harm. |

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 4.4 The Operational Security Formula

The rav is derived from three categories defined within the scope: Operational Security, Controls and Limitations. In order to begin, we must first aggregate and associate all of our input information into the appropriate categories for each input variable.

The rav equation requires that each of the categories be assigned a logarithmic base value to scale the three factors of Actual Security in accordance with the scope.

| Category | | OPSEC | Limitations |
|---|---|---|---|
| Operations | | Visibility | Exposure |
| | | Access | Vulnerability |
| | | Trust | |
| Controls | Class A - Interactive | Authentication | Weakness |
| | | Indemnification | |
| | | Resilience | |
| | | Subjugation | |
| | | Continuity | |
| | Class B - Prozess | Non-Repudiation | Concern |
| | | Confidentiality | |
| | | Privacy | |
| | | Integrity | |
| | | Alarm | |
| | | | Anomalies |

*The information contained within the rav is comprised of how operations balances with controls and limitations. There are no "weights" to skew the results leaving a flexible quantification of the attack surface that allows it to be compared to the security of anything else no matter size, vector, or Channel.*

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *Porosity*

Operational Security, also known as the scope's Porosity, is the first of the three factors of Actual Security that should be determined. It is initially measured as the sum of the scope's visibility ( $P_V$ ), access ( $P_A$ ),and trust ( $P_T$ ).

$$OpSec_{sum} = P_V + P_A + P_T$$

When calculating the rav it is however necessary to determine the Operational Security base value, $OpSec_{base}$ . The Operational Security base value is given by the equation

$$OpSec_{base} = \log^2\left(1 + 100 \times OpSec_{sum}\right).$$

Since the logarithm of 0 is not defined in the calculation we needed to include the 1+100 here. The log of 1 is 0. So if we have 0 Porosity and want to express this lack of interaction as perfect security of 100 rav then we needed to add +1 to the equation. Without the 1+100 we would have undefined numbers in the case that the sums of any of those factors are 0. This is required by the methodology because the absence of interactions represents perfect security and therefore the logarithm should equal 0 to provide the 100 rav.

## 4.5 The Controls Formula

The next step in calculating the rav is to define the Loss Controls; the security mechanisms put in place to protect the operations. First the sum of the Loss Controls, $LC_{sum}$ , must be determined by adding together the 10 Loss Control categories.

| Controls | **Class A** | | |
|---|---|---|---|
| | | Authentication | $LC_{Au}$ |
| | | Indemnification | $LC_{Id}$ |
| | | Resilience | $LC_{\mathrm{Re}}$ |
| | | Subjugation | $LC_{Su}$ |
| | | Continuity | $LC_{Ct}$ |
| | **Class B** | | |
| | | Non-Repudiation | $LC_{NR}$ |
| | | Confidentiality | $LC_{Cf}$ |
| | | Privacy | $LC_{\mathrm{Pr}}$ |
| | | Integrity | $LC_{It}$ |
| | | Alarm | $LC_{Al}$ |

Thus the Loss Control sum $LC_{sum}$ is given as

$$LC_{sum} = LC_{Au} + LC_{Id} + LC_{\mathrm{Re}} + LC_{Su} + LC_{Ct} + LC_{NR} + LC_{Cf} + LC_{\mathrm{Pr}} + LC_{It} + LC_{Al}.$$


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *Missing Controls*

Given that the combination of each of the 10 Loss Controls balance the value of 1 OpSec loss (visibility, access, trust) it is necessary to determine the amount of Missing Controls, $MC_{sum}$, in order to assess the value of the Security Limitations. This must be done individually for each of the 10 Loss Control categories. For example, to determine the Missing Controls for Authentication ($MC_{Au}$) we must subtract the sum of Authentication Controls ($LC_{Au}$) of the scope from the $OpSec_{sum}$. The Missing Controls can never be less than zero however.

The equation for determining the Missing Controls for Authentication ($MC_{Au}$) is given by

$$\text{IF } OpSec_{sum} - LC_{Au} \leq 0$$
$$\text{THEN } MC_{Au} = 0$$
$$\text{ELSE } MC_{Au} = OpSec_{sum} - LC_{Au}.$$

The resulting Missing Control totals for each of the 10 Loss Controls must then be added to arrive at the total Missing Control value ($MC_{sum}$) as seen below.

$$MC_{sum} = MC_{Au} + MC_{Id} + MC_{\mathrm{Re}} + MC_{Su} + MC_{Ct} + MC_{NR} + MC_{It} + MC_{\mathrm{Pr}} + MC_{Cf} + MC_{Al}$$

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### True Controls

True Controls ($TC_{sum}$) is the inverse of Missing Controls which means the True Controls for each individual control also need to be calculated before the results can be tallied into $TC_{sum}$.

The equation for determining the True Controls for Authentication ($TC_{Au}$) is given by

$$TC_{Au} = OpSec_{sum} - MC_{Au}$$

The resulting True Control totals for each of the 10 Loss Controls must then be added to arrive at the total True Control value ($TC_{sum}$) as seen below.

$$TC_{sum} = TC_{Au} + TC_{Id} + TC_{\mathrm{Re}} + TC_{Su} + TC_{Ct} + TC_{NR} + TC_{It} + TC_{\mathrm{Pr}} + TC_{Cf} + TC_{Al}$$

True Controls are used to measure the ideal placement of controls. The base value also helps to eliminate the influence of a disproportionate placement of controls on security. The True Controls base ($TC_{base}$) value is given as:

$$TC_{base} = \log^2\left(1 + 100 \times (OpSec_{sum} - MC_{sum} \times 0.1)\right).$$

Based on the same idea as True Controls, True Coverage (TCvg) can be used to measure the percentage of controls in place regarding the optimal amount and placement of controls. True Coverage is then derived using the Missing Control totals and the following equation:

$$\text{IF } OpSec_{sum} \leq 0$$
$$\text{THEN } TCvg = 0$$
$$\text{ELSE } TCvg = 1 - \frac{MC_{sum}}{10 \times OpSec_{sum}}.$$

### Full Controls

Full Controls, on the other hand, take into account all controls in place regardless of a balanced distribution. This value is important for measuring the worth of two-factor authentication, for example, and other instances of defense in depth for the same visibility, access or trust. The Full Controls base ($FC_{base}$) value is given as:

$$FC_{base} = \log^2\left(1 + 10 \times LC_{sum}\right)$$


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 4.6 The Limitations Formula

Next, the Limitations are individually weighted. The weighting of the Vulnerabilities, Weaknesses and Concerns are based on a relationship between the Porosity or $OpSec_{sum}$, the Loss Controls and in the case of Exposures and Anomaly the existence of other Limitations also plays a role. An Exposure or Anomaly poses no problems alone unless a Vulnerability, Weakness or Concern is also present. Think of an Exposure like a pointer. If there is a pointer that goes nowhere, or in this case doesn't lead to anything exploitable (Vulnerability, Weakness, Concern) and all Controls are accounted for, then at the time of the test the Exposure has no effect on security and thus has no value in the rav.

The following value table is used to calculate the $SecLim_{sum}$ variable, as an intermediate step between the Security Limitation inputs and the $SecLim_{base}$ variable, which is the Security Limitations basic input for the rav equation.

$$\text{IF } OpSec_{sum} \leq 0$$
$$\text{THEN } MCvg = 0$$
$$\text{ELSE } MCvg = \frac{MC_{sum} \times 0.1}{OpSec_{sum}}$$

| Input | Weighted Value | Variables |
|---|---|---|
| **Vulnerability** $L_V$ | $\frac{(OpSec_{sum} + MC_{sum})}{OpSec_{sum}}$ | $MC_{sum}$ : sum of Missing Controls |
| **Weakness** $L_W$ | $\frac{(OpSec_{sum} + MC_A)}{OpSec_{sum}}$ | $MC_A$ : sum of Missing Controls in Control Class A |
| **Concern** $L_C$ | $\frac{(OpSec_{sum} + MC_B)}{OpSec_{sum}}$ | $MC_B$ : sum of Missing Controls in Control Class B |
| **Exposure** $L_E$ | $\frac{((P_V + P_A) \times MCvg + L_V + L_W + L_C)}{OpSec_{sum}}$ | $P_V$ : sum of Visibility<br>$P_A$ : sum of Accesses<br>$MCvg$ : Percent Missing Coverage |
| **Anomaly** $L_A$ | $\frac{(P_T \times MCvg + L_V + L_W + L_C)}{OpSec_{sum}}$ | $P_T$ : sum of Visibility<br>$MCvg$ : Percent Missing Coverage |

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *Security Limitations Base*

$SecLim_{sum}$ is then calculated as the aggregated total of each input multiplied by its corresponding weighted value as defined in the table above.

$$SecLim_{sum} = \left( L_V \times \frac{(OpSec_{sum} + MC_{sum})}{OpSec_{sum}} \right) + \left( L_W \times \frac{(OpSec_{sum} + MC_A)}{OpSec_{sum}} \right) + \left( L_C \times \frac{(OpSec_{sum} + MC_B)}{OpSec_{sum}} \right) + \left( L_E \times \frac{((P_V + P_A) \times MCvg + L_V + L_W + L_C)}{OpSec_{sum}} \right) + \left( L_A \times \frac{(P_T \times MCvg + L_V + L_W + L_C)}{OpSec_{sum}} \right)$$

The Security Limitations base equation is given as:

$$SecLim_{base} = \log^2(1 + 100 \times SecLim_{sum})$$

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 4.7 The Actual Security Formula

This is the final part for using all previous calculations in three different ways.

### *Actual Security Delta*

The Actual Security Delta is useful for comparing products and solutions by previously estimating the change (delta) the product or solution would make in the scope. We can find the Actual Security Delta, $ActSec\Delta$, with the formula:

$$ActSec\Delta = FC_{base} - OpSec_{base} - SecLim_{base}.$$

### *True Protection*

Can be used as a simplified expression for the optimal coverage of a given scope where 100 signifies an optimal relationship between the Porosity, True Controls and Security Limitations. True Protection is given as:

$$\text{TruPro} = 100 + TC_{base} - OpSec_{base} - SecLim_{base}$$

### *Actual Security*

To measure the current state of operations with applied controls and discovered limitations, a final calculation is required to define Actual Security. As implied by its name this is the whole security value which combines the three values of operational security, controls, and limitations to show the actual state of security.

Actual Security (total), $ActSec$, is the true state of security provided as a hash of all three sections. A rav of 100 signifies a perfect balance of security however the Actual Security is not a true percentage value. Scores above 100 are also possible which signifies that the tested scope has more controls implemented than necessary which could also be proof of overspending. The final rav equation for Actual Security is given as:

$$ActSec = 100 + ActSec\Delta - \frac{1}{100} \times (OpSec_{base} \times FC_{base} - OpSec_{base} \times SecLim_{base} + FC_{base} \times SecLim_{base})$$

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

**Trusting everyone is insecure but not trusting anyone is inefficient.**

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

# Chapter 5 – Trust Analysis

> *"If you could take a pill that would make you more trusting, would you?" is how an informal ISECOM study began to help people better understand how they misuse trust as a concept. The general public answers no to this question. One security professional answered, "Yes but only if everyone else has to take it too."*

Trust can be both a problem and a solution. It is a problem where it puts security in a compromising position. Like the concept of potential energy in physics, trust creates a concentration of authorization which can explode into a big problem should the trust fail or the trusted target be deceived into harming the trust-giver. However it can also reduce the need for continuous, possibly redundant re-authentication, increasing the efficiency of operations. For that reason, trust is often seen as an "authenticate once and walk away" protocol. This is most often seen in Human Security where Human Resources departments research a candidate before the hire and afterward that person has continuous access to resources until they are no longer an employee. Re-authentication is then done seldom or sporadically and rarely at the same depth as when hired.

In operational security, Trust is merely a contributor to porosity, just another interaction to control. It differs from Access (the other form of interaction), in how it relates to other targets within the scope. So where Access is interaction between two sides of a vector into and out of the scope, Trust is measured as the interactions between targets within the scope. However, most people don't use trust so concretely. Trust is usually applied to a specific person or item and a specific act such as, "Can I trust this employee to deliver before the deadline?" or "Can I trust this computer?". There are correct answers for these questions but people often lack the skills needed to quantify the level of Trust for that person or object which would let us make a more rational and logical decision. However, to quantify trust, we need to first understand it.

## 5.1 Understanding Trust

Trust is a decision. While some people claim it is an emotion, like love, or a feeling, like pain, its clearly a complex quality we humans are born with. Unlike an emotion or a feeling, we can choose to trust or not to trust someone or something even if it feels wrong to do so. It appears that we are capable to rationalize in a way to supersede how we feel about trusting a target. This means we can quantify it by applying a logical process. It also means we can assign trust values to objects and processes as well as people based on these values. This brings new power to those who can analyze trust and make decisions based on that analysis. It also means Analysts with this skill can better control bias, identify fallacies (especially those from authoritative or trusted sources), and handle unknowns for transparent reporting. One point to note, however once the trust is quantified, it is only a vehicle for rationalizing the trust. It will not make something feel trustworthy now or in the future. Some people have strong feelings of aversion or attraction which may be at odds with the facts.

As part of OpSec, trust is one part of a target's porosity. Where security is like a wall that separates threats from assets, trust is a hole in that wall. It is wherever the target accepts interaction from other targets within the scope. However, people tend to use improper or incomplete operational controls with their trusts like authentication that has been made with improper identification such as a voice over a telephone, a business card, or even just the assumption that because a person is in the room that they are authorized to be there. This opens people up to fraud and deceit. The use of additional controls are required to secure a trust, to assure its integrity and resilience.

Unfortunately, while using more controls works with objects and processes, it may not work between people. Many times social norms consider controls beyond simple authentication like matching a face or

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

voice with an identity to be offensive to the person to be trusted. Society often requires us to be more trusting as individuals in order to benefit society as a whole and sometimes at the expense of everyone's individual protection.

As stated earlier, operational trust is measured as a negative thing which comes from an interaction between two entities in a scope. When a trust has no controls, it's what people call "blind trust" which may be good for relationships and can speed interactions but is bad for operational security. People generally apply controls to trusts even if they don't think of it as such at the time. Some controls are inherently given more weight than others depending on the situation and need. When selecting a person who they need to depend on, they may put a larger value on integrity and resilience. When making a financial transaction, they may put a larger value on authentication, continuity, and confidentiality. They may put a larger value on alarm and subjugation for advice on a product unless it's a medical prescription then they would prefer privacy and non-repudiation. Realistically though, they are not actually giving more value to particular controls. Instead they are actually evaluating on the ten trust properties and looking for those specific controls for comfort to their trust decisions. Using the trust properties allows them to make a decision to trust or not even when the information they have about the target is incomplete. Since uninformed and unpracticed trust decision making is a dangerous gamble the very least a formal process like applying the trust properties can provide is to inform the decision maker of exactly how much they don't know and allow them to seek more information before continuing. This means that the real need for being able to quantify operational trust occurs when we must rely on many unknowns to determine and rationalize trust.

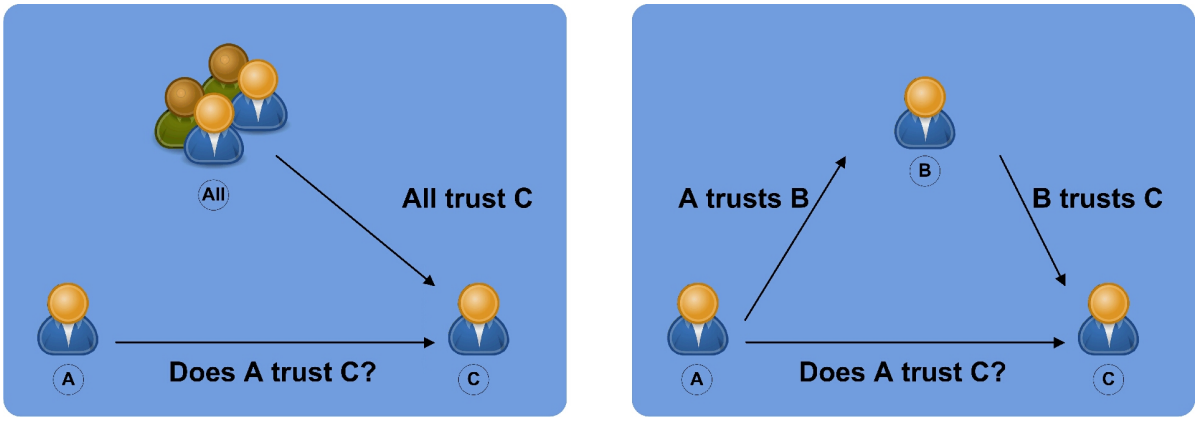
The trust properties are the quantifiable, objective elements which are used to create trust. We can say these properties are what we would say give us "reason to trust". These properties are to be made into baseline rules based on the target and situation which we are verifying. Unfortunately, many illogical trust properties exist and are all too commonly in use which makes it more difficult for us to make proper trust decisions without it *feeling* wrong. However, it's exactly the feeling part which makes us more error prone. During research, many potential trust properties were discovered which are commonly in use and even official, government and industry regulations recommend, however they failed logic tests and were discarded from our set of properties leaving only ten.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 5.2 Fallacies in Trust

Unfortunately, most people are bad at understanding and using trust. Many illogical methods for trust exist and are popularly used. Two examples of the most common, fallacious, trust properties are *composability* and *transitivity*. These properties are popularly used by people to make trust decisions about the unknown. In composability, a person makes a trust choice based on what a large number of people have to say about the thing or person in question even if those people aren't individually trusted. Basically, a person accepts the group's trusts as their own. This is similar to the pressure created by social or political groups and mass media. The reason why this is illogical is because the individual experiences of others, especially strangers, are all relative and cannot verify the consistent trustworthiness of future events.




*Common examples of fallacious trust use, first with Composability and secondly, with Transitivity.*

The other common fallacious use of trust is transitivity. It is when a person accepts the trust decision of a trusted person for themselves. It is also known as the chain of trust: you trust Alice and Alice trusts Jack therefore you can trust Jack. However, transitive trust is illogical as well because you may trust Alice for some things but perhaps not the same things for which she trusts Jack. There is also the possibility that Alice has approached the trust for some emotional benefit not available to you.

People who often trust "their gut" to make trust decisions are lauded when they are right as if they have some secret, powerful sense above other humans. However, other than just luck, some people are better at paying attention to details, seeing emotional micro-expressions in faces, and applying logic quickly to common situations which they themselves might not be able to express verbally as to how but rather they do *feel* what's wrong. These people learned to do this naturally and built upon it with experience filled with trial and error not really obvious to themselves any more than anyone notices the millions of small decisions they make each day and their consequences. The trust properties allow ordinary people who do not have this natural ability to analyze any of their trust decisions with skill, distancing themselves from their own under-developed "gut instinct" until they can recondition themselves to do so automatically, fluently, sharpening their instincts until they work "from the gut".

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 5.3 The Ten Trust Properties

The ten trust properties to make proper trust analysis are:

| Trust Property | | | Description |
|---|---|---|---|
| | | | |
| 1 |  | ***Size*** | The number to be trusted. Must the trust extend to just one or to many? Is the group to be a trusted one which is meant to make collective decision? |
| 2 |  | ***Symmetry*** | The vector (direction) of the trust. Trust may be one way (asymmetrical) and defined as to which way the trust must travel or both ways (symmetrical). A person who must also trust you has to consider the reciprocation from breaking the trust. |
| 3 |  | ***Visibility*** | The level of transparency of all operational parts and processes of the target and its environment. |
| 4 |  | ***Subjugation*** | Also called *control*, the amount of influence over the scope by the operator. |
| 5 |  | ***Consistency*** | The historical evidence of compromise or corruption of the target. |
| 6 |  | ***Integrity*** | The amount and timely notice of change within the target. |
| 7 |  | ***Offsets*** | The *offsets of sufficient assurance* are compensation for the trust giver or punishment for the trust breaker. It is a value placed on the trust with the target. |
| 8 |  | ***Value*** | The financial offset for risk, the amount of win or gain for which the risk of putting trust in the target is sufficient to offset the risk of failure in the trust. |
| 9 |  | ***Components*** | The number of other elements which currently provide resources for the target either through direct or indirect interactions, similar to Intervention of the Four Point Process. |
| 10 |  | ***Porosity*** | The amount of separation between the target and the external environment. |


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 5.4 The Trust Rules

Using the trust properties allows us to create only quantifiable rules, not "soft" rules that can neither substantiate the trust level nor disrupt it with a biased, emotional weight. However, the properties on their own are useless if they cannot become quantifiable properties, objective, or understandable by the common person not necessarily involved in the security field. Therefore we still need to turn the trust properties into trust rules, calculations of directly relevant operations made from all the trust properties. We do this in the form of questions where the answers are unbiased numbers which will be used to create a percentage for easier comprehension and which matches our common use of qualifiers of trust in normal speech like *almost*, *sometimes*, *always*, and *never*.

When creating the trust rules from the trust properties it is important to note that trust decisions are not linear. There is no building towards trust in a particular order or even an effort value system where it can be determined that one level requires more effort than another. In methodology terms, it appears irrational when calculated. A decision to trust therefore may be concluded by an answer from just one of the following tests which makes up the trust rules. However, doing so is our conscious choice to make a trust where the calculation specifically says not to. This may make most sense in a life or death situation where the result of trustworthiness is very low but the Value of Reward (one's life) is so incredibly great that no other choice can be made.

The trust rules must be created specifically for the target. While this may seem cumbersome, it is possible to make generically topic-specific trust rules which will suit the purpose. The benefit of this is that the trust properties can then be made into rules fitting any purpose and any situation where one must make a trust decision on another person, thing, process, system, or action. With practice, these trust rules can be made automatically and very quickly as part of one's decision process, focusing only on the rules which can be answered and discovering the ones where there can be no known answer with the information available.

The application of the trust rules into specific verification tests that provide a quantity is good however ideally you need to determine a finite quantity. An infinite quantity may be too relative to the tester and does not provide the constraints necessary for expressing the result in a percentage. For example, to apply the third property, transparency, the components should be counted as indexed so that there is a finite amount. So the parts of a computer can have an end number before the computer is completely built and a process can have a precise, finite number of steps before it is completed. For people, however, this may not be so easy to do but it is possible if applied properly to the situation. In the case of a security clearance, you may count all relationships within a given time range and of those, the number which are with people who have criminal records. This allows for a finite number even if rather large. Then, you may want to complete other tests specific to the third rule as that one may only give one type of influence. Others may be financial necessities, work experiences, memberships, convictions, and anything that will give a good representation as to how transparent that person is. The final calculation however has to be the sum total of all tests which will provide a single transparency percentage for that rule.

The resulting percentage for each trust rule can be viewed individually to show where controls must be applied to improve or maintain necessary levels of trustworthiness. This may also show where improvements must be made before a trust can be considered. For example, a trust analysis for a costly and difficult military campaign may show that rule four, subjugation, is at 10% because some of the necessary participants are civilians and not under military control. This gives the theater operators of the campaign specific, actionable information to make the necessary adjustments to get that percentage up to a level that's acceptable or else apply more controls to better assure compliance from those civilian members.

Another result from analyzing the percentages of individual trust rules is that unknowns become glaringly

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

obvious because the less that is known, the lower the percentage will be. This means unknowns will be at or very close to 0%.

The end metric however is one which is the mean of all percentages. This provides a big picture understanding you could rationally have of the target of the trust. This is especially useful when it is difficult to make a trust decision because of personal bias. Use of trust rules in formal security analysis as well as regular decision making can greatly minimize bias and mistakes. Therefore, the Analyst should be practiced in this skill so as to be able to apply them quickly so that it can be used even in high-pressure or emergency situations where a snap decision is necessary and a wrong decision is tragedy.

### *Example Trust Rules*

This is a sample of generic trust rules anyone can employee to make better hiring decisions beyond that of just the technical qualification of the applicant. It follows the 10 trust properties. The goal is to make quantifiable questions which can be answered for each of the properties and applied by any person and on any potential new hire. Solid trust rules allows for consistency in quality rather than relying on the "gut instinct" of the gate keepers who need to make the trust decisions.

1. ***Size***:
   1.1. Calculate the applicant divided by the total group of applicants.

   1.2. Calculate the number of people the applicant appears to know in the group divided by total applicants from the total group.

   1.3. Calculate the number of current employees the applicant knows (and is "friends" with) in this location and divide it by the total number of employees in this location.

   1.4. Record the average of these results.

2. ***Symmetry***:
   2.1. The number of people the applicant must rely on to do their job in this position (including the applicant) divided by the number of professionals who must rely on the applicant in this position.

3. ***Visibility***:
   3.1. The number of hours per day the applicant will be working alone, unassisted, unmonitored divided by the number of working hours.

4. ***Subjugation***:
   4.1. The number of decisions the employee will be making daily, independently, without input, divided by the total number of decisions the position normally requires in a day.

   4.2. The applicant divided by the number of team members the applicant will be working with daily.

   4.3. Record the average of these results.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

5. ***Consistency***:
   5.1. The total number of months which the applicant has not been employed divided by the total number of months the applicant has been on the workforce and eligible for employment.

   5.2. The total number of criminal offenses known divided by the current age less eighteen years (or the legal age of an adult in your region) of the applicant.

   5.3. The number of neutral or negative references from past employers divided by the total number of past employers.

   5.4. Record the average of these results.

6. ***Integrity***:
   6.1. The number of deliverables the applicant must produce or show for on a weekly basis divided by the work week.

7. ***Offsets***:
   *7.1. Amount of assets by value the applicant will have access to divided by a standardized cost of prosecution and cost of recovery.*

8. ***Value***:
   8.1. The monthly income created or saved by the applicant in the position divided by the monthly cost of the applicant. *(We don't measure the amount paid by the position compared to the national average because no clear correlation exists between pay grade and job satisfaction preventing an employee from leaving, stealing, or sabotaging the workplace.)*

9. ***Components***:
   9.1. The number of processes which require the applicant divided by the total number of processes for the position.

   9.2. The number of resources the employee will use monthly divided by the total number of resources available for all employees in that position.

   9.3. Record the average of these results.

10. ***Porosity***:
    10.1. The amount of time weekly the applicant would spend interacting directly with competitors, partners, or clients divided by the total number of weekly work hours.

    10.2. The number of employees living in the same community as the applicant divided by the total number people in the community.

    10.3. Record the average of these results.

*Each example of a calculation is to make a percentage which will be averaged with the other percentages of all trust properties to create a final trust value. The final value will tell you how much you should trust the new employee. Re-evaluations can then be made regularly to see how much has changed and if this should influence any permissions provided to the employee, pay rate, or other bonuses.*

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 5.5 Applying Trust Rules to Security Testing

Security tests will verify which operational trusts exist however the use of trust rules are required to know if they should exist. This is determined with the use of the Trust Rules during security testing.

Security management and policy creation is generally based on risk which defines the permissible interactions within and throughout an organization. This method essentially defines rules for users and configurations for systems which will provide the required level of protection when followed. The policy may also dictate how to handle problems which can occur should the rules or configurations be insufficient or not properly followed. Therefore the security policy will outline what the organization determines as trustworthy or not and which operational trusts will be allowed. However to test operational trust as established by the security policy is not security testing and it will not help an organization better determine where its protection is limited.

Security testing against a particular policy to assure the rules are followed is called compliance testing and it is not the same as security testing. The use of the OSSTMM audit will determine the existing operational trusts whether or not they are acknowledged within the security policy. These findings subjected to trust analysis where the Trust Rules have been applied on people, systems, and processes will provide a precise measurement of where controls need to be. This can then be compared to the security policy to find the deficiencies that impact current protection measures as well as future security plans. Ultimately the Analyst would use trust metrics in place of risk analysis for a more accurate means of protecting a scope.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

**There are only 2 ways to steal something: either you take it yourself or you have someone else take it and give it to you.**

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

# Chapter 6 – Work Flow

The OSSTMM flow begins with a review of the target's posture. The posture is the culture, rules, norms, contracts, 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 step is the review of the records of the audit trail. For the Analyst, this is simply: you know what you need to do, you do it, and then you check what you have done.

This methodology separates what needs to be done into this hierarchical format:

1. CHANNEL
2. MODULE
3. TASK

The work 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 Data Networks channel and the Wireless channel. This is why a properly defined testing plan is so important. Channel hybridization is a constant and should not be overlooked. The OSSTMM is fully capable of a "sidewalk to kernel" security review and therefore is completely capable of applying an analysis to a target whether its channels are clearly distinct and separate or comprised of multiple channels. Therefore, for all targets, the Analyst 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 Analyst will miss targets only available under other channels.

This methodology applies to all five channels. It has 17 modules and all the same properties apply to all five 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 any of five things:

1. The channel was obstructed in some way during the performance 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.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

A previous trust analysis may be incorporated to determine scope according to vector and channel. A trust analysis can also be used to predetermine which modules need to be performed as independent tests. However, remember that modules are parts of a whole test and the assumption that any particular module can just be omitted is false and will lead to an improper test. If there is no input for a particular module though, 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 a trust decision 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 plan. For example, if the Analyst 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 the 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. 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 Analyst, the target, the test environment, and the test plan.

## 6.1 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 Analyst 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. 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 does not represent a failure of the Analyst 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 Analyst 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.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *The Memory of Operations*

*This is an example of how PHYSSEC operational tests in a stochastic environment over a linear time frame are affected by their own memory.*

**Scenario 1**
The Analyst tests entry into a secured area with false authentication. The guard examines the badge briefly and allows the Analyst to enter. The Analyst performs the audit to the point where the Analyst is identified and the nature of the audit is revealed, if at all.

**Scenario 2**
The Analyst tests entry into a secured area with false authentication. The guard examines the badge briefly and doubting its authenticity, does not allow the Analyst to enter. The Analyst tries additional tactics until entry is gained. The Analyst performs the audit to the point where the Analyst is identified and the nature of the audit is revealed, if at all.

In both scenarios 1 and 2, there may or may not be a record of the entry attempt. If there is a record, that record can be re-used either by the Analyst the next time if the badge is denied as proof of its authenticity or by the guard who may be doubting its authenticity and wants to see what other guards have done.

For the next audit, the Analyst may try the same badge again, attempt other means to gain entry through social engineering techniques, or try using a different badge. That guard, other guards that the guard may have spoken with, and any log records of either the successful or failed attempt are all memories of the Analyst, the technique, and should the guard know of the audit, the audit itself.

However, should scenario 2 occur, it is possible that the interaction escalating through the additional techniques used by the Analyst means that scenario 2 is a more thorough test as more tests are made within the same interaction. It also means that the audit and the Analyst will more likely be remembered by the guard.

If the Analyst does not gain entry at all, then the completeness of the test is limited as to when the Analyst ran out of techniques, with each failed technique making entry that much more difficult. If the Analyst goes through all techniques outlined by tasks in the methodology, then the tests have been completed. If not, then the tests not yet conducted need to be tried on a different guard with different results as different people behave differently.

While this may seem to be a human problem, it is not. A door or window forced open too often will remain damaged until it is replaced. Physical use always results in physical deterioration. Even in wired communications, the act of snooping traffic will cause delays (sometimes noticeable) or change power consumption, both with either direct or indirect and often varied results.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 6.2 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 Analyst may want to schedule the details of the audit by phase.

There are four phases in the execution of this methodology:

A. Induction Phase
B. Interaction Phase
C. Inquest Phase
D. Intervention Phase

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

### *A. Induction Phase*

Every trip begins with a direction. In the induction phase, the Analyst 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.

| Module | | Description | Explanation |
|---|---|---|---|
| | | | |
| 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. |

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *B. Interaction 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.

| Module | | Description | Explanation |
|---|---|---|---|
| | | | |
| B.4 | **Visibility Audit** | The determination of the 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. |
| 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 between targets in the scope. | 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 | **Control 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. |


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### C. *Inquest Phase*

Much of security auditing is about the information that the Analyst uncovers. In this phase, the various types of value or the detriment from misplaced and mismanaged information as an asset are brought to light.

| Module | | Description | Explanation |
|---|---|---|---|
| | | | |
| C.8 | **Process Verification** | The determination of the existence and effectiveness of the record and maintenance of existing actual security levels 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** | 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 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. |
| 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. |

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *D. Intervention Phase*

These tests are focused on the resources the targets require in the scope. Those resources can be switched, changed, overloaded, or starved to cause penetration or 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 out. The final module, D.17, of Alert and Log Review, is required to verify prior tests which provided no interactivity back to the Analyst. Most security tests that do not include this phase may still need to run an end review from the perspective of the targets and assets to clarify any anomalies.

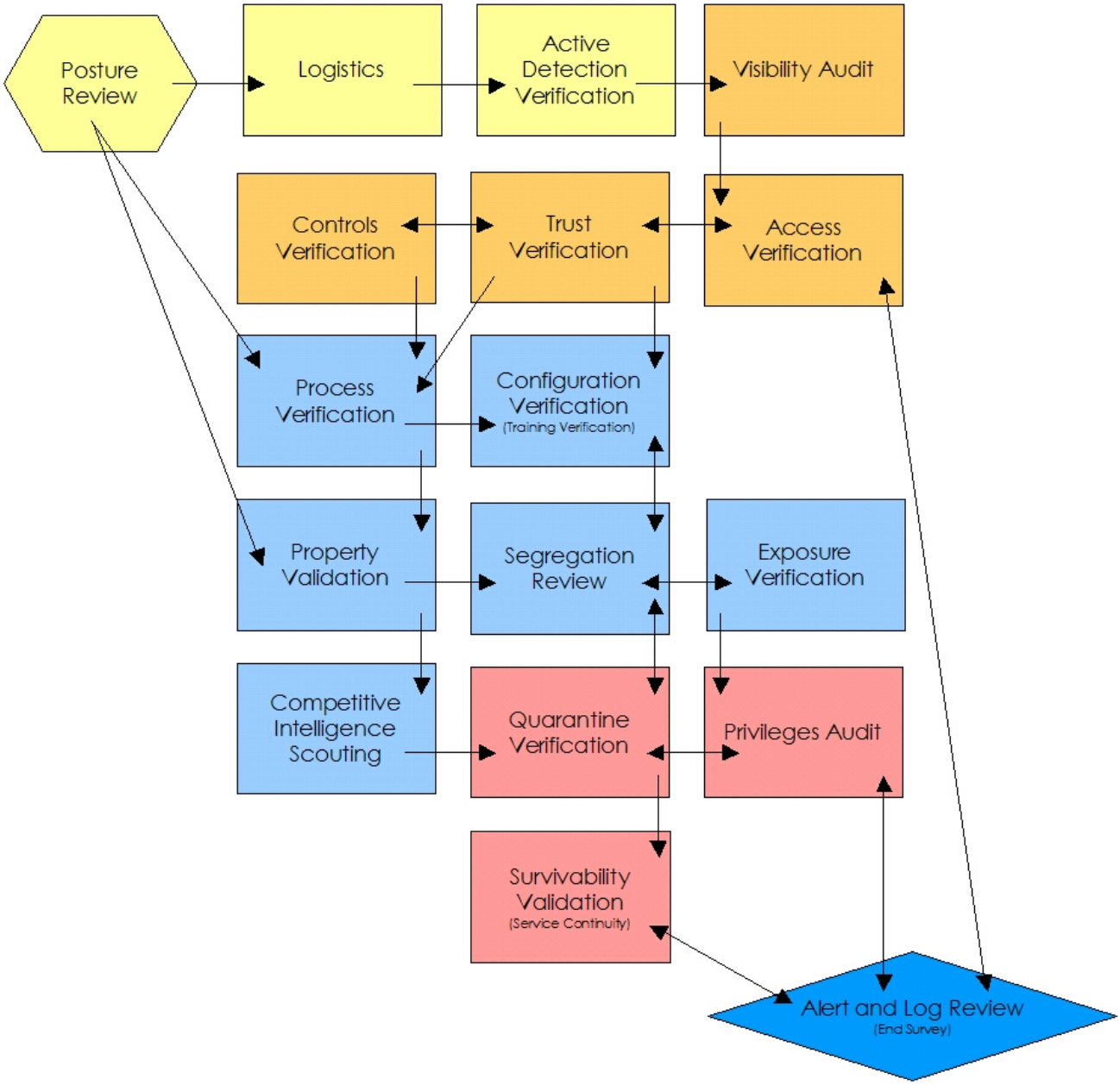
| Module | | Description | Explanation |
|---|---|---|---|
| | | | |
| D.14 | **Quarantine Verification** | The determination and measurement of effective use of quarantine for all access to and within the target. | Determine the effectiveness of authentication and subjugation controls in terms of black 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. | Determine the effectiveness of authorization on authentication, indemnification, and subjugation controls in terms of depth and roles. |
| D.16 | **Survivability Validation / Service Continuity** | The determination and measurement of the resilience of the target to excessive or adverse changes where continuity and resilience controls would be impacted. | Determine the effectiveness of continuity and resilience controls through the verification of denial of service and denial of interactivity. |
| D.17 | **Alert and Log Review / End Survey** | 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. |

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 6.3 One Methodology

Putting all the modules together provides one methodology to know and work with. This is one methodology which is applicable to any and all types of security tests. Whether the target be a particular system, a location, a person, a process, or thousands of them, this one methodology will assure the most thorough and efficient test possible.




Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

**In roulette you need to bet on the person spinning the wheel and throwing the ball. Like any other human they get bored and fall into a routine. Exploit the person whose predictability has inevitably better odds than the machine.**

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

# Chapter 7 - Human Security Testing

Human Security (HUMSEC) is a subsection of PHYSSEC and includes Psychological Operations (PSYOPS). Testing this channel requires interaction with people in gatekeeper positions of assets.

This channel covers the involvement of people, primarily the operating personnel within the target scope or framework. While some services consider this simply as "social engineering", the true compliance objective of security testing in this channel is personnel security awareness testing and gap measurement to the required security standard outlined in company policy, industry regulations, or regional legislation.

The Analyst will be required to have multiple tools and methods for the completion of some tasks to assure that suspicion is not raised among personnel and tests are not made invalid due to an early discovery or heightened paranoia. It may also be pertinent to limit test subjects to one per department or other boundary.

Competent Analysts will require both diligent people 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. In personam: Scope restrictions target those personnel who are under direct legal contract with the scope owner and, therefore, have legal responsibility for their security awareness and obligations.

2. Plausible deniability: No direct personnel security testing will take place for personnel who have not been trained, informed, or can be said to possess security awareness experience or obligations due to job responsibility requirements.

3. Human rights: Where personnel to be tested are randomly chosen or are not said to have job responsibilities directly related to gate keeping, security, or safety, the Analyst will refrain from personally identifying the person and report solely on a statistical basis.

4. Incommunicado: Personnel given time will discuss the actions of the test with others and alter the course of the testing.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *7.1 Posture Review*

Initial studies of the posture includes the laws, ethics, policies, industry regulations, and political culture which influence the security and privacy requirements for the scope. This review forms a matrix to which testing should be mapped but not constrained.

### 7.1.1 Policy

Review and document appropriate organizational policy regarding security, integrity, and privacy responsibilities of personnel in the scope.

### 7.1.2 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.

### 7.1.3 Culture

Review and document appropriate organizational culture in the scope towards security and privacy awareness, required and available personnel training, organizational hierarchy, and recognized trust interaction between employees.

### 7.1.4 Relationships

Review and document the appropriate influential relationships between personnel from the organizational hierarchy from within the scope.

### 7.1.5 Regional Culture

Review and document the appropriate influence of regional and foreign cultures on social hierarchy in the environment in which the scope resides.

### 7.1.6 Economics

Review and document the appropriate influence of economics and pay scale on social status of personnel from both the vector of personnel within the scope and that of the outside community on which the scope resides.


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 7.2 *Logistics*

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

### 7.2.1 Communications Equipment

Test for communications that provide identification to the receiver such as caller ID, FAX back, IP address logging, locator badges, and e-mail gateway headers. Test whether the identification be blocked, removed, or obfuscated, and to what degree of anonymity.

### 7.2.2 Communications

Test which languages are used within the scope and which languages are communicated between the scope and the customers, partners, and resellers outside the scope.

### 7.2.3 Time

Test for the timezone, holidays, and work schedules for various roles and jobs within the scope including partners, resellers, and influential customers interacting with the scope.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 7.3 *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 creating false positives and negatives in the test result data as well as changing the alarm status of monitoring personnel or agents.

### 7.3.1 Channel Monitoring

Test whether help desk or support channels over telephone, instant messaging, chat, web-based forums, or e-mail, are monitored by a third party for quality control.

### 7.3.2 Channel Moderating

Test whether help desk or support channels over telephone, instant messaging, chat, web-based forums, or e-mail, are filtered or quarantined by personnel or automated system to verify for authenticity, strip extraneous data, ignore repeated requests, or moderate interactions.

### 7.3.3 Supervision

Test whether support personnel may answer requests without confirmation from a supervisor or similar personnel.

### 7.3.4 Operator Assistance

Test what access to which personnel via the telecommunications channel must be made through an operator, whether manned by personnel or automated.


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 7.4 Visibility Audit

Enumeration and verification tests for the visibility of personnel with which interaction is possible via all channels.

### 7.4.1 Access Identification

Test for channels which provide interactions with personnel from outside the scope and document all methods used and the results of those methods.

### 7.4.2 Personnel Enumeration

Enumerate the number of personnel within the scope with both authorized and unauthorized access to processes within the scope, regardless of time or access channel, and the method for obtaining that data.

## 7.5 Access Verification

Tests for the enumeration of access points to personnel within the scope. While access to personnel outside of the scope is a real scenario and one often used for information property theft, this may be limited to scope-only interaction to protect the independent privacy rights of the personnel in their private life.

### 7.5.1 Access Process

Map and explore the use of channels into the scope to reach assets. Document all methods used and the results of those methods.

### 7.5.2 Authority

Use personnel in positions of authority with access-control or who hold gatekeeper positions to assets within the scope. Document methods used in discovery of key personnel.

### 7.5.3 Authentication

Enumerate and test for inadequacies from gateway personnel and what privileges are required to interact with them to assure that only identifiable, authorized, intended parties are provided access.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 7.6 *Trust Verification*

Tests for trusts between personnel within the scope where trust refers to access to information or physical assets from other targets within the scope.

### 7.6.1 Misrepresentation

Test and document the depth of requirements for access to assets within the scope with the use of misrepresentation as a member of the "internal" support or delivery personnel from within the scope without any credentials.

### 7.6.2 Fraud

Test and document the depth of requirements for access to assets within the scope with the use of fraudulent representation as a member of the management or other key personnel.

### 7.6.3 Misdirection

Test and document the depth of requirements for access to assets within the scope with the use of misrepresentation as a member of support or delivery personnel from outside the scope.

### 7.6.4 Phishing

Test and document the depth of requirements for access to personnel-controlled information or physical assets through all discovered channels to personnel within the scope with the use of a fraudulent gateway where personnel are asked to supply credentials. Document the methods and all credentials collected in this manner.

### 7.6.5 Resource Abuse

Test and document the depth of requirements to take assets outside of the scope to a known and trusted source or throughout the scope itself to other personnel without any established, required credentials.

### 7.6.6 In Terrorem

Test and document the depth of requirements to incite fear, revolt, violence, and chaos, through the disruption of personnel and the use of rumor or other psychological abuse.


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 7.7 Controls Verification

Tests to enumerate types of loss controls used to protect the value of assets.

### 7.7.1 Non-repudiation

Enumerate and test for use or inadequacies from gateway personnel to properly identify and log access or interactions to assets for specific evidence to challenge repudiation. Document the depth of the interaction which is recorded.

### 7.7.2 Confidentiality

Enumerate and test for use or inadequacies from all segments of communication with personnel within the scope over a channel or properties transported over a channel using secured lines, encryption, "quieted" or "closed" personal interactions to protect the confidentiality of the information assets known only to those with the proper security clearance classification of that asset.

### 7.7.3 Privacy

Enumerate and test for use of or inadequacies from all segments of communication with personnel within the scope over a channel or properties transported using specific, individual signatures, personal identification, "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, information, or physical assets.

### 7.7.4 Integrity

Enumerate and test for inadequacies in all segments of communication with personnel within the scope where assets are transported over a channel using a documented process, signatures, encryption, hash, or markings to protect and assure that the information or physical assets cannot be changed, switched, redirected, or reversed without it being known to parties involved.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *7.8 Process Verification*

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

### 7.8.1 Maintenance

Examine and document the timeliness, appropriateness, access to, and extent of processes for the notification and security awareness of all personnel in regards to operational security, actual security, and loss controls.

### 7.8.2 Misinformation

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

### 7.8.3 Due Diligence

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

### 7.8.4 Indemnification

Document and enumerate the abuse or circumvention of employee policy, insurance, non-disclosure, non-compete, liability contracts, or use/user disclaimers with all access personnel within the scope over all channels.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 7.9 *Training Verification*

Tests to examine the ability to circumvent or disrupt functional security awareness education and training in gateway personnel.

### 7.9.1 Education Mapping

Map types and frequency of security awareness assistance, education courses, and training provided to personnel, partners, customers, and specifically to gatekeepers.

### 7.9.2 Policy Disruption

Discover and examine the process and depth of self-policing from personnel for the disruption or non-conformity of security policy.

### 7.9.3 Awareness Mapping

Map the limitations discovered in security awareness training for personnel through gap analysis with actual procedures, including but not limited to: the provision of assets 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 one's self and assets, the handling of confidential and sensitive assets, and the conformity to organizational security policy.

### 7.9.4 Awareness Hijacking

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.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *7.10 Property Validation*

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

### 7.10.1 Sharing

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

### 7.10.2 Black Market

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.

### 7.10.3 Sales Channels

Verify public, out of scope businesses, auctions, or property sales which provide contact information through channels originating within the scope.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *7.11 Segregation Review*

Tests for appropriate separation of private or personal information assets 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.

### 7.11.1 Privacy Containment Mapping

Map gatekeepers of private information assets within the scope, what information is stored, how and where the information is stored, and over which channels the information is communicated.

### 7.11.2 Evident Information

Enumerate and map information regarding individual gateway personne. such as names, race, sex, religion, vacation days, personal web pages, published resumes, personal affiliations, directory inquiries, bank branch(es), electoral register, and any particular personal information stated implicitly as private in regulations and policy.

### 7.11.3 Disclosure

Examine and document types of disclosures of private information assets on personnel from gatekeepers responsible for this segregation according to policy and regulations as determined in the Posture Review and the basic human right to privacy.

### 7.11.4 Limitations

Examine and document types of gateways and channel alternatives with gateways accessible to people with physical limitations within that channel.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 7.12 Exposure Verification

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

### 7.12.1 Exposure Mapping

Enumerate and map personnel 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, log-ins, log-in schemes, passwords, back-up methods, insurers, or any particular organizational information stated implicitly as confidential in regulations and policy.

### 7.12.2 Profiling

Profile and verify the organization, employee skill requirement types, pay scales, channel and gateway information, technologies, and direction.

## 7.13 Competitive Intelligence Scouting

Tests for scavenging property 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.

### 7.13.1 Business Grinding

Map gatekeepers of business assets within the scope, what information is stored, how and where the information is stored, and over which channels the information is communicated between personnel.

### 7.13.2 Business Environment

Explore and document from individual gateway personnel business details such as alliances, partners, major customers, vendors, distributors, investors, business relations, production, development, product information, strategic planning, stocks and trading, and any particular business information or property stated implicitly as confidential in regulations and policy.

### 7.13.3 Organizational Environment

Examine and document types of disclosures of business assets 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 assets stated implicitly as confidential in regulations and policy.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 7.14 Quarantine Verification

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

### 7.14.1 Containment Process Identification

Identify and examine quarantine methods and process at the gateways in all channels for aggressive and hostile contacts such as sales people, head-hunters, grifters, journalists, competitors, job seekers, job candidates, and disruptive persons.

### 7.14.2 Containment Levels

Verify the state of containment, length of time, and all channels where interaction with gatekeepers has quarantine methods. Ensure that methods are within legal context and boundaries.

## 7.15 Privileges Audit

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

### 7.15.1 Identification

Examine and document the process for obtaining identification through both legitimate and fraudulent means on all channels.

### 7.15.2 Authorization

Verify the use of fraudulent authorization on all channels to gain privileges similar to that of other personnel.

### 7.15.3 Escalation

Verify and map access to assets through the use of privileges to gain higher or more extensive privileges beyond that which is authoritatively designated to the role.

### 7.15.4 Discrimination

Verify information requested and privileges granted from gatekeepers in cases where age (specifically those who are legally minors for the region), sex, race, custom/culture, and religion are factors which may be discriminated against in accordance to the Posture Review.

### 7.15.5 Subjugation

Enumerate and test for inadequacies of assets communicated over channels where those controls are not required, can be circumvented or ignored such as insecure e-mail or over a public telephone line.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 7.16 Service Continuity

Determining and measuring the resilience of the gatekeepers within the scope to excessive or hostile changes designed to cause service failure.

### 7.16.1 Resilience

Enumerate and test for inadequacies on all channels from personnel within the scope whereby removing or quieting gateway personnel will allow for direct access to assets.

### 7.16.2 Continuity

Enumerate and test for inadequacies from all personnel with regard to access delays and service response time through back-up personnel or automated means for access to alternate gateway personnel.

### 7.16.3 Safety

Map and document the process of gatekeepers disconnecting channels due to evacuation or safety concerns as a gap analysis with regulation and security policy.

## 7.17 End Survey

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.

### 7.17.1 Alarm

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 noted by personnel upon suspicion of circumvention attempts, social engineering, or fraudulent activity.

### 7.17.2 Storage and Retrieval

Document and verify the privileged and efficient access to alarm, log, and notification storage locations and property.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

**The most useless types of physical security controls are the kinds that don't protect against what you need them to and those which protect against anything for no reason.**

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

# Chapter 8 - Physical Security Testing

PHYSSEC (Physical Security) is a classification for the material security within the physical realm which is within the limits of human-interactive 3D space. Testing this channel requires non-communicative interaction with barriers and humans in gatekeeper positions of assets.

This channel covers the interaction of the Analyst within proximity of the targets. While some services consider this simply as "breaking and entering", the true compliance objective of security testing in this channel is physical and logical barrier testing and gap measurement to the required security standard as outlined in company policy, industry regulations, or regional legislation.

The Analyst will be required to have multiple tools and methods for the completion of some tasks to assure that suspicion is not raised among personnel and tests are not made invalid due to an early discovery or heightened paranoia. It may also be pertinent to limit test subjects to one per department or other boundary. Analysts will also need to be prepared for the possibility of accidental bodily harm from conventional barriers and weapons, interactions with animals, subjection to harmful bacteria, viruses, and fungi, exposure to electromagnetic and microwave radiation, especially that which can permanently damage hearing or sight, and poisonous or corrosive chemical agents in any form.

Competent Analysts will require physical strength, endurance, agility, and critical thinking skills to assure factual data collection creates factual results through correlation and analysis.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *Considerations*

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

1. Conatus: All attempts to traverse physical barriers require an unbiased judgment of the amount of difficulty required to reach and interact with the target and the danger involved. These considerations are to be made with regard to the "will to live" of humans as well as any effect on the targets should the attack be made without regard for life (suicidal).

2. Ecce hora: All physical tests require close attention be made to time. Records must be kept of the time the test is made, time on target, and time the test finishes, whether successful or not, because that will also assist in determining what can be accomplished within the time range to fail. Knowing such information can help understand what may be a deceptive attack so as to be sure resources are not wasted in one area while leaving another open.

3. Abuse of discretion: The Analyst must take care not to ignore or misinterpret the results from testing a physical barrier or obstacle because it is not within the range of the Analyst's physical possibilities. The Analyst should remain unbiased and not over-estimate or over-value personal skills and ability and instead apply the tests as a highly skilled and highly able person could.

4. Magister pecuarius: The Analyst should not dismiss the reasonable potential of an attacker using trained animals to circumvent barriers and obstacles where a human being cannot.

5. Plausible deniability: No direct or physical personnel security testing will take place for personnel who have not been trained, informed, or can be said to possess security awareness experience or obligations due to job responsibility requirements.

6. Sui generis: All interaction with physical barriers will leave record of this interactivity and, in more extreme cases, may weaken or destroy the barrier. The Analyst should take care in testing one-of-a-kind type targets which may not be replaceable. The Analyst should also take care not to leave permanent markings wherever possible and to keep record of all barriers tested to verify them for damage after the audit.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *8.1 Posture Review*

Initial studies of the posture includes the laws, ethics, policies, industry regulations, and political culture which influence the security and privacy requirements for the scope. This review forms a matrix to which testing should be mapped but not constrained.

### 8.1.1 Policy

Review and document appropriate organizational policy regarding security, safety, integrity (i.e. supply chain), and privacy requirements for barriers in the scope.

### 8.1.2 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.

### 8.1.3 Culture

Review and document appropriate organizational culture in the scope towards security and privacy awareness, required and available personnel training, organizational hierarchy, and recognized trust interaction between employees.

### 8.1.4 Relationships

Review and document the appropriate influential relationships between personnel from the organizational hierarchy from within the scope.

### 8.1.5 Regional Culture

Review and document the appropriate influence of regional and foreign cultures on safety, social hierarchy, the supply chain, and services in the environment in which the scope resides.

### 8.1.6 Economics

Review and document the appropriate influence of economics and pay scale on social status and criminal intent on personnel from both the vector of personnel within the scope and that of the outside community in which the scope resides.

### 8.1.7 Environment

Review for the target region the weather patterns, dangerous weather extremes (i.e. flooding, tornadoes, hurricanes), temperature extremes, humidity maximums, air quality, tectonic stability, typical fauna, forms of natural or man-made disaster and general insect infestation.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *8.2 Logistics*

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

### 8.2.1 Environment

(a) Examine the scope to determine if any special equipment is required for the environment of the targets. Equipment can range from rope to climb walls to SCUBA gear to travel under water. Equipment types are not limited to just the environment but also the barriers one must circumvent.
(b) Verify damaged safety equipment which may lead to Analyst injury.
(c) Examine the targets for hazardous, contaminated, or poorly maintained terrain, air, water, buildings, or structures.
(d) Examine noise, electromagnetic radiation, and magnetic field levels at the scope.

### 8.2.2 Communications

(a) Test which languages are used within the scope and which languages are communicated between the scope and the customers, partners, and resellers outside the scope.
(b) Examine the means of communication between personnel and whether it is enhanced through the use of tools such as flags, flares, radios, binoculars, night vision, etc.

### 8.2.3 Time

(a) Test for the timezone, holidays, and work schedules for various roles and jobs within the scope including partners, resellers, and influential customers interacting with the scope.
(b) Determine if decreased mobility or visibility during time of day, week, month, or season (day or night, fog, rain, or snow) will have an impact upon operations at the target.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 8.3 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 creating false positives and negatives in the test result data as well as changing the alarm status of monitoring personnel or agents.

### 8.3.1 Monitoring

(a) Verify that the scope is monitored by a third party for intrusion via look-outs, guards, cameras, or sensors. The date and time of entry as well as departure of the target should be recorded.
(b) Determine the range of the monitoring and whether the travel of a threat to the target can be intercepted in a timely manner.
(c) Verify if travel to the target requires increased time on target and exposure. This includes, but is not limited to: quarantine rooms, long empty hallways, parking lots, large empty expanses, difficult or unnatural terrain, and guest or holding areas.
(d) Verify that the lighting and visible contrast on approach to the target allows for interception of threats.

### 8.3.2 Reacting

(a) Verify if interactive controls for the target will react timely to extreme environmental conditions according to the Environment review task of the Posture Review.
(b) Verify if the target will react timely to a disturbance in air, water, and soil quality.
(c) Verify if the target will react timely to critical noise disturbances.
(d) Verify if the target will react timely to magnetic field disturbances.
(e) Verify if the target will react timely to fires.
(f) Verify if the target will react timely to denial of target access via blockade or quarantine.
(g) Verify if the target will react timely to threats of fear, revolt, or violence within the scope.
(h) Determine the finality of threat interception.

## 8.4 Visibility Audit

Enumeration and verification tests for the visibility of targets and assets. In PHYSSEC, assets must also include supplies such as food, water, fuel, etc. and operational processes which may affect those supplies like the proper removal of waste and other contaminants, loading and unloading supply shipments, sleep and rest cycles, proper acclimatization, etc.

### 8.4.1 Reconnaissance

(a) Map and detail the scope perimeter determined by visible and assisted viewing techniques, publicly accessible areas, public plans, and public sources.
(b) Enumerate and detail targets and assets visible from outside the scope.
(c) Enumerate and detail target traffic patterns, foot traffic, occupied areas, and sensors visible outside the scope.
(d) Enumerate directories and internal telephone books identifying locations of sensitive information processing facilities that are not readily accessible by the public.
(e) Map and enumerate the physical location and layout of the targets, the size and navigability of obstacles, barriers, and hazards which will increase time on target.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *8.5 Access Verification*

Tests for the enumeration of access points to interact with the targets and assets within the scope. While access to walls and fences bordering property outside of the scope is a real scenario and one often used in an attack, this audit is limited to scope-only interaction to protect the property rights of third parties.

### 8.5.1 Enumeration

(a) Map and explore the navigable of terrain, barriers, and obstacles into the scope to reach the targets and assets. Document all methods used and the results of those methods.
(b) Map and verify all access points that allow stealthy or unmonitored, direct (3 seconds or less time on target) interaction with the target.
(c) Verify the size and navigable of public and private access points and all paths to target.

### 8.5.2 Authentication

(a) Enumerate and test for inadequacies which privileges are required to access, the process of obtaining those privileges, and assure that only identifiable, authorized, intended parties are provided access.
(b) Verify the process of authenticating which items may be taken into the scope by both authorized and unauthorized personnel.
(c) Verify the process of authenticating which items may be taken out of the scope by both authorized and unauthorized personnel.
(d) Verify the process of recording access and which items were entered and removed.

### 8.5.3 Location

(a) Map the distance from the scope perimeter to the visible targets and assets from outside the scope.
(b) Map and identify all paths to access points which can be reached in a noisy, not stealthy, direct (3 seconds or less time on target) interaction with that access point. This may include attacks which are sans conatus (without regard for the attacker's life).

### 8.5.4 Penetration

(a) Determine which barriers and obstacles in the scope provide remote access to change, disrupt, destroy, or obtain assets (visually, aurally, and magnetically).
(b) Determine the effectiveness of barriers and obstacles to withstand conditions defined in the Posture Review.
(c) Determine and rate the effectiveness of barriers and obstacles to withstand fire, explosions, and general concussive forces such as gunshots and vehicular ramming.
(d) Determine and rate the effectiveness of barriers and obstacles to reduce incoming: critical noise levels, heat, cold, smoke, humidity, disruptive or caustic odors, intense magnetic fields, harmful light, and pollutants.
(e) Determine and rate the effectiveness of barriers and obstacles to reduce outgoing: sounds, smells, vibrations, conditions for acclimatization, smoke, magnetic fields, waste, and pollutants.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 8.6 *Trust Verification*

Tests for trusts between processes within the scope where trust refers to access to assets without the need for identification or authentication.

### 8.6.1 Misrepresentation

(a) Test and document the depth of requirements for access to assets with the use of misrepresentation as a member of the "internal" support or delivery personnel without proper credentials.
(b) Test and document the depth of requirements for access to assets with the use of misrepresentation as a disabled person.

### 8.6.2 Fraud

Test and document the depth of requirements for access to assets with the use of fraudulent representation of authority as a member of the management or other key personnel.

### 8.6.3 Misdirection

Test and document the depth of requirements for access to assets with the use of misrepresentation as a member of support or delivery personnel outside the scope.

### 8.6.4 Stowage

Test and document the depth of requirements for access to assets through stealthy stowage with a transport of support or delivery to take the stowage outside the scope.

### 8.6.5 Embezzlement

Test and document the depth of requirements to hide assets within the scope (whole or destroyed), take assets outside of the scope to a known and trusted source, and throughout the scope itself to other personnel without any established, required credentials.

### 8.6.6 In Terrorem

Test and document the depth of requirements to incite fear, revolt, violence, and chaos, through the disruption of processes and the contamination of supplies.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 8.7 Controls Verification

Tests to enumerate types of loss controls used to protect the value of assets.

### 8.7.1 Non-repudiation

Enumerate and test for use or inadequacies from monitors and sensors to properly identify and log access or interactions with assets for specific evidence to challenge repudiation. Document the depth of the interaction which is recorded.

### 8.7.2 Confidentiality

Enumerate and test for use or inadequacies from all signals, physical communication, and transported items between both internal and external-reaching processes and personnel using codes, undecipherable language, "quieted" or "closed" personal interactions to promote the confidentiality of the communication only to those with the proper security clearance classification for that communication.

### 8.7.3 Privacy

Enumerate and test for use of or inadequacies from all interactions within the scope using unmarked or non-obvious packaging or labeling, "quieted" or "closed room" interactions, and within randomly chosen quarters to hide or protect the privacy of the interaction and only to those with the proper security clearance for that process or asset.

### 8.7.4 Integrity

(a) Enumerate and test for inadequacies in all signals and communication between processes and personnel using a documented process, seals, signatures, hashing, or encrypted markings to protect and assure that the assets cannot be changed, redirected, or reversed without it being known to the parties involved.
(b) Enumerate and test for inadequacies in all processes and interactions with assets in transport which use a documented process, signatures, seals, break-away tape, brands, tags, sensors, or encrypted markings to protect and assure that the assets cannot be changed, redirected, or reversed without it being known to the parties involved.
(c) Verify all storage mediums for information are not in danger from unnatural decay such as heat or humidity damage, fading from direct sunlight, or magnetic degradation (bit rot).

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 8.8 Process Verification

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

### 8.8.1 Maintenance

(a) Examine and document the timeliness, appropriateness, access to, and extent of processes for equipment and barrier repair in regards to operational security, actual security, and loss controls.
(b) Verify the repair and determine the extent to which notice and quality of repairs can be misrepresented and falsified.

### 8.8.2 Indemnification

(a) Document and enumerate the ability to abuse or circumvent employee policy, insurance, non-disclosure, non-compete, liability contracts, or use/user disclaimers for personnel within the scope.
(b) Enumerate the use of signs warning of danger, surveillance or alarms in effect, health issues, and postings of no entrance.
(c) Verify the extent and finality of legal action used to uphold indemnification.

## 8.9 Configuration Verification

Tests to examine the operation of processes under various levels of security conditions. Understanding how processes work under daily routine and efficiencies provides insight to how they should behave under more extreme conditions.

### 8.9.1 Education Mapping

Map types and frequency of physical security and safety assistance, education courses, and training provided to personnel, partners, customers, and specifically to gatekeepers.

### 8.9.2 Policy Disruption

Discover and examine the process and depth of self-policing from personnel for the disruption or non-conformity of physical security and safety policy.

### 8.9.3 Threat Conditions

(a) Map the ready responses of security processes in reaction to increased threat condition levels (i.e. green, yellow, orange, and red alerts) as per requirements determined in the Posture Review.
(b) Determine which triggers are required to increase threat levels and verify that they are met.
(c) Map the ready responses of security processes in reaction to decreased threat condition levels as per requirements determined in the Posture Review.
(d) Discover and examine the extent to which a non-official person provides misinformation regarding threat levels in an authoritative manner to purposely raise or lower ready status.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *8.10 Property Validation*

Tests to examine physical property available within the scope or provided by personnel which may be illegal or unethical.

### 8.10.1 Sharing

Verify the extent to which personal assets or those of the organization have been faked, reproduced, or shared illegally and intentionally according to the requirements of the Posture Review through sharing, lending, renting, or leasing services, personal libraries, and personal caches or unintentionally through ignorance or negligence.

### 8.10.2 Black Market

Verify the extent to which personal assets or those of the organization have been faked or reproduced and are being promoted, marketed, or sold between personnel or by the organization.

### 8.10.3 Sales Channels

Verify assets in auctions, flea markets, want-ads, yard sales, swap meets, or property sales which provide contact information through channels originating within the scope.

### 8.10.4 Storage

(a) Verify storage locations and small caches of organizational assets are in the appropriate location within the scope.
(b) Verify storage locations and small caches of organizational assets for use or for sale publicly or to other members of the organization are not being deliberately hidden, hoarded, controlled, or saved.

### 8.10.5 Resource Abuse

(a) Enumerate personal items which consume power, fuel, food, water, or other assets within the requirements defined in the Posture Review.
(b) Enumerate personal items using channels which are the property of the organization (i.e. Internet servers, jukeboxes, fax machines, etc.).
(c) Enumerate openly viewable personal items which symbolize beliefs not within the requirements defined in the Posture Review.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *8.11 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, transport, and control of personnel, partner, and customer private information property.

### 8.11.1 Privacy Containment Mapping

Map storage locations of private information property within the scope, what information is stored, how and where the information is stored, and how and where the property is discarded.

### 8.11.2 Evident Information

Enumerate and map from the target documents and physical property with unsecured personal information as defined implicitly as private in regulations and policy of the Posture Review (i.e. full names, race, sex, religion, vacation days, personal web pages, published resumes, personal affiliations, directory inquiries, bank branch, electoral register, etc.).

### 8.11.3 Disclosure

Verify access to stores of private information property of personnel as determined in the Posture Review.

### 8.11.4 Limitations

Examine and document mobility alternatives accessible to people with physical limitations within that channel.

### 8.11.4 Offensive Materials

Verify openly viewable personal property does not flaunt or offend as determined offensive or private in the Posture Review.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *8.12 Exposure Verification*

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

### 8.12.1 Exposure Mapping

Discover and enumerate unsecured documents and items with building information regarding the organization such as blueprints, logistics, schedules, keys, access tokens, badges, uniforms, or any particular organizational assets which provide deeper or broader access.

### 8.12.2 Profiling

(a) Profile and verify the structural definition of the targets including material type, height, thickness, and security or safety properties.
(b) Discover and enumerate access control sensors, cameras, monitors, man-traps, cages, gates, fences, etc. for type, technology, maker, materials, and security or safety properties.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *8.13 Competitive Intelligence Scouting*

Tests for scavenging property 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.

### 8.13.1 Business Grinding

Discover and map storage locations of business property within the scope, what information is stored, how and where the information is stored, and how and where the property is discarded.

### 8.13.2 Business Environment

Discover and enumerate documents and items with business details such as personnel, pay rates, alliances, partners, major customers, vendors, distributors, investors, business relations, production, development, product information, planning, stocks and trading, and any particular business information or property determined implicitly as confidential or non-compete from the Posture Review.

### 8.13.3 Organizational Environment

Discover and enumerate documents and items with organizational details such as 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 or non-compete from the Posture Review.

### 8.13.4 Operational Environment

Discover and enumerate processes which expose operational details such as packaging, shipping, distribution, arrival and departure times of employees, management, customers, methods of interaction, advertising and marketing plans, product development, product capacity, and any particular operational property stated implicitly as confidential or non-compete from the Posture Review.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *8.14 Quarantine Verification*

Tests for verifying the proper fielding and containment of people and processes with aggressive or hostile intent within the scope.

### 8.14.1 Containment Process Identification

(a) Identify and examine physical quarantine methods and processes within the scope for aggressive and hostile contacts such as chaotic or violent people, unscheduled sales people, head-hunters, grifters, journalists, competitors, job seekers, job candidates, and disruptive people.
(b) Identify and examine physical quarantine methods and process within the scope for managing dangerous and harmful items or substances, illegal substances, and illegally removed company property.
(c) Identify and examine physical quarantine methods and processes within the scope for merely suspicious behavior or items and substances of suspect utility.

### 8.14.2 Containment Levels

(a) Verify the state of containment location, length of time, and process of the quarantine method. Ensure that methods are within legal context and boundaries as per the Posture Review.
(b) Verify proper procedures are followed for a full lock-down as per the requirements in the Posture Review for environmental threats, biological, chemical, or other contamination threats and in cases of workplace violence.
(c) Verify proper procedures for quarantine recovery and return to the proper secure state following a state of lock-down as per the requirements in the Posture Review.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *8.15 Privileges Audit*

Tests for gaining access credentials and privileges as supplied to other personnel with the appropriate permissions.

### 8.15.1 Identification

Examine and document the process for obtaining identification through legitimate, illegal (i.e. graft, theft, threats, etc.) and fraudulent (forgery, misrepresentation, etc.) means.

### 8.15.2 Authorization

Verify the use of fraudulent authorization to gain privileges similar to that of other personnel.

### 8.15.3 Escalation

Verify and enumerate accesses to assets through the use of privileges to gain higher privileges to that of gatekeepers.

### 8.15.4 Special Circumstances

Verify gaining access privileges as requested in cases where age (specifically those regarded legally as minors for the region), relationship (i.e. son, daughter, father, mother, etc.) sex, race, custom/culture and religion are factors which may be granted special circumstances or discriminated against in accordance to the Posture Review.

### 8.15.5 Subjugation

Enumerate and test for inadequacies in access to assets not controlled by the source providing the access (i.e. PINs, ID photos, etc. selected by the actor, sign-ins with identification numbers written in by the actor, etc.).

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *8.16 Survivability Validation*

Determining and measuring the resilience of the barriers and guards within the scope to excessive or hostile changes designed to cause operations failure.

### 8.16.1 Resilience

(a) Enumerate and verify that the distraction, removal or quieting of gateway personnel will not allow for direct access to assets or operations.
(b) Enumerate and verify that the disabling or destruction of operational security measures or controls will not allow for direct access to assets or operations.
(c) Verify that the isolation of the scope from resources such as fuel, power, food, water, communications, etc. does not allow for direct access to assets or operations.
(d) Verify that high alert threat conditions do not shut down or minimize operational security measures or controls allowing for direct access to assets or operations.

### 8.16.2 Continuity

(a) Enumerate and verify conditions where access delays are properly addressed through back-up personnel or an automated means for timely access to services, processes, and operations.
(b) Enumerate and verify that the distraction, removal or quieting of gateway personnel will not halt or deny timely access to services, processes, and operations.
(c) Enumerate and verify that the disabling or destruction of operational security measures or controls will not deny timely access to services, processes, and operations.
(d) Verify that the isolation of the scope from resources such as fuel, electrical power, food, water, communications, etc. will not halt or deny access to services, processes, and operations.
(e) Verify that the inability to remove waste, pollutants, or other contaminants from the scope will not halt or deny access to services, processes, and operations.
(f) Verify that high alert threat conditions do not halt or deny access to services, processes, and operations.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *8.17 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.

### 8.17.1 Alarm

Verify and enumerate the use of a localized or scope-wide warning system, log or message for each access gateway where a suspect situation is noted by personnel upon suspicion of circumvention attempts, fraudulent activity, trespass, or breach. Ensure that the sensors/systems are installed to national, regional or international standards and regularly tested to cover all accessible points.

### 8.17.2 Storage and Retrieval

Document and verify the permissions and efficient access to alarm, log, and notification storage locations and property. Access to areas where sensitive information is processed or stored should be controlled and restricted to authorized personnel only; an audit trail of all access should be securely maintained.


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

**The information to be found within the wireless spectrum is not limited to product specifications.**

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

# Chapter 9 - Wireless Security Testing

Spectrum security (SPECSEC) is the security classification which includes electronics security (ELSEC), signals security (SIGSEC), and emanations security (EMSEC). ELSEC are the measures to deny unauthorized access to information derived from the interception and analysis of non-communications electromagnetic radiations. SIGSEC are the measures to protect wireless communications from unauthorized access and jamming. EMSEC are the measures to prevent the machine emanations that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by information systems equipment. Testing this channel requires interaction with barriers to assets over Electromagnetic (EM) and Microwave (MW) frequencies.

This channel covers the interaction of the Analyst within proximity range of the targets. While some services consider this simply as "scanning", the true compliance objectives of security testing in this channel are physical and logical barrier testing and gap measurement to the required security standard outlined in company policy, industry regulations, or regional legislation.

The Analyst will be required to have adequate protection from electromagnetic power sources and other forms of radiation. Analysts will also need to be prepared for the possibility of accidental bodily harm from exposure to electromagnetic and microwave radiation, especially that which can permanently damage hearing or sight. Proper equipment should warn when within range of Electromagnetic and Microwave radiation from -12dB and greater. Specific frequencies may adversely affect implanted medical devices, cause vertigo, headaches, stomach cramps, diarrhea, and other discomforts on both an emotional and physical level.

Competent Analysts will require sufficient knowledge of EM and MW radiation 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: Analysts 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, Analysts have presumed knowledge of the law. Analysts are considered professionals in this subject matter and, therefore, the assumption exists that even regarding what may not be common knowledge for the average person about a foreign region's laws regarding EM and MW communication systems, will be known to the Analyst.

2. In personam: Testing must specifically target only SPECSEC from personnel who are under direct legal contract with the scope owner, computer systems on the property of the scope owner, and EM or MW signals or emanations of power level great enough to disrupt or harm wireless communications within the scope. Analysts must make efforts to not invade upon a person's private life such as listening to or recording personal communications originating within the scope, where that private life has made efforts to separate itself from the scope.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 9.1 *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 to which testing should be mapped but not constrained.

### 9.1.1 Policy

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

### 9.1.2 Legislation

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.

### 9.1.3 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.

### 9.1.4 Age

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

### 9.1.5 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.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 9.2 *Logistics*

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

### 9.2.1 Communications Equipment

Test for equipment which may transmit Electromagnetic Radiation, such as CRTs, LCDs, printers, modems, and cell phones, and which may be used to recreate the data that is displayed on the screen, printed, or transmitted, etc. Exploiting this vulnerability is known as Van Eck phreaking.

### 9.2.2 Communications

Test which protocols are used within the scope and methods of transmission.

### 9.2.3 Time

Test for the time frame of equipment operation. For example, is a wireless access point (AP) available 24/7 or just during normal business hours?

## 9.3 *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 creating false positives and negatives in the test result data as well as changing the alarm status of monitoring personnel or agents.

### 9.3.1 Channel Monitoring

Test whether controls are in place for monitoring intrusion or signal tampering.

### 9.3.2 Channel Moderating

Test whether controls are in place to block signals (jamming) or alert for unauthorized activities.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 9.4 *Visibility Audit*

Enumeration and verification tests for the visibility of personnel with which interaction is possible via all channels.

### 9.4.1 Interception

Locate Access Control, Perimeter Security, and Ability to Intercept or Interfere with wireless channels.

### 9.4.2 Passive Signal Detection

(a) Determine which frequencies and signals can leak into or out of the target area using a directional, high gain antenna and passive detection means such as frequency analysis.
(b) Create a heat map of the scope showing all sources of the radiation and their radii and strength.
(c) Test for sources that interact without authorization.
(d) Collect information broadcast by these sources.
(e) Map all found data to the emission limit values currently required in the region for all detected radiation.

### 9.4.2 Active Signal Detection

Examine which frequencies or electromagnetic signal broadcasts trigger responses such as that from RFID or other interactive wireless sources. (Radio Frequency Identifier tags are composed of an integrated circuit, which is sometimes half the size of a grain of sand, and an antenna – usually a coil of wires. Information is stored on the integrated circuit and transmitted via the antenna when probed by the right signal. The exact frequencies used in RFID systems may therefore vary by country or region.)

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 9.5 *Access Verification*

Tests for the enumeration of access points to personnel within the scope. While access to personnel outside of the scope is a real scenario and one often used for information property theft, the Analyst may be limited to scope-only interaction to protect the independent privacy rights of the personnel in their private life.

### 9.5.1 Evaluate Administrative Access to Wireless Devices

Determine if access points are turned off during portions of the day when they will not be in use.

### 9.5.2 Evaluate Device Configuration

Test and document using directional and high-gain antennas that wireless devices are set to the lowest possible power setting to maintain sufficient operation that will keep transmissions within the secure boundaries of the organization.

### 9.5.3 Evaluate Configuration, Authentication, and Encryption of Wireless Networks

Verify that the access point's default Service Set Identifier (SSID) has been changed.

### 9.54 Authentication

Enumerate and test for inadequacies in authentication and authorization methods.

### 9.5.5 Access Control

Evaluate access controls, perimeter security, and ability to intercept or interfere with communication, determining the level of physical access controls to access points and devices controlling them (keyed locks, card badge readers, cameras, etc.).

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 9.6 *Trust Verification*

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

### 9.6.1 Misrepresentation

Test and document the authentication-method of the clients.

### 9.6.2 Fraud

Test and document the depth of requirements for access to wireless devices within the scope with the use of fraudulent credentials.

### 9.6.3 Resource Abuse

Test and document the depth of requirements to send the property outside of the scope to a known and trusted source or throughout the scope itself to other personnel without any established, required credentials.

### 9.6.4 Blind Trust

Test and document the connections that are made to a false or compromised receiver.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 9.7 *Controls Verification*

Tests to enumerate types of loss controls used to protect information.

### 9.7.1 Non-repudiation

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, and document the depth of the recorded interaction and the process of identification.

### 9.7.2 Confidentiality

Enumerate and test for use of equipment to dampen Electromagnetic transmission signals outside of the company and the controls in place for securing or encrypting wireless transmissions.

### 9.7.3 Privacy

Determine the level of physical access controls to access points and devices controlling them (keyed locks, card badge readers, cameras, etc.).

### 9.7.4 Integrity

Determine that data can only be accessed and modified by those that are authorized and ensure that adequate encryption is in use for guaranteeing signing and confidentiality of communications.


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 9.8 *Process Verification*

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

### 9.8.1 Baseline

Examine and document the baseline configuration to ensure the security stance is in-line with the security policy.

### 9.8.2 Proper Shielding

Examine and determine that proper shielding is in place. For example, determine that printers are in specially shielded cabinets to block EMT, panels or metallic paint are used to block wireless signals, etc.

### 9.8.3 Due Diligence

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

### 9.8.4 Indemnification

Document and enumerate that 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. Verify the legality and appropriateness of the language in the disclaimers.

## 9.9 *Configuration Verification*

Tests to examine the ability to circumvent or disrupt functional security in assets.

### 9.9.1 Common Configuration Errors

Perform brute force attacks against access points to discern the strength of passwords. Verify that passwords contain both upper and lower case letters, numbers, and special characters. Access points which use case insensitive passwords, make it easier for attackers to conduct a brute force guessing attack due to the smaller space of possible passwords.

### 9.9.2 Configuration Controls

Examine controls, including baseline configuration, to validate configurations are according to the security policy.

### 9.9.3 Evaluate and Test Wiring and Emissions

Verify that all wiring feeds into and out of shielded rooms are made of fiber, where possible.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 9.10 Property Validation

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

### 9.10.1 Sharing

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

### 9.10.2 Rogue Wireless Transceivers

Perform a complete inventory of all wireless devices. Verify that the organization has an adequate security policy that addresses the use of wireless technology.

## 9.11 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.

### 9.11.1 Privacy Containment Mapping

Map gatekeepers of private information within the scope, what information is stored, how and where the information is stored, and over which channels the information is communicated.

### 9.11.3 Disclosure

Examine and document types of disclosures of private information in wireless spectrum.

### 9.11.4 Limitations

Examine and document types of gateways and channel alternatives accessible to people with physical limitations within that channel.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 9.12 Exposure Verification

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

### 9.12.1 Exposure Mapping

Enumerate and map personnel 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, log-ins, log-in schemes, passwords, back-up methods, insurers, or any particular organizational information stated implicitly as confidential in regulations and policy.

### 9.12.2 Profiling

Examine and verify with the use of a directional and high-gain antenna if wireless signals with information regarding the device are extending out past the target's walls or property.

## 9.13 Competitive Intelligence Scouting

Tests for scavenging property 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.

### 9.13.1 Business Grinding

Map targets within the scope from active and passive analysis of emanations: what information is stored, how and where the information is stored, and how the information is communicated.

### 9.13.2 Business Environment

Explore and document 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.

### 9.13.3 Organizational Environment

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.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 9.14 Quarantine Verification

The determination and measurement of effective use of quarantine for all access to and within the target.

### 9.14.1 Containment Process Identification

Identify and examine quarantine methods and processes at the target in all channels for aggressive and hostile contacts.

### 9.14.2 Containment Levels

Verify the state of containment, length of time, and all channels where interactions have quarantine methods. Ensure that methods are within legal context and boundaries.

## 9.15 Privileges Audit

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

### 9.15.1 Identification

Examine and document the process for obtaining identification through both legitimate and fraudulent means on all channels.

### 9.15.2 Authorization

Verify the use of fraudulent authorization on all channels to gain privileges similar to that of other personnel.

### 9.15.3 Escalation

Verify and map access to information through the use of privileges to gain higher privileges.

### 9.15.4 Subjugation

Enumerate and test for inadequacies from all channels to use or enable loss controls not enabled by default.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 9.16 *Survivability Validation*

Determining and measuring the resilience of the target within the scope to excessive or hostile changes designed to cause service failure.

### 9.16.1 Continuity

Enumerate and test for inadequacies from target with regard to access delays and service response time through back-up personnel or automated means for alternate access.

### 9.16.2 Resilience

Map and document the process of gatekeepers disconnecting channels due to breach or safety concerns as a gap analysis with regulation and security policy.

## 9.17 *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.

### 9.17.1 Alarm

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 noted by personnel upon suspicion of circumvention attempts, social engineering, or fraudulent activity.

### 9.17.2 Storage and Retrieval

Document and verify unprivileged access to alarm, log, and notification storage locations and property.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

**In telecommunications people are as much a part of the process as are the machines. They are rarely mutually exclusive.**

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org



# Chapter 10 - Telecommunications Security Testing

COMSEC is a classification for the material security within the ELSEC realm which is within the limits of telecommunications over wires.

This channel covers the interaction of the Analyst with the targets. While some services consider this simply as "phreaking", the true compliance objective of security testing in this channel is logical barrier testing and gap measurement against the required security standard as outlined in company policy, industry regulations, or regional legislation.

The Analyst will be required to have multiple tools and methods for the completion of some tasks to assure that suspicion is not raised among personnel by continual and sequential ringing of phones and that tests are not made invalid due to an early discovery or heightened paranoia. Analysts will also need to be prepared for working with both digital and analog telecommunications equipment, sound frequency analyzers, and within information networks providing regional content through local phone providers.

Competent Analysts will require an electronics background in both analog and digital telephony 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: Analysts 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. Analysts are considered professionals in this subject matter and, therefore, the assumption exists that even what may not be common knowledge for a normal person about a foreign region's laws regarding computer systems, will be known by professionals as they are aware of the laws necessary to engage in their undertakings.

2. Property rights: Testing must specifically target only systems which are under direct legal ownership of the scope owner or computer systems on the property of the scope owner. Such property or personal effects should remain personal and private unless it specifically involves the scope owner through disparagement, false light, competitiveness, or reasons stated in personnel contract agreements. Analysts 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. Analysts with a special agreement to test systems which are under direct contract but not owned, or are owned but not housed on the owner's legal property, must take great caution to assure tests have minimum impact on other systems outside the scope or contract.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *10.1 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. In most cases, a target may also have contracts with providers and other third parties which may need to be reviewed and documented. This review forms a matrix against which testing should be mapped but not constrained, 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.

### 10.1.1 Policy

(a) Review and document appropriate organizational policy regarding security, integrity, and privacy requirements of the scope. Verify the limitations on telecommunications imposed by the security policy.
(b) Review and document contracts and Service Level Agreements (SLAs) with service providers and other involved third parties.

### 10.1.2 Legislation

Review and document appropriate regional and national legislation 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. Where applicable, pay special attention to privacy and data retention of Call Detail Records, laws and rulings governing interception or monitoring of telecommunications, and provision of critical services such as E-911.

### 10.1.3 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.

### 10.1.4 Age

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

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

#### 10.1.5 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.

#### 10.1.6 Attack Vectors

(a) PBX testing
(b) Voice mailbox testing
(c) FAX and Modem surveying, polling, and testing
(d) Remote Access Services (RAS) testing
(e) Backup ISDN lines testing
(f) Voice over IP testing
(g) X.25 packet switched network testing

### *10.2 Logistics*

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

#### 10.2.1 Framework

(a) Verify the scope and the owner(s) of the targets outlined for the audit, along with the carrier(s) and other third parties managing the telecommunication lines and infrastructure for the targets.
(b) Determine the property location and the owner of the property housing the targets.
(c) Search for other targets from the same owner.
(d) Find and verify the paths of telecommunication services which interact outside of target for the paths they follow into and out of the scope.
(e) Determine the physical location of the targets.
(f) Test which protocols are used within the scope (example: PSTN, ISDN, GSM, UMTS, SIP, H.323, RTP, XOT, DECNET, IPX, etc.).
(g) Verify and document the special limitations imposed by the contract with client.

#### 10.2.2 Network Quality

(a) Measure the maximum and minimum connection speeds supported by targets.
(b) Determine and verify the appropriate connection speed, parity, RING time, and other specific configuration parameters to be used for scanning and testing.
(c) Verify and document particular limitations imposed by the scope (example: X.25 network congestion, XOT strict routes, access filters based on CLID).

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

10.2.3 Time and Additional Costs

(a) Test the time frame of equipment operation (example: call redirect to answering machine out of normal business hours).
(b) Determine and document the time settings (timezone, DST, etc.) for the targets.
(c) Assure the Analyst's time clock is in sync with the time of the targets. Certain equipment like fragile artifacts may have time settings that do not represent a valid time; if the Analyst's time clock is put in sync with these it may have an impact on the result of the test.
(d) Determine the additional financial costs involved in performing thorough tests from a remote location (example: scanning for modems/FAX, testing Remote Access Services not on toll-free numbers, placing X.25 calls without reverse charge).

## *10.3 Active Detection Verification*

Determination of active controls to detect intrusion and 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 personnel within the scope.

10.3.1 Monitoring

(a) Test whether telecommunications are monitored by an authoritative party for relaying improper network data, code injections, malicious content and improper conduct, and record responses and response time.
(b) Test whether controls are in place for monitoring fraudulent activities or services tampering, and record responses and response time such as in periodic billing reconciliation using Call Detail Records (CDR).

10.3.2 Filtering

(a) Test whether network-level controls are in place for blocking unauthorized activities and record responses and response time such as access filters based on Call Line Identification (CLID), Network User Address (NUA), or Closed User Group (CUG).
(b) Test whether application-level controls are in place for blocking unauthorized activities and record responses and response time.

10.3.3 Active Detection

(a) Verify active responses to probes from systems and services.
(b) Verify if protection from brute force attacks such as account locking are in place.
(c) Map any applications, systems, or network segments within the scope which produce logs, alarms, or notifications.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *10.4 Visibility Audit*

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

### 10.4.1 Network Surveying

(a) Compile a map of communication protocols in use within the scope.
(b) Outline the topology of the telecommunication networks within the scope.

### 10.4.2 Enumeration

(a) PBX testing: enumerate telephony systems within the scope.
(b) Voice mailbox testing: find voice mailboxes within the scope.
(c) FAX testing: enumerate FAX systems within the scope.
(d) Modem survey: find all systems with listening and interactive modems within the scope.
(e) Remote Access Services testing: enumerate RAS systems within the scope.
(f) Backup ISDN lines testing: enumerate network devices with backup ISDN lines within the scope.
(g) Voice over IP testing: enumerate VoIP systems within the scope.
(h) X.25 packet switched network testing: find live and reachable systems within the scope, recording their response codes.

### 10.4.3 Identification

(a) Identify OS types and versions in use on systems within the scope.
(b) Identify service types and versions in use on systems within the scope.
(c) Identify modem and FAX types and operating programs.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 10.5 Access Verification

Tests for the measurement of the breadth and depth of interactive access points leading within the scope and required authentication.

### 10.5.1 Access Process

(a) PBX testing: find PBX systems that are allowing remote administration or world access to the maintenance terminal, either via telephone dial-in or IP network.
(b) Voice mailbox testing: find voice mailboxes that are world accessible.
(c) FAX testing: find FAX systems that are allowing remote administration or world access to the maintenance terminal.
(d) Modem survey: test and document the authentication protocols in use (example: terminal, PAP, CHAP, others).
(e) Remote Access Services testing: test and document the authentication protocols in use (example: terminal, PAP, CHAP, others).
(f) Backup ISDN lines testing: test and document the authentication protocols in use (example: terminal, PAP, CHAP, others).
(g) Voice over IP testing: verify the possibility of performing toll fraud, call eavesdropping or tracing, call hijacking, CLID spoofing, and Denial of Service, using attacks targeting converging networks, VoIP network elements, signaling and media transport protocols.
(h) X.25 packet switched network testing: find systems that are allowing remote administration, access to other services via specific CUDs, or reverse charge, verify how many Virtual Channels (VCs) and Permanent Virtual Channels (PVCs) are in use and how they are managed (CUG, sub-addresses mapping, incoming X.25 calls screening, filtering based on NUA, etc.).

### 10.5.2 Services

(a) Request known, common remote services.
(b) Identify the components of services and their versions.
(c) Verify service uptime to latest vulnerabilities and patch releases.
(d) For each identified service, remotely test, and document configuration errors.
(e) For each identified application, remotely test, and document programming errors.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

10.5.3 Authentication

(a) Enumerate telecommunication resources requiring authentication and verify all acceptable forms of privileges to interact or receive access.
(b) Document the authentication schemes in use, verify the process for receiving authentication, and test for logic errors.
(c) Verify the methods of authorization and the identification required.
(d) Ensure administrative accounts do not have default or easily guessed credentials.
(e) Ensure user accounts do not have default or easily guessed credentials.
(f) Verify and test protections against brute force and dictionary type attacks.
(g) Verify and test password complexity checks and voice mailbox PIN size, password aging, and frequency of change controls.
(h) Try "known" credentials on all enumerated access points, to verify password re-usage controls.
(i) Verify the format used for storage of authentication credentials and document clear-text or obfuscated passwords and weak encryption algorithms.
(j) Verify the format used for transmission of authentication credentials through the network and document clear-text or obfuscated passwords and weak encryption algorithms.
(k) Verify that authentication information whether attempted, successful, or failed. is appropriately logged.

## *10.6 Trust Verification*

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

10.6.1 Spoofing

(a) Test and document the access methods in use that do not require submission of authentication credentials.
(b) Test and document the depth of requirements for interaction with and access to property within the scope by means of spoofing a trusted source (example: CLID and X.25 NUA spoofing).

10.6.2 Resource Abuse

(a) Test and document the depth of requirements to take property outside of the scope to a known and trusted source or throughout the scope itself without any established, required credentials.
(b) Test and document the property available from outside of the scope due to information leaks.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *10.7 Controls Verification*

Tests to enumerate and verify the operational functionality of safety measures for assets and services, defined by means of process-based (Class B) loss controls. The control of alarm is verified at the end of the methodology.

### 10.7.1 Non-repudiation

(a) Enumerate and test for use or inadequacies from applications 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 interaction are properly recorded with proper identification.
(d) Identify methods of identification which defeat repudiation.

### 10.7.2 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 involved parties.
(b) Verify the acceptable methods used for confidentiality.
(c) Test the strength and design of the encryption or obfuscation methods.
(d) Verify the outer limits of communication which can be protected via the applied method of confidentiality.

### 10.7.3 Privacy

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 privacy of the interaction and the process of providing assets only to those within the proper security clearance for that process, communication, or asset.

### 10.7.4 Integrity

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, switched, redirected, or reversed without it being known to parties involved.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *10.8 Process Verification*

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

### 10.8.1 Baseline

Examine and document the baseline services to ensure the processes are in line with the security policy.

### 10.8.2 Maintenance

Examine and document the timeliness, appropriateness, access to, and extent of processes for the notification and security awareness of personnel in regards to operational security, actual security, and loss controls.

### 10.8.3 Misinformation

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

### 10.8.4 Due Diligence

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

### 10.8.5 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 effect of the disclaimers upon security or safety measures.
(d) Examine the language of the insurance policy for limitations on types of damages or assets.
(e) Compare cultural access policy with indemnification policy for evidence of weaknesses.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *10.9 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.

### 10.9.1 Configuration Controls

(a) Examine controls, including baseline configuration, to validate proper configurations of equipment, systems, and applications within the scope.
(b) Examine controls to ensure configurations of equipment, systems, and applications match the intent of the organization and reflect a business justification.
(c) Examine Access Control Lists (ACLs) configured on networks, systems, services, and applications within the scope, to ensure they match the intent of the organization and reflect a business justification.

### 10.9.2 Common Configuration Errors

(a) PBX testing: check for unnecessary, insecure or unused services/features and default credentials, verify the patch level of PBX systems to identify known vulnerabilities.
(b) Voice mailbox testing: check for unnecessary, insecure or unused services/features and default credentials, verify the patch level of voice mailbox systems to identify known vulnerabilities.
(c) FAX testing: check for unnecessary, insecure or unused services/features and default credentials, verify the patch level of FAX systems to identify known vulnerabilities.
(d) Modem survey: check for unnecessary or unused answering modems within the scope.
(e) Remote Access Services testing: check for unnecessary, insecure or unused services/features and default credentials, verify the patch level of RAS servers to identify known vulnerabilities.
(f) Backup ISDN lines testing: check for unnecessary, insecure or unused services and default credentials, verify the patch level of network equipment to identify known vulnerabilities.
(g) Voice over IP testing: check for unnecessary, insecure or unused services/protocols and default credentials on all systems within the VoIP infrastructure, and verify their patch level to identify known vulnerabilities.
(h) On X.25 packet switched network testing check for unnecessary, insecure or unused services and default credentials on all X.25 systems, and verify their patch level to identify known vulnerabilities.

### 10.9.3 Source Code Audit

Examine the available source code of applications where available to validate controls balance operations.


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *10.10 Property Validation*

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

### 10.10.1 Sharing

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

### 10.10.2 Black Market

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.

### 10.10.3 Sales Channels

Verify public, out of scope businesses, auctions, or property sales which provide contact information through channels originating within the scope.

### 10.10.4 Rogue Modems

Perform a complete inventory of all modems within the scope. Verify that the organization has adopted an adequate security policy that addresses the use and provision of modems.

## *10.11 Segregation Review*

Tests for appropriate separation of private or personal information 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 .

### 10.11.1 Privacy Containment Mapping

Map gatekeepers of private information within the scope, what information is stored, how and where the information is stored, and over which channels the information is communicated.

### 10.11.2 Disclosure

Examine and document types of disclosures of private information in communication services from gatekeepers responsible for this segregation according to policy and regulations as determined in the Posture Review and the basic human right to.

### 10.11.3 Limitations

Examine and document types of gateways and channel alternatives with gateways accessible to people with physical limitations within that channel such as in the TTY service.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *10.12 Exposure Verification*

Tests for uncovering public information which describes indirect visibility of targets within the scope or provides for or leads to authenticated access.

10.12.1 Exposure Mapping

(a) Identify personal and business information such as personal and work phone numbers, mobile phone numbers, toll-free phone numbers, FAX numbers, owners of the telecommunication lines, carriers, and organizational affiliations, using all available means such as company websites, phone books, on-line directory information, and telecommunication subscriber's databases.
(b) Identify other telecommunication lines such as X.25, using both company websites and search engines.
(c) Identify personal and business information such as organization charts, key personnel titles, job descriptions, private and public e-mail addresses, log-ins (example: X.25 PSI mail information leak), log-in schemes, passwords, back-up methods, insurers, or any particular organizational information stated implicitly as confidential in regulations and policy.

10.12.2 Profiling

Profile and verify the organization, its public telecommunication networks, employees, technologies, and business direction.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *10.13 Competitive Intelligence Scouting*

Tests for scavenging property 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.

### 10.13.1 Business Grinding

(a) Map gatekeepers of business property within the scope, what information is stored, how and where the information is stored, and over which channels the information is communicated.
(b) Measure the cost of telecommunication infrastructure based on equipment (example: phones, PBX, modems, FAX, etc.).
(c) Measure the cost of the support infrastructure, based on carrier and maintenance costs, including technical personnel.
(d) Verify what kind of business is managed through the telecommunication infrastructure (example: call center, customer care, help desk, etc.).
(e) Verify the amount of traffic in a defined time range.

### 10.13.2 Business Environment

(a) Explore and document 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) Identify telecommunication lines which are part of the business of partners.

### 10.13.3 Organizational Environment

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.

## *10.14 Quarantine Verification*

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

### 10.14.1 Containment Process Identification

Identify and examine quarantine methods and processes at the target in all channels for annoying, aggressive, or hostile contacts such as telemarketers, head hunters, and stalkers.

### 10.14.2 Containment Levels

Verify the state of containment, length of time, and all channels where interactions have quarantine methods. Ensure that methods are within legal context and boundaries.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *10.15 Privileges Audit*

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

10.15.1 Identification

Examine and document the process for obtaining identification through both legitimate and fraudulent means on all channels.

10.15.2 Authorization

(a) Verify the use of fraudulent authorization on all channels to gain privileges similar to that of other personnel.
(b) Test and document possible paths for bypassing Access Control Lists (ACLs) configured for networks, systems, services, and applications within the scope.

10.15.3 Escalation

Verify and map access to information through the use of privileges to gain higher privileges.

10.15.4 Subjugation

Enumerate and test for inadequacies from all channels to use or enable loss controls not enabled by default.

## *10.16 Survivability Validation*

Determining and measuring the resilience of the target within the scope to excessive or hostile changes designed to cause service failure.

10.16.1 Continuity

(a) Enumerate and test for inadequacies from target with regard to access delays and service response time through back-up personnel or automated means for alternate access.
(b) Enumerate and test for inadequacies from target with regard to Quality of Service issues and performance requirements of telecommunication technologies.

10.16.2 Resilience

Map and document the process of gatekeepers disconnecting channels due to breach or safety concerns as a gap analysis with regulation and security policy.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *10.17 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.

10.17.1 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 upon suspicion of intrusion attempts or fraudulent activity and determine clipping levels.
(b) Review outgoing and incoming call detail logs for signs of abuse or fraud.
(c) Test and document log management systems.

10.17.2 Storage and Retrieval

(a) Document and verify the unprivileged access to alarm, log, and notification storage locations and property.
(b) Test and document logging backup policy and logging to multiple locations, to ensure that audit trails cannot be tampered with.
(c) Test and document log management systems.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

**The 3 rules of data security tools are: 1. tools don't know when they lie, 2. tools are only as smart as their designers, and 3. tools can only work properly within the confines of the environment they were made for.**

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

# Chapter 11 - Data Networks Security Testing

The tests for the Data Networks 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 organizations 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, or regional legislation.

During testing, end operators and artificial intelligence can recognize on-going attacks both by process and signature. For this reason, the Analyst 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 the discovery of new problems only leave room for fixes and not designs for future improvements.

Competent Analysts 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: Analysts 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. Analysts 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. Analysts 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. Analysts 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 and tertiary parties outside the scope or contract.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *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 against which testing should be mapped but not constrained 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.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 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 information.
(d) Verify the owner of the target domains from domain registration information.
(e) Verify the ISP(s) providing network access or redundancy.
(f) Search for other IP blocks and targets related to the same owner(s).
(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) 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.
(m) Use reverse name look-ups as an additional information source towards determining 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 timezone, holidays, and work schedules for the various systems within the scope including partners, resellers, and influential customers interacting with the scope.
(b) Identify the Time To Live (TTL) distance to the gateway and the targets.
(c) Assure the Analyst's clock is in sync with the time of the targets.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *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 relay of improper materials, code injections, malicious content, and improper conduct and record 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 relay of improper materials, code injections, malicious content, and improper conduct and record 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, Security Information Management tools (SIMs), application logs, and the like.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 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 target network segment(s) and the vector from which they will be tested.
(b) Use network sniffing to identify emanating protocols from network service responses or requests where applicable. For example, Netbios, ARP, SAP, NFS, BGP, OSPF, MPLS, RIPv2, etc.
(c) Query all name servers and the name servers of the ISP or hosting provider, if available, for corresponding A, AAAA, and PTR records as well as ability to perform zone transfers to determine the existence of all targets in the network and any related redundancies, load balancing, caching, proxying, and virtual hosting.
(d) Verify broadcast requests and responses from all targets.
(e) Verify and examine the use of traffic and routing protocols for all targets.
(f) Verify ICMP responses for ICMP types 0-255 and ICMP codes 0-2 from all targets.
(g) Verify default and likely SNMP community names in use are according to practical deployments of all SNMP versions.
(h) Verify responses from targets to select ports with TTL expiration set to less than 1 and 2 hops from the targets. For example:
TCP 8, 22, 23, 25, 80, 443, 445, 1433
UDP 0, 53, 139, 161
ICMP T00:C00, T13:C00, T15:C00, T17:C00
(i) Trace the route of ICMP packets to all targets.
(j) Trace the route of TCP packets to all targets for ports SSH, SMTP, HTTP, and HTTPS ports.
(k) Trace the route of UDP packets to all targets for DNS and SNMP ports.
(l) Identify TCP ISN sequence number predictability for all targets.
(m) Verify IPID increments from responses for all targets.
(n) Verify the use of Loose Source Routing to the target gateway and outer perimeter systems to route packets to all targets.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

11.4.2 Enumeration

(a) Search newsgroups, forums, 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) Examine service and application emanations. Manipulate and replay captured traffic to invoke new requests or responses, gain depth, or expose additional information. For example, SQL, Citrix, HTTP, SAP, DNS, ARP, etc.
(e) Search web logs and intrusion logs for system trails from the target network.
(f) Verify all responses from UDP packet requests to ports 0-65535.
(g) Verify responses to UDP packet requests FROM SOURCE ports 0, 53, 139, and 161 to 0, 53, 69, 131, and 161.
(h) Verify responses to UDP packet requests with BAD CHECKSUMS to all discovered ports and for 0, 53, 69, 131, and 161.
(i) Verify service request responses to common and contemporary UDP remote access malware ports.
(j) Verify responses from TCP SYN packet requests to ports 0-65535.
(k) Verify responses from TCP service requests to ports 0, 21, 22, 23, 25, 53, 80, and 443.
(l) 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.
(m) Verify responses from TCP SYN fragments to ports 0, 21, 22, 23, 25, 53, 80, and 443.
(n) Verify responses from all combinations of TCP flags to ports 0, 21, 22, 23, 25, 53, 80, and 443.
(o) Verify the use of all targets with HTTP or HTTPS based VPNs, proxies, and URL redirectors to redirect requests for targets within the scope.
(p) Verify the use of all targets with sequential IPIDs to enumerate systems within the network.
(q) Map and verify for consistency visible systems and responding ports by TTLs.

11.4.3 Identification

Identify targets' TTL response, system uptime, services, applications, application faults, and correlate this with the responses from system and service fingerprinting tools.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 11.5 Access Verification

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

11.5.1 Network

(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) Manipulate network service and routing to access past restrictions within the scope.
(d) Request known, common Trojan services which utilize UDP for connections from all addresses.
(e) Request known, common Trojan services which utilize ICMP for connections from all addresses.
(f) 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 service banners (flags) for discovered TCP ports.
(b) Verify service banners (flags) 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 system uptime compared to the 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 uptime compared to the latest vulnerabilities and patch releases.
(h) Verify service and application against TTL and OS fingerprint results for all addresses.
(i) Verify HTTP and HTTPS for virtual hosting.
(j) Verify VoIP services.
(k) Manipulate application and service requests outside of standard boundaries to include special characters or special terminology of that service or application to gain access.

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 obtaining the proper Authorization for the authentication.
(c) Verify the method of being properly Identified for being provided the authentication.
(d) Verify the logic method of authentication.
(e) Verify the strength of the authentication through password cracking and re-applying discovered passwords to all access points requiring authentication.
(f) Verify the process for receiving authentication.
(g) Test for logic errors in the application of the authentication.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *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 do 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 within 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 if information is sent to the outside of the scope as padding to network packets such as that which has occurred previously as "Etherleak".
(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.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *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 of 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 involved 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 methods of confidentiality.

11.7.3 Privacy

(a) Enumerate services within the scope for communications or assets transported using specific, individual signatures, personal identification, "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 protocol.

11.7.4 Integrity

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, redirected, or reversed without it being known to the parties involved.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *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

(a) Examine and document the timeliness, appropriateness, access to, and extent of processes for notification and security response in regards to network and security monitoring.
(b) Verify the appropriateness and functionality of incident response and forensics capabilities for all types of systems.
(c) Verify the level of incident or compromise which the support channels can detect and the length of response time.

### 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

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.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *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 the configurations and baselines of systems, equipment and applications meet the intent of the organization and reflect a business justification.
(b) 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 and that they 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 administration interfaces of the equipment.

### 11.9.3 Limitations Mapping

(a) Check for unnecessary or unused services/features available.
(b) Check for default credentials.
(c) Identify if any known vulnerabilities are residing on the systems.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *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

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

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

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


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 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

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 legally identified as minors and verify what and how identifying information is provided from that child.

### 11.11.4 Discrimination

Verify information requested and privileges granted from gatekeepers in cases where age (specifically minors), 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, log-ins, log-in 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.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *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

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 employee skill requirement types, pay scales, channel and gateway information, technologies, and organizational direction from sources outside the scope.
(b) Profile data network set-ups and configurations from job databases and newspapers hiring ads for 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

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.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *11.14 Quarantine Verification*

The containment measures dictate the handling of traversal, malicious programs and egress. The identification of the security mechanisms and the response policy need to be targeted. It may be necessary to request first a new test mail account or desktop system that the administrator can monitor. Tests for verifying the proper fielding and containment of aggressive or hostile contacts at the gateway points.

### 11.14.1 Containment Process Identification

Identify and examine quarantine methods for aggressive and hostile contacts such as malware, rogue access points, unauthorized storage devices, etc.

### 11.14.2 Containment Levels

(a) Measure the minimum resources that need to be available to this subsystem in order for it to perform its task.
(b) Verify any resources available to this subsystem that it does not need to perform its tasks and what resources are shielded from use by this subsystem.
(c) Verify the detection measures present for the detection of attempted access to the shielded resources.
(d) Verify the features of the containment system.
(e) Verify detection measures are present for detection of 'unusual' access to the needed resources
(f) Measure the response and process against encoded, packaged, condensed, renamed, or masqueraded inputs.
(g) 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.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## *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

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 any means for gaining fraudulent authorization to gain privileges similar 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 persons with high privileges. Look for 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.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 11.16 Survivability Validation

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

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's 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 to target access which 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

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

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 noted 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.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

**Compliance requirements which enforce protection measures as a surrogate for responsibility are also a substitute for accountability.**

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

# Chapter 12 - 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. Legislative.** 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. Examples are Sarbanes-Oxley, HIPAA, and the various Data Protection and Privacy legislation.

**2. Contractual.** Compliance to contractual requirements are in accordance to the industry or within the group that requires the contract and may take action to enforce compliance. Failure to comply with contractual requirements often leads to dismissal from the group, a loss of privileges, loss of reputation, civil charges, and in some cases where legislation exists to support the regulatory body, criminal charges. An example is the payment card industry data security standard (PCI DSS) promoted and required by VISA and MasterCard.

**3. Standards based.** Compliance to standards is in accordance with the business or organization where the compliance to standards is enforced as policy. Failure to comply with standards often leads to dismissal from the organization, a loss of privileges, a loss of reputation or brand trust, civil charges, and in some cases where legislation exists to support the policy makers, criminal charges. Examples are the OSSTMM, ISO 27001/5, and ITIL.

The OSSTMM is developed with concern for major legislation, contractual requirements, and standards conformance. As not all compliance objectives are created equally, the main focus of the OSSTMM is security. Compliance measures that require specific products or services, commercial or otherwise, often through specially lobbied efforts, may have good intentions; however, may actually be a waste of resources or a lesser version of security than is desired. That a compliance objective can require a specific product at all should be illegal itself.

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, proving proper and valid operational protection and controls such that as can be proved by an OSSTMM test may or may not be satisfactory. Therefore, in addition a certified OSSTMM test complete with the STAR should also be presented to the appropriate auditing bodies.

The following list is only for compliance 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. If you are able to verify compliance measures not listed here according to the OSSTMM or need a specific compliance measure verified please send it to ISECOM for inclusion in this list. The compliance measure must be in English or sent to an ISECOM partner which exists within a region with that local language.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## 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.
- Australian Communications Authority - http://www.aca.gov.au/
- Australian Radiation Protection and Nuclear Safety Agency http://www.arpansa.gov.au/mph2.htm

### *Austria*

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

### *Belgium*

- Belgisch Staatsblad N. 189, June 2005

### *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.
- Royal Society of Canada - http://www.rsc.ca/

### *Estonia*

- Minister of Economic Affairs and Communications Information Security Policy

### *France*

- Société Française de Radioprotection - http://www.sfrp.asso.fr/


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *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-Grundschutz Catalogues) 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).
- Bundesamt für Strahlenschutz - http://www.bfs.de/

### *India*

- The Information Technology Act, 2000.

### *Italy*

- D.Lgs. n. 196/2003 - Codice in materia di protezione dei dati personali. Where in a Contract/Agreement the Client, owner of the treatment of the data, must assume any law responsibility as a sensitive data as medical, personal, judicial of Employees or Customers but even Dealers and Partners. A tester must be willing to accept all the consequent responsibility when accepting the Non Disclosure Agreement especially about the derived risk from the possible knowledge of sensitive data and the clause of reservation to the time limit of this special care which could be indefinite.

### *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.

### *Netherlands*

- Dutch Computer Crime Act II of September 1, 2006 changing the Dutch Computer Crime Act of 1993
- Council of Europe's Cybercrime Convention (CCC), 23 November 2001
- The ratification of Treaty "Convention on Cybercrime, Budapest, 23.XI.2001" effective June 1, 2006

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *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.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

### *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).
- Bundesamt für Kommunikation (BAKOM)
- Bundesamt für Umwelt

### *Thailand*

- Computer Crime Law.
- Privacy Data Protection Law.

### *United Kingdom*

- UK Data Protection Act 1998.
- Freedom of Information Act 2000
- Human Rights Act 2000
- Regulation of Investigatory Powers Act 2000
- Access to Health Records Act 1990
- Proceeds of Crime Act 2002
- Money Laundering Regulations 2003
- Electronics Communications Act 2000
- Electronics Signature Regulations 2002
- Privacy and Electronic Communications (EC Directive) Regulations 2003
- Electronic Commerce (EC Directive) Regulations 2003
- Companies (Audit, Investigations and Community Enterprise) bill
- 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.


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *United States of America*

- AICPA SAS 70 - verification 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).
- Computer Security Act of 1987 (P.L. 100-235)
- Office of Personnel Management (OPM) - Regulations Implementing Training Requirements of Computer Security Act of 1987 - 5 CFR Part 930, Subpart C
- COSO section 7 Information & Communication
- COBit section 3 Educate & Train Users
- North American Electric Reliability Council (NERC) - Standard 1300 section 1303.a.1, 1303.a.2, 1303.a.3
- U.S. Geological Survey Manual, 600.5 - Automated Information Systems Security - General Requirements, section 6 A
- Department of Veterans Affairs - VA DIRECTIVE 6210 section 2(d)(3)Security Awareness & Training
- Federal Information Security Management Act (FISMA) § 3544(a)(4), (b)(4)
- Executive Directive Appendix III to OMB Circular No. A-130
- State of Virginia ITRM Standard 95-1 section VI
- Food and Drug Administration - http://www.fda.gov
- Federal Communications Commission - http://www.fcc.gov/

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

**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.
- 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**

- 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).
- PCI-DSS 1.2 (Payment Card Industry - Data Security Standard)
- ISO/IEC 27001:2005 (Information security management systems - Requirements )
- ISO/IEC 27002:2005 (Code of Practice for Information Security Management)
- ILO and IMO Code of Practice – Security in Ports, Section 10
- Basel II (International)

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

**Security awareness should be the continuing practice of a skill and not the continuous reminder of a threat.**

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

# Chapter 13 – Reporting with the STAR

The STAR is the Security Test Audit Report. Its purpose is to serve as an executive summary of precise calculation stating the Attack Surface of the targets tested within a particular scope. This precision is made through the requirement of specifically noting what was NOT tested in addition to what has been tested in accordance to the OSSTMM.

The provided template is to be filled out completely (a copy of this template by itself can be found at the ISECOM website) and signed by the Analyst. It is then provided either to ISECOM with the scope owner's explicit permission or directly to the scope owner along with the full security test report. It is not a substitute for a full report.

When providing the STAR to ISECOM for verification, it is printed, signed by the verification auditor, and stamped by ISECOM. A certificate is provided for all tests which state the scope has been tested and verified. There is no passing or failing since there is no particular Attack Surface rav value that exists for all scopes as the cut-off between one that passes and one that fails. However, rav values for a scope above 90% will be marked by a stamp of excellence.


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org



# Security Test Audit Report

## OSSTMM 3.0 Security Verification Certification

OSSTMM.ORG - ISECOM.ORG

| | | | |
|---|---|---|---|
| **Report ID** | | **Date** | |
| **Lead Auditor** | | **Test Date Duration** | |
| **Scope and Index** | | **Vectors** | |
| **Channels** | | **Test Type** | |

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

| **SIGNATURE** | **COMPANY STAMP/SEAL** |
|---|---|
| | |
| **ISECOM Certification #** | **ISECOM Certification #** |

### OPERATIONAL SECURITY VALUES

| | |
|---|---|
| Visibility | |
| Access | |
| Trust | |

### LIMITATIONS VALUES

| | |
|---|---|
| Vulnerability | |
| Weakness | |
| Concern | |
| Exposure | |
| Anomaly | |

| | |
|---|---|
| **OpSec** | |
| **Limitations** | |

### CONTROLS VALUES

| | |
|---|---|
| Authentication | |
| Indemnification | |
| Resilience | |
| Subjugation | |
| Continuity | |
| Non-Repudiation | |
| Confidentiality | |
| Privacy | |
| Integrity | |
| Alarm | |

| | |
|---|---|
| **True Controls** | |
| **Security Δ** | |

| | | | |
|---|---|---|---|
| **True Protection** | | **Actual Security** | |

## 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 that is consistent and repeatable.

## ABOUT ISECOM

ISECOM, the creator and maintainer of the OSSTMM, is an independent, non-profit security research organization and certification authority defined by the principles of open collaboration and transparency.

## 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 the OSSTMM 3 vocabulary, which has been based on NCSC-TG-004 (Teal Green Book) from the US Department of Defense where applicable.

## 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 that provides evidence of the test and the results as defined in the statement of work between the testing organization and the client.

## VALIDITY

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 that maintain vigilance over their rav levels and have them validated yearly from an independent third-party auditor. Validation of security tests or quarterly metrics is subject to the ISECOM validation requirements to assure consistency and integrity.

## 1. POSTURE REVIEW

| | TASK | COMMENTS | COMPLETION STATUS |
|---|---|---|---|
| 1.1 | Identified business objectives and markets. | | |
| 1.2 | Identified legislation and regulations applicable to the targets in the scope. | | |
| 1.3 | Identified business policies. | | |
| 1.4 | Identified business and industry ethics policies. | | |
| 1.5 | Identified operation cultures and norms. | | |
| 1.6 | Identified operation times and flows applicable to the targets in the scope. | | |
| 1.7 | Identified all necessary Channels for this scope. | | |
| 1.8 | Identified all Vectors for this scope. | | |

## 2. LOGISTICS

| | TASK | COMMENTS | COMPLETION STATUS |
|---|---|---|---|
| 2.1 | Applied testing safety measures. | | |
| 2.2 | Determined and accounted for test instabilities. | | |
| 2.3 | Determined and accounted for downtime in scope. | | |
| 2.4 | Determined and accounted for test pace according to the test environment and the security presence. | | |

## 3. ACTIVE DETECTION VERIFICATION

| | TASK | COMMENTS | COMPLETION STATUS |
|---|---|---|---|
| 3.1 | Determined and accounted for interferences. | | |
| 3.2 | Tested with both interferences active and inactive. | | |
| 3.3 | Determined restrictions imposed on tests. | | |
| 3.4 | Verified detection rules and predictability. | | |

## 4. VISIBILITY AUDIT

| | TASK | COMMENTS | COMPLETION STATUS |
|---|---|---|---|
| 4.1 | Determined targets through all enumeration tasks. | | |
| 4.2 | Determined new targets by researching known targets. | | |

## 5. ACCESS VERIFICATION

| | TASK | COMMENTS | COMPLETION STATUS |
|---|---|---|---|
| 5.1 | Verified interactions with access points to all targets in the scope. | | |
| 5.2 | Determined type of interaction for all access points. | | |
| 5.3 | Determined source of interaction defined as a service or process. | | |
| 5.4 | Verified depth of access. | | |
| 5.5 | Verified known security limitations of discovered access points. | | |
| 5.6 | Searched for novel circumvention techniques and security limitations of discovered access points. | | |

## 6. TRUST VERIFICATION

| | TASK | COMMENTS | COMPLETION STATUS |
|---|---|---|---|
| 6.1 | Determined interactions that rely on other interactions to complete the test interaction according to the tasks. | | |
| 6.2 | Determined targets with trust relationships to other targets in the scope to complete interactions. | | |
| 6.3 | Determined targets with trust relationships to other targets outside the scope to complete interactions. | | |
| 6.4 | Verified known security limitations of discovered trusts between the trusts. | | |
| 6.5 | Verified known security limitations of discovered trusts between targets in the scope and the trusted interactions. | | |
| 6.6 | Searched for novel circumvention techniques and security limitations of discovered trusts. | | |

## 7. CONTROLS VERIFICATION

| | TASK | COMMENTS | COMPLETION STATUS |
|---|---|---|---|
| 7.1 | Verified controls for Non-Repudiation functioning according to all tasks. | | |
| 7.2 | Verified controls for Confidentiality functioning according to all tasks. | | |
| 7.3 | Verified controls for Privacy functioning according to all tasks. | | |
| 7.4 | Verified controls for Integrity functioning according to all tasks. | | |
| 7.5 | Verified controls for Alarm functioning according to all tasks. | | |
| 7.6 | Verified known security limitations of all controls Class B categories. | | |
| 7.7 | Searched for novel circumvention techniques and security limitations of all controls Class B categories. | | |

## 8. PROCESS VERIFICATION

| | TASK | COMMENTS | COMPLETION STATUS |
|---|---|---|---|
| 8.1 | Determined all processes controlling the action of interactivity with each access. | | |
| 8.2 | Verified the interaction operates within the confines of the determined process. | | |
| 8.3 | Verified the interaction operates within the confines of the security policy for such interactions. | | |
| 8.4 | Determined the gap between the operations of interactions and the requirements of posture from the Posture Review. | | |
| 8.5 | Verified known security limitations of discovered processes. | | |
| 8.6 | Searched for novel circumvention techniques and security limitations of discovered processes. | | |

## 9. CONFIGURATION AND TRAINING VERIFICATION

| | TASK | COMMENTS | COMPLETION STATUS |
|---|---|---|---|
| 9.1 | Verified configuration/training requirements according to the posture in the Posture Review. | | |
| 9.2 | Verified the application of appropriate security mechanisms as defined in the Posture Review. | | |
| 9.3 | Verified the functionality and security limitations within the configurations/training for the targets in the scope. | | |
| 9.4 | Searched for novel circumvention techniques and security limitations within configurations/training. | | |

## 10. PROPERTY VALIDATION

| | TASK | COMMENTS | COMPLETION STATUS |
|---|---|---|---|
| 10.1 | Determined the amount and type of unlicensed intellectual property distributed within the scope. | | |
| 10.2 | Verified 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 |
|---|---|---|---|
| 11.1 | Determined the amount and location of private information as defined in the Posture Review available through the targets. | | |
| 11.2 | Determined the type of private information as defined in the Posture Review available within the scope. | | |
| 11.3 | Verified the relationship between publicly accessible information outside the target detailing private or confidential information defined in the Posture Review and the scope. | | |
| 11.4 | Verified the accessibility of public accesses within the target to people with disabilities. | | |

## 12. EXPOSURE VERIFICATION

| | TASK | COMMENTS | COMPLETION STATUS |
|---|---|---|---|
| 12.1 | Searched for available targets through publicly available sources outside of the scope. | | |
| 12.2 | Searched for available organizational assets as defined in the Posture Review through publicly available sources outside of the scope. | | |
| 12.3 | Determined access, visibility, trust, and controls information available publicly within the targets. | | |
| 12.4 | Determined a profile of the organization's channel infrastructure for all channels tested through publicly available information within the targets. | | |
| 12.5 | 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 |
|---|---|---|---|
| 13.1 | Determined the business environment of partners, suppliers, workers, and market through publicly available information on targets within the scope. | | |
| 13.2 | Determined the business environment of partners, vendors, distributors, suppliers, workers, and market through publicly available information outside the scope. | | |
| 13.3 | Determined the organizational environment through publicly available information on targets within the scope. | | |
| 13.4 | Determined the organizational environment through publicly available information outside the scope. | | |

## 14. QUARANTINE VERIFICATION

| | TASK | COMMENTS | COMPLETION STATUS |
|---|---|---|---|
| 14.1 | Verified quarantine methods for interactions to the targets in the scope. | | |
| 14.2 | Verified quarantine methods for interactions from the targets to other targets outside the scope. | | |
| 14.3 | Verified length of time of quarantine. | | |
| 14.4 | Verified quarantine process from receive to release. | | |
| 14.5 | Verified known security limitations of discovered quarantines. | | |
| 14.6 | Searched for novel circumvention techniques and security limitations of discovered quarantines. | | |

## 15. PRIVILEGES AUDIT

| | TASK | COMMENTS | COMPLETION STATUS |
|---|---|---|---|
| 15.1 | Verified the means of legitimately obtaining privileges for all authenticated interactions. | | |
| 15.2 | Verified the use of fraudulent identification to obtain privileges. | | |
| 15.3 | Verified the means of circumventing authentication requirements. | | |
| 15.4 | Verified the means of taking non-public authentication privileges. | | |
| 15.5 | Verified the means hijacking other authentication privileges. | | |
| 15.6 | Verified known security limitations of discovered authentication mechanisms to escalate privileges. | | |
| 15.7 | Searched for novel circumvention techniques and security limitations of discovered authentication mechanisms to escalate privileges. | | |
| 15.8 | Determined depth of all discovered authentication privileges. | | |
| 15.9 | Determined re-usability of all discovered authentication privileges on the authentication mechanisms on all targets. | | |
| 15.10 | Verified requirements towards obtaining authentication privileges for discriminatory practices according to the Posture Review. | | |
| 15.11 | Verified means towards obtaining authentication privileges for discriminatory practices for people with disabilities. | | |

## 16. SURVIVABILITY VALIDATION AND SERVICE CONTINUITY

| | TASK | COMMENTS | COMPLETION STATUS |
|---|---|---|---|
| 16.1 | Determined measures applicable to disrupt or stop service continuity to and from the targets. | | |
| 16.2 | Verified continuity processes and safety mechanisms active for the targets. | | |
| 16.3 | Verified known security limitations of discovered safety and service continuity processes and mechanisms. | | |
| 16.4 | Searched for novel circumvention techniques and security limitations of discovered safety and service continuity processes and mechanisms. | | |

## 17. END SURVEY, ALERT AND LOG REVIEW

| | TASK | COMMENTS | COMPLETION STATUS |
|---|---|---|---|
| 17.1 | Verified methods for recording and alerting interactions to the targets in the scope. | | |
| 17.2 | Verified methods for recording and alerting interactions from the targets to other targets outside the scope. | | |
| 17.3 | Verified speed of recording and alerting. | | |
| 17.4 | Verified persistence of recording and alerting. | | |
| 17.5 | Verified integrity of recording and alerting. | | |
| 17.6 | Verified distribution process of recording and alerting. | | |
| 17.7 | Verified known security limitations of discovered recording and alerting methods. | | |
| 17.8 | Searched for novel circumvention techniques and security limitations of discovered recording and alerting methods. | | |

**The more you move away from the prison concept of security, the more you require the cooperation and good intentions from the people you are securing.**

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

# Chapter 14 – What You Get

What we will get from utilizing OSSTMM is really just about having a deep understanding of the interconnectedness of things. The people, processes, systems, and software all have some type of relationship. This interconnectedness requires interactions. Some interactions are passive and some are not. Some interactions are symbiotic while others are parasitic. Some interactions are controlled by one side of the relationship while others are controlled by both. Then some controls are flawed or superfluous, which is harmful to at least one side of the relationship, if not both. Other controls balance perfectly with the interactions. Whatever becomes of the interconnectedness, however the interactions occur, however they are controlled, they are the operations that make survival possible. When we test operations we get the big picture of our relationships. We get to see the interconnectedness of the operations in fine detail. We get to map out how we, our businesses, and our operations will survive and even thrive.

Unfortunately, how we interact is just based on a collection of biases we accumulate during life, which are subjected to the emotional or bio-chemical state we are under when we have them. These are our shortcuts. Due to the incredible number of decisions we must make through-out all of our interactions we use a mental cheat-sheet to compare similar interactions rather than calculate each situation independently. We are, after all, only human. Most often though our opinions are limited and restricted to a small scope we know as "our little world". We apply them everywhere because they make life easier. But when we take them with us and try to adhere them to larger, different, more complicated series and types of interactions, we will likely make mistakes. What may make perfect sense to us based on our experiences may not make any sense at all outside of "our little world". So what we need is a better, less biased way of looking at the bigger, more dynamic, less personal, world beyond ourselves.

Furthermore, our little world is something we take around with us. When we are outside, our little world is outside with us. We interact in the space on the assumptions and prejudices we know and carry. When we go inside, we take our little world inside with us. This means we bring our ways of doing things and new interactions into a new environment. And it has always been this way. There is no perimeter. There is no us and them. It is each individual interacting and interconnecting with everyone and everything; each individual with their own little world of issues and preconceptions impacting on the rest, while at the same time being impacted by others. This means we need a way to see more than just the bigger world; we also need a way to see into each individual's own little worlds too.

Often the difficulty in creating security is blamed on the sophistication and the persistence of the attacks. However that only serves to shift the blame, but not solve the problem. The real challenge is in protecting particular interactions in an interconnected world filled with uncontrollable elements. Taken at face value, the sheer number of interactions may be daunting. Protection solutions often address this challenge by broadly addressing particular types of interactions or by monitoring all interactions as they occur for malicious intent. Unfortunately, broad security programs and processes cannot address enough of the elements as to provide significant protection. This leads security in practice to be more of an art depending on the practitioner to apply their own little world to the challenge of security. This can only add more complexity and new problems. The means to finding global, persistent protection in perfect balance with operations is through the Möbius Defense.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

## The Möbius Defense

Due to the multitude of means in which interactions occur to and from any organization, such as the various Channels and vectors, the perimeters to be defended appear to take the shape of a Möbius strip. A Möbius Strip is a shape with no inside or outside which means there is no "side" to defend from. Therefore, what is needed is a defense designed to protect an environment where in each individual can be interacting and interconnecting with everyone and everything. The Möbius Defense does this in three steps:

1. Improving verification and analysis: verify and analyze operations for interactions and controls and not just flaws.
2. Establishing defense in width: apply defensive tactics to balance the controls of all interactions with operations.
3. Implementing a trust strategy: compartmentalize how interactions are authorized or controlled.

### *1. Improving Verification and Analysis*

The practice of verifying operational security must include more than just finding flaws. There needs to be a better accounting for and understanding of errors that will make tests inaccurate. There needs to be an improvement in test accuracy through a better understanding of what to test and when to test it. Increasing the accuracy of test results will serve to both provide results that can be repeated and results which can be used to make consistent measurements. The security test must catalog and classify all points of interaction, determine which controls exist for those interactions, and verify the functionality of those controls. Flaws within the scope or the controls must be classified by how they affect operations and not the possible or potential risk they pose to operations. The security test must also track that which was not tested and which tests were not performed to assure repeatability and fair comparisons with past and future tests. Finally, the testing Analyst must be capable of properly understanding the results of the test and what they mean for operations. The means to do all of this are provided within this manual.

### *2. Establishing Defense in Width*

The main concept behind a Möbius Defense is to provide Defense in Width and a balanced variety of controls to each interactive point. A perfect balance is achieved with the flawless application of all ten types of operational controls for each interactive point. This differs from Defense in Depth by assuring different types of controls applied to all interactive points rather than just any controls at various points within a process. With new information from the security test, a defensive posture can be created by verifying that a balance of controls exists at all points of interaction. This changes the environment in which inter-connectivity occurs, and curtails the possible operational changes caused by chaotic elements either inside or outside.

The balance of controls is important because each control can add to the attack surface of an operation. Assuring a balance also assures that different types of controls are used which provide protection in different ways. This increases the range of attack types and problems that the interactive point can be defended against. The ravs are to be used to measure the amount of balance attained and to assure balance is maintained as new operations are introduced to the scope. This manual covers all the information required to build Defense in Width.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

### *3. Implementing a Trust Strategy*

To know which interactions require less balance than others from Defense in Width is a matter of knowing which interactions we should trust. For the operations we have less reason to trust, we should apply more of the ten controls to achieve perfect balance. Individuals we have less reason to trust we place in environments where all interactions are protected by more of the ten controls. Conversely, trustworthy individuals can be authorized to have more individual control over the interactions in their environment. Finally we should separate elements from the environment when no significant reason to trust or benefit to the operation can be found in those elements. Doing so will also keep Defense in Width within a reasonable scale of operations so that efficiency and expense do not outweigh the benefits of protection.

The trust metrics provided within this manual assure that the reasons to trust are based on facts. As the reasons to trust approach 100% we are not only certain that the individual or the operation are incapable of malicious or accidental damage but that it has been proven. This is no risk assessment or guess based on what we know from our "own little world." The difficulty in this process however may be in assigning trust metrics to people. Unlike the informal and almost capricious way trust is often assigned, this new manner may seem cold and heartless. But it isn't because while you are investigating what reasons you have to trust someone you are also able to fully inform them of what they can do to give you more reason to trust them. The typical means of trusting or not trusting is not so specific, nor is it so kind. It is more of a social game of being likeable or not to the person providing the authorization. The trust metrics are more transparent and more neutral aside from how someone feels based on their "own little world." The trust metrics can even be verified by others, such as a board or a department, who can maintain the trust calculations neutrally and re-assess regularly or whenever it's necessary.

## Get What We Need

The application of the Möbius Defense has many ramifications. First, it assures that the results of security tests are the facts. It assures that the tests have been thorough and based on the processes of operations and not the skills of the Analyst. This provides an organization with an incredible amount of intelligence over their own operations for comparisons with other organizations, or even just trending self assessments. It is the kind of information that decisions require, and that which foster significant operational improvements.

Second, it changes the frequency of security tests required because, instead of defenses being based on reacting to attacks and vulnerabilities, they are part of change control instead. Therefore when new operations are initiated, the environment will be re-assessed for new or different points of interaction. The need to test for new flaws is no longer necessary nor is the need to test for compatibility of security updates after fixing those flaws. Security updates, if desired, will instead become part of the change control process and can be tested on schedule. This will drastically reduce the time spent putting out fires so that new focus can be put on improving operations and building better infrastructure.

Third, it changes the often secretive and socially demanding way we use trust within organizations. It allows the performance and history of each individual to speak for itself. This adds accountability to each role and removes prejudices that can strangle an organization, either operationally or legally. Not to mention it is the most fair means of assuring each person has the responsibility over their own successes and failures.

The changes required by the typical organization to achieve these benefits are actually small. The changes required by the security industry to meet the new needs of the implementers of the Möbius Defense will be huge. And change will bring new opportunities.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

**This methodology is free precisely because we prefer to be free as well.**

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

# Chapter 15 – Open Methodology License

## The OML 3

This license is provided under the Creative Commons 3.0 Attribution, 2010 by ISECOM.

**PREAMBLE**

This license is intended 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 are 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 developers to include this Open Methodology License (OML) to anything which is not modifiable 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 (i.e. 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 or OML 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 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 attribution for 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 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, internal, or non-commercial use including software, checklists, or tools, or within a class or training for educational purposes without explicit consent from the creator providing points 3 and 4 are complied with.


Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

6. No persons may distribute an adaption, modification, or change of this Methodology nor commercially sell a product, tool, checklist, or software which applies this Methodology without explicit consent from the creator.

7. All persons may utilize the Methodology or any portion of it to create or enhance 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 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 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 or other parties provide the methodology "as is" without a 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 of 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.

Creative Commons 3.0 Attribution-Non-Commercial-NoDerivs 2010, ISECOM, www.isecom.org, www.osstmm.org
Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

# NO WORRIES!

## OSSTMMTRAINING.ORG

KNOWING HOW TO APPLY THE OSSTMM TAKES YOUR WORRIES AWAY.
OSSTMM TRAINING MAKES YOU A BETTER, MORE EFFICIENT SECURITY TESTER
AND ANALYST WHICH MAKES WHAT YOU NEED TO SECURE BE MORE SECURE.

OSSTMM OPSA Professional Security Analyst

OSSTMM OPST Professional Security Tester

OSSTMM OPSE Professional Security Expert

OSSTMM OWSE Wireless Security Expert

OSSTMM CTA Certified Trust Analyst

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

# OSSTMM 3

***Why test operations? Unfortunately, not everything works as configured. Not everyone behaves as trained. Therefore the truth of configuration and training is in the resulting operations. That's why we need to test operations.***

The Open Source Security Testing Methodology Manual strives to be the ultimate security guide. Better known to security experts and hackers alike as the OSSTMM, spoken like "awesome" but with a "t", is a formal methodology for breaking any security and attacking anything the most thorough way possible.

Released for free for the first time in 2001 as the underdog to the security industry's product-focused security advice, the manual achieved an instant following. Being open to anyone for peer review and further research led to it growing from its initial 12 page release to its current size of over 200 pages. For testing security operations and devising tactics it has no equal.

The OSSTMM is in its third version and is a complete re-write of the original methodology. It now includes the ever-elusive security and trust metrics at its foundation. It required 7 years of research and development to produce the perfect operational security metric, an algorithm which computes the Attack Surface of anything. In essence, it is a numerical scale to show how unprotected and exposed something currently is. Security professionals, military tacticians, and security researchers know that without knowing how exposed a target is, it's just not possible to say how likely a threat will cause damage and how much. But to know this requires a thorough security test which happens to be exactly what the OSSTMM provides.

To say the OSSTMM 3 is a very thorough methodology is an understatement. It covers proper attack procedures, error handling, rules of engagement, proper analysis, critical security thinking, and trust metrics. It provides 17 modules like Visibility Audit, Trust Verification, Property Validation, and Competitive Intelligence Scouting, each which describes multiple attacks (called Tasks), for 5 different interaction types with a target (called Channels) organized by technical knowledge and equipment requirements as Human, Physical, Telecommunications, Data Networks, and Wireless. The OSSTMM has indeed become a complex organism but with a new focus on readability and usability, it is far from complicated to use.

**Security doesn't have to last forever; just longer than everything else that might notice it's gone.**

Official OSSTMM Certifications: www.opsa.org, www.opst.org, www.opse.org, www.owse.org, www.trustanalyst.org

Copyright 2010, ISECOM, www.isecom.org, www.osstmm.org

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES