



INSTITUTE FOR SECURITY AND OPEN  
METHODOLOGIES

# **OSSTMM WIRELESS 2.9.1**

**Wireless Security Testing Section  
Open-Source Security Testing Methodology Manual**

**Created by Pete Herzog**

<b>CURRENT VERSION:</b>	OSSTMM Wireless 2.9.1
<b>NOTES:</b>	This is the first of a series of OSSTMM Section separations to provide focus to various types of security tests and promote higher quality peer-review.  <b>All updated material until 3.0 will only be released only to subscribers.</b>
<b>CHANGES:</b>	Fixed mistake in EMF Testing module.
<b>DATE OF CURRENT VERSION:</b>	Wednesday, October 30, 2003
<b>DATE OF ORIGINAL VERSION:</b>	Monday, December 18, 2000

## OSSTMM Contributors

Those who have contributed to this manual in consistent, valuable ways have been listed here although many more people should receive our thanks. Each person here receives recognition for the type of contribution although not as to what was contributed. The use of contribution obscurity in this document is for the prevention of biases and to promote fresh ideas. If you are interested in contributing, please see the ISECOM website for more information.

<b>CREATED BY:</b>	Pete Herzog	Managing Director of ISECOM - pete<at>isecom.org
<b>KEY CONTRIBUTORS:</b>	Marta Barceló Robert E. Lee Rick Tucker Nigel Hedges Colby Clark Tom O'Connor Andrea Barisani Gary Axten Marco Ivaldi Raoul Chiesa	<i>Assistant Director of ISECOM</i> - marta<at>isecom.org <i>co-Chairman of the Board of ISECOM</i> - robert<at>isecom.org <i>Board Advisor of ISECOM</i> - rick<at>isecom.org nigel.hedges<at>ca.com colby<at>isecom.org tom91<at>elivfree.net lcars<at>infis.univ.trieste.it gary.axten<at>lineone.net raptor<at>mediaservice.net raoul<at>mediaservice.net
<b>KEY ASSISTANCE:</b>	Dru Lavigne Felix Schallock Anton Chuvakin Efrain Torres Lluís Vera Rogelio M. Azorín Richard Feist Rob J. Meijer John Pascuzzi Miguel Angel de Cara L Chris N Shepherd Darren Young Clemens Wittinger Nabil Ouchn Sean Cocat Leonardo Loro Carles Alcolea Claudia Kottmann	<i>Manager of the OPRP of ISECOM</i> - dru<at>isecom.org felix.schallock<at>e-security-net.de anton<at>chuvakin.org et<at>cyberspace.org lvera<at>isecb.com rma<at>isecb.com rfeist<at>nyxtec.net rmeijer<at>xs4all.nl johnpas<at>hushmail.com miguelangel.decara<at>dvc.es chris.shepherd<at>icctcorp.com darren<at>younghome.com cwr<at>atsec.com ghosted<at>ccc.ma scocat<at>remingtonltd.com leoloro<at>microsoft.com calcolea<at>menta.net claudia.kottmann<at>gmx.net
<b>KEY SUPPORTERS:</b>	Jaume Abella Travis Schack Andre Maxwell John Regney Peter Klee Martin Pivetta Daniel Fdez. Bleda Clément Dupuis Waidat Chan Josep Ruano Bou Tyler Shields Javier Fdez. Sanguino Vicente Aguilera John Rittinghouse Kris Buytaert Xavier Caballé Brennan Hay	jaumea<at>salleurl.edu travis<at>vitalisec.com amaxwel3<at>bellsouth.net sregney<at>gedas.es klee<at>de.ibm.com martin.pivetta<at>itatwork.com dfernandez<at>isecauditors.com cdupuis<at>cccure.org waidat<at>interrorem.com jruano<at>capside.com tcroc<at>cow.pasture.com jfernandez<at>germinus.com vaguilera<at>isecauditors.com jwr<at>rittinghouse.homeip.net buytaert<at>stone-it.be xavi<at>caballe.com hayb<at>ncr.disa.mil

**Key Contributors:** This designation is for those individuals who have contributed a significant portion of their time and energy into creating a better OSSTMM. This required complete section rewrites, module enhancements, and rules of engagement development.

**Key Assistance:** This designation is for those individuals who have contributed significantly to the ideas, design, and development of the OSSTMM. This required section rewrites, module contributions, and significant editing.

**Key Supporters:** This designation is for those individuals who have made significant efforts towards promoting and explaining the OSSTMM in the name of ISECOM. This required article and press writings, improvements to the OSSTMM, and regular knowledge support.

## Foreword

In previous versions of the OSSTMM a primary focus was on *what* we do as security testers. Due to the success of those releases and the OSSTMM's growing approval amongst the IT security community, I have had the continued pleasure to expand upon the OSSTMM. To help deliver this methodology, I created the OSSTMM Professional Security Tester (OPST) and Analyst (OPSA) certifications. I've had the pleasure to teach these now on a number of occasions, and it has been during some of these classes that I have observed a growing requirement to define *why* we do security testing.

When dealing with security and risk management, many think of these in terms of odds and predictability. They ask: What are the odds that an incident, threat or attack will occur? Just how predictable is it that this event will occur? While it is true that some defenses are proactive enough to address unknown and unpredictable attacks, most organizations depend on defenses that are strengthened by a database of known attacks. A penetration tester knows that to counteract these he/she must also have a database of known up-to-date attacks. This aids in the swiftness and effectiveness of each attempt. Time and time again, a certain set of "ethical hacks" will prove successful, so the tester will savor these jewels from his/her database of attacks, and log the success ratios. Armed with this information the penetration tester will attempt to exploit a customer's network until one of the attacks succeeds. This technique is well and good, however in practice the client's organization becomes a casino and the penetration testers are playing against the client's predetermined odds. This is much like the gambler is at the mercy of the odds set by the casino. For those unfamiliar with casinos and forms of gambling, it is important to understand that established games of chance like those found at a casino, can never have a 50/50 win to lose ratio because the casino will not make money. Therefore, casinos will choose to offer games which will offer a higher lose than win ratio to assure money is made over a set period of time which is known as "setting the odds". Players who learn to "cheat" at casino games use techniques to upset the win to lose ratio in the other direction. This is never more true than when a player knows how to play a game better than the casino (which is extremely rare but happens) in which case the casino would consider this cheating even if it relied on memory abilities like counting cards (blackjack), skills like calculating an extremely large number of variables to place bets accordingly (sports betting and animal racing), or something simple like pattern recognition (roulette). Penetration testers who gain privileged access through higher skills and better knowledge than the client has is also sometimes seen as "cheating" although they are actually changing the rules of the game by exploiting security defenses which have been minimized for business justification and usability. Changing the rules of the game is very different than playing by the rules and setting your own odds in the test. Often times the client is aware of these risks which are necessary for business. You can't open a store without inviting people to shop.

Methodical security testing is different from penetration testing. It relies on a combination of creativeness, expansive knowledge bases of best practices, legal issues, and the client's industry regulations as well as known threats, and the breadth of the target organization's security presence (or points of risk) to "cheat" at the casino, thus making our own odds. We do this by exploiting predictability and best practices to the most thorough extent possible. In other words, we test all extremes of everything considered predictable and fully utilize best practices to test against the worst-case scenarios that may not be as predictable. For organizations truly committed to reduce as much risk as possible, it almost goes without saying that it is our duty as security testers to explore the breadth, depth of risk, and to properly identify this during the testing of the target.

The types of questions we must continually ask ourselves in the testing process are: Which assets can I access at what time to force the maximum security risk? Under what circumstances do I find the most weaknesses? When am I most likely to put *confidentiality*, *integrity* and *availability* to the test? By remaining methodical and persistent, the accumulative effect of these tests will paint an accurate picture for us of the risks, weaknesses, information leaks, and vulnerabilities. This will assist us greatly with any business justifications for safeguards, as well as satisfying any regulative/legislative requirements through due care and diligence.

The following points will aid you well as you set out to create and deliver your high standard security tests:

- **When to test is as important as *what* and *why* to test.**

Waiting to make the test, waiting to report the problems, and waiting to address problems are all mistakes. As you left your house to go on vacation, did you wait until you returned to test if you actually locked the doors? Of course not. You locked the door and rattled the knob to make sure it was locked. Waiting until you return to test would also require going through the house to see what's missing, and you don't need reminding that an audit takes much longer than a security test.

- **Do sweat the small stuff, because it's all small stuff.**

Testing is in the details and often it is the smallest details that lead to the biggest security breaches. In addition, it is the accumulation of the small stuff, which individually may not represent much risk although when aggregated, may also lead to a security breach.

- **Do make more with less.**

As budgets for security defense remain small, the security tester needs to operate with efficiency and creativity to do more in less time. If inefficient security testing becomes too costly it is tempting for an organization to see security testing as an extraneous cost. This is unfortunate because the risks associated from not conducting security testing still remains unknown. Therefore, as we balance thoroughness with efficiency in our security tests, the results will time and time again speak for themselves - many more organizations will view security testing as a cost justified weapon in their defensive posture.

- **Don't underestimate the importance of the Security Policy *in any form*.**

This policy is the company's official declaration of what they want to accomplish. Very few people ever arrive somewhere without first intending to get there. A security policy is all about that intention, and the organization's goal of security within it. The security policy for an organization is often very complex with multiple persons tasked to develop and maintain it. Mistakes due to policy in one section will often form a negative flow-on effect that will impact other sections. It only takes a few termites in a wall to lead to infestation of the whole house. For example, if a policy is not in place to specify controls that check people who leave with boxes or equipment, then information leakage may occur. Security Policy specifies many more controls that have a direct effect on standards and procedures, such as what egression rules exist on the screening router, or what e-mails one may forward out from inside the company.

- **What they get is all about *how you give it*.**

Despite all attempts at thoroughness and efficiency, one of the largest factors about determining the success of a security posture is still based on economics. This is all handled far away from the tester's toolbox. It requires a certain level of project management skills, perceptiveness about your client, and good communication skills. Has enough time for the test been budgeted? Will there be enough in the budget for fixing discovered vulnerabilities? What types of risk will senior management accept or feel is unworthy of budgeting? The end result of the security test will be some form of deliverable to your client or client's management – and all these economic factors should have been worked out before hand. After all, what's the difference between a good and a bad security test if the report is ignored?

## Table of Contents

OSSTMM Contributors .....	3
Foreword .....	5
Introduction .....	8
Scope .....	9
Intended Audience .....	9
Accreditation .....	9
End Result .....	10
Analysis .....	10
Internet and Network Related Terms .....	10
Compliance .....	14
Legislation .....	14
Best Practices .....	16
Rules Of Engagement .....	17
Process .....	19
The Security Map .....	20
Security Map Module List .....	21
Risk Assessment .....	22
Risk Evaluation .....	22
“Perfect” Security .....	23
Risk Assessment Values .....	25
Risk Types .....	25
Sections and Modules .....	27
Test Modules and Tasks .....	28
Module Example .....	28
Methodology .....	29
Section E – Wireless Security .....	30
Risk Assessment Values .....	31
Modules .....	32
1. EMR (Electromagnetic Radiation) Testing .....	32
2. 802.11 Wireless Networks Testing .....	33
3. Bluetooth Network Testing .....	37
4. Wireless Input Device Testing .....	40
5. Wireless Handheld Security Testing .....	41
6. Cordless Communications Testing .....	42
7. Wireless Surveillance Device Testing .....	43
8. Wireless Transaction Device Testing .....	44
9. RFID Testing .....	45
10. Infrared Systems Testing .....	47
Open Methodology License (OML) .....	49

## Introduction

This manual is a combination of ambition, study, and years of experience. The individual tests themselves are not particularly revolutionary, but the methodology as a whole does represent the benchmark for the security testing profession. And through the thoroughness of its application you will find a revolutionary approach to testing security.

This manual is a professional standard for security testing in any environment from the outside to the inside. As a professional standard, it includes the rules of engagement, the ethics for the professional tester, the legalities of security testing, and a comprehensive set of the tests themselves. As security testing continues to evolve into being a valid, respected profession, the OSSTMM intends to be the professional's handbook.

The objective of this manual is to create one accepted method for performing a thorough security test. Details such as the credentials of the security tester, the size of the security firm, financing, or vendor backing will impact the scale and complexity of our test – but any network or security expert who meets the outline requirements in this manual will have completed a successful security profile. You will find no recommendation to follow the methodology like a flowchart. It is a series of steps that must be visited and revisited (often) during the making of a thorough test. The methodology chart provided is the optimal way of addressing this with pairs of testers however any number of testers are able to follow the methodology in tandem. What is most important in this methodology is that the various tests are assessed and performed where applicable until the expected results are met within a given time frame. Only then will the tester have addressed the test according to the OSSTMM model. Only then will the report be at the very least called thorough.

Some security testers believe that a security test is simply a “point in time” view of a defensive posture and present the output from their tests as a “security snapshot”. They call it a snapshot because at that time the known vulnerabilities, the known weaknesses, and the known configurations have not changed. Is this snapshot enough? The methodology proposed in this manual will provide more than a snapshot. Risk Assessment Values (RAVs) will enhance these snapshots with the dimensions of frequency and a timing context to the security tests. The snapshot then becomes a profile, encompassing a range of variables over a period of time before degrading below an acceptable risk level. In the 2.5 revision of the OSSTMM we have evolved the definition and application of RAVs to more accurately quantify this risk level. The RAVs provide specific tests with specific time periods that become cyclic in nature and minimize the amount of risk one takes in any defensive posture.

Some may ask: “Is it worth having a standard methodology for testing security?” Well, the quality of output and results of a security test is hard to gauge without one. Many variables affect the outcome of a test, including the personal style and bias of a tester. Precisely because of all these variables, it is important to define the right way to test based on best practices and a worldwide consensus. If you can reduce the amount of bias in testing, you will reduce many false assumptions and you will avoid mediocre results. You'll have the correct balanced judgment of risk, value, and the business justification of the target being tested. By limiting and guiding our biases, it makes good security testers great and provides novices with the proper methodology to conduct the right tests in the right areas.

The end result is that as security testers we participate and form a larger plan. We're using and contributing to an open-source and standardized methodology that everyone can access. Everyone can open, dissect, add to, suggest and contribute to the OSSTMM, where all constructive criticism will continue to develop and evolve the methodology. It just might be the most valuable contribution anyone can make to professional security testing.

We welcome your feedback.

Pete Herzog  
Managing Director, ISECOM

## Scope

This is a document of security testing methodology; it is a set of rules and guidelines for which, what, and when events are tested. This methodology only covers external security testing, which is testing security from an unprivileged environment to a privileged environment or location, to circumvent security components, processes, and alarms to gain privileged access. It is also within the scope of this document to provide a standardized approach to a thorough security test of each section of the security presence (e.g. physical security, wireless security, communications security, information security, Internet technology security, and process security) of an organization. Within this open, peer-reviewed approach for a thorough security test we achieve an international standard for security testing to use as a baseline for all security testing methodologies known and unknown.

The limitation to the scope of external security testing is due to the substantial differences between external to internal and internal to internal testing. These differences are fundamentally in the access privileges, goals and deliverables associated with internal to internal testing.

The testing towards the discovery of unknown vulnerabilities is not within the scope of this document nor is it within the scope of an OSSTMM security test. The security test described herein is a practical and efficient test of known vulnerabilities, information leaks, and deviations from law, industry standards, and best practices.

ISECOM requires that a security test may only be considered an OSSTMM test if it is:

- Quantifiable.
- Consistent and repeatable.
- Valid beyond the "now" time frame.
- Based on the merit of the tester and analyst not on brands.
- Thorough.
- Compliant to individual and local laws and the human right to privacy.

ISECOM does not claim that using the OSSTMM constitutes a legal protection in any court of law however it does serve as the highest level of appropriate diligence when the results are applied to improve security in a reasonable time frame.

## Intended Audience

This manual is written for security testing professionals. Terms, skills, and processes mentioned in here may not be clear to those not directly involved and experienced with security testing.

Designers, architects, and developers will find this manual useful to build better defense and testing tools. Many of the tests do not have a way to be automated. Many of the automated tests do not follow a methodology or follow one in an optimal order. This manual will address these issues.

## Accreditation

A security test data sheet is required to be signed by the tester(s) and accompany all final reports to submit an OSSTMM certified test. This data sheet *available with OSSTMM 2.5*. This data sheet will show which modules and tasks had been tested to completion, not tested to completion and why, and not applicable and why. The checklist must be signed and provided with the final test report to the client. A data sheet which indicates that only specific Modules of an OSSTMM Section has been tested due to time constraints, project problems, or customer refusal can NOT be said then to be a full OSSTMM test of the determined Section.

**Reasons for the data sheet are:**

- Serves as proof of thorough, OSSTMM testing.
- Makes a tester(s) responsible for the test.
- Makes a clear statement to the client.
- Provides a convenient overview.
- Provides a clear checklist for the tester.

The use of this manual in the conducting of security testing is determined by the reporting of each task and its results even where not applicable in the final report. All final reports which include this information and the proper, associate checklists are said to have been conducted in the most thorough and complete manner and may include the following statement and a stamp in the report:



*This test has been performed in accordance to the **Open Source Security Testing Methodology** available at <http://www.osstmm.org/> and hereby stands within best practices of security testing.*

All stamps (color and b&w) are available at <http://www.isecom.org/stamps.htm>

## End Result

The ultimate goal is to set a standard in security testing methodology which when used results in meeting practical and operational security requirements. The indirect result is creating a discipline that can act as a central point in all security tests regardless of the size of the organization, technology, or defenses.

## Analysis

The scope of this document does not include direct analysis of the data collected when using this manual. This analysis is the result of understanding the appropriate laws, industry regulations, and business needs appropriate to the particular client and the best practices and regulations for security and privacy other the client's regions of operation. However, analysis of some form is implied by the use of "Expected Results" within the methodology so some analysis must be done to assure at least these expected results are met.

## Internet and Network Related Terms

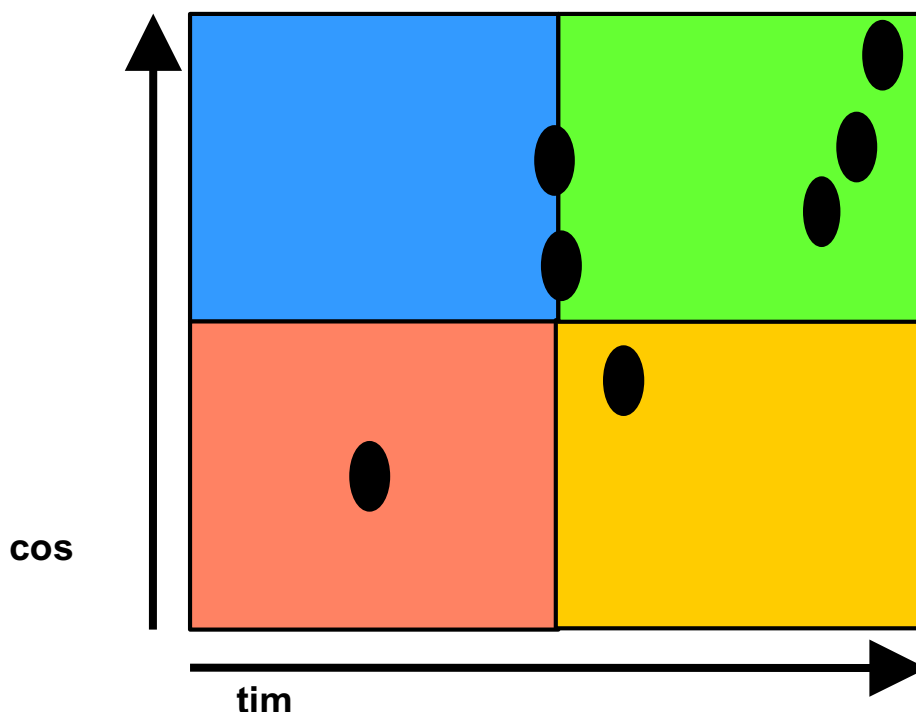
Throughout this manual we refer to words and terms that may be construed with other intents or meanings. This is especially true through international translations. For definitions not associated within this table below, see the reference of the [OUSPG Vulnerability Testing Terminology glossary](http://www.ee.oulu.fi/research/ouspg/sage/glossary/) available at <http://www.ee.oulu.fi/research/ouspg/sage/glossary/>.

<b>Application Test</b>	The security testing of any application whether or not it's part of the Internet presence.
<b>Assessment</b>	An overview of the security presence for the estimation of time and man hours.
<b>Automated Testing</b>	Any kind of unattended testing that also provides analysis
<b>Black Box</b>	The tester has no prior knowledge of the test elements or environment
<b>Black Hat</b>	A hacker who is chaotic, anarchistic and breaks the law
<b>Client</b>	This refers to a sales recipient with whom confidentiality is enforced through a signed non-disclosure agreement.
<b>Competitive Intelligence</b>	A practice legally for extracting business information from competitors.

<b>Containment Measures</b>	A process for quarantine and validation
<b>Customer</b>	This refers to a sales recipient with whom confidentiality is only ethically implied as no non-disclosure agreement or contract has been signed by either party.
<b>Environment</b>	The interactive, co-dependent state of the network in operation. Also known as the setting
<b>Estimate</b>	A document of the time and man hours required for a test and may include price
<b>Ethical Hacking</b>	A form of penetration testing originally used as a marketing ploy but has come to mean a pen test of all systems – where there is more than one goal, generally, everything is a goal
<b>Expected Results</b>	The findings from a specific module
<b>Firewall</b>	The software or hardware tool for imposing an Access Control List (ACL) on a system or network
<b>Goal</b>	The end result to be achieved. May sometimes be a trophy which is a finding on the network that has potential, financial worth like a database of credit card numbers
<b>Gray Box</b>	The tester has some prior knowledge of the test elements or environment
<b>Gray Hat</b>	A hacker who is chaotic and anarchistic but does not break the law, however the actions often lack integrity or ethics
<b>Hacker</b>	A clever person who has a natural curiosity, likes to know how things work and is interested in circumvention techniques or exploiting processes to see what happens
<b>Intrusion Detection System (IDS)</b>	Either passive or active, host-based or network based, this tool is designed to monitor and sometimes stop attacks in action
<b>Liability</b>	The financial assurance of diligence and responsibility.
<b>Location</b>	The physical location.
<b>Man Hours</b>	This stands for the work one person does in one hour. Two man hours can be the work two people can do in one hour OR the work one person can do in two hours
<b>Manual Testing</b>	A test which requires a person to input data throughout the testing process and monitor the outcome to provide analysis
<b>Man Weeks</b>	This is the amount of work one person can do in one work week of 40 hours
<b>Modules</b>	These are viewpoints based in business security for individual OSSTMM sections
<b>Network Scope</b>	This refers to what a tester may legally test
<b>Non Disclosure Agreement</b>	A legal contract to stop the spread of information beyond the need to know basis of those sharing the NDA
<b>PBX</b>	Stands for Phone Exchange and is the central server in an organization for handling phone lines
<b>Penetration Test</b>	A security test with a defined goal which ends when the goal is achieved or time runs out
<b>Plan</b>	A calendar of tasks to be systematically completed in a test
<b>Posture Assessment</b>	The U.S. Military term for a security test
<b>Practical</b>	Defines security which is usable and applies to business justification
<b>Privileges Testing</b>	Tests where credentials are supplied to the user and permission is granted for testing with those credentials
<b>Privileges</b>	Credentials and permission
<b>RAV</b>	Risk Assessment Values. This is the de facto risk assessment tool of the OSSTMM which relies on cycles and degradation factors in the modules
<b>Remote Access</b>	This is defined as access from outside the location
<b>Risk Assessment</b>	In the OSSTMM this is used to describe security degradation as a comparison marker which can quantify a level of security over time
<b>Router</b>	A software or hardware device for routing packets
<b>Scope</b>	A description of what is permitted in a security test
<b>Scouting</b>	Document grinding for new or unique business information and trends
<b>Sections</b>	In the OSSTMM, these are used to define general security viewpoints. The

	OSSTMM uses 6 viewpoints; IT, Information, Wireless, Communications, Physical and Process
<b>Security Audit</b>	A hands-on, privileged security inspection of the OS and Applications of a system. In the U.S.A. and Canada “Auditor” is an official term and official job only to be used by a licensed practitioner. However, in other countries, “security audit” is a common term for a penetration or security test.
<b>Security Presence</b>	How security is applied to all six security sections of an organization
<b>Security Scope</b>	Another term for scope
<b>Security Test</b>	A test for the security presence. May be specified by section
<b>Social Engineering</b>	An active attack against processes
<b>Tasks</b>	Specific security tests in a module to achieve one or more of the defined Expected Results
<b>Time</b>	Physical time - the fourth dimension - 24 hours a day
<b>Usability</b>	A step to making security understandable and efficient so as not to be intentionally bypassed for any legitimate reason
<b>Verification Test</b>	A follow-up security test after all the fixes have been fixed
<b>Visibility</b>	Components of the security presence which can be remotely discerned
<b>Vulnerability Test</b>	A test for services, open ports and known vulnerabilities
<b>White Box</b>	The tester has full prior knowledge of the test elements or environment
<b>White Hat</b>	A hacker who does not break the law and acts in an ethical manner

For clarity, ISECOM applies the following terms to types of system and network security testing as based on time and cost for Internet Security Testing:



1. Vulnerability Scanning refers generally to automated checks for known vulnerabilities against a system or systems in a network.
2. Security Scanning refers generally to vulnerability scans which include manual false positive verification, network weakness identification, and customized, professional analysis.
3. Penetration Testing refers generally to a goal-oriented project of which the goal is the trophy and includes gaining privileged access by pre-conditional means.
4. Risk Assessment refers generally to security analysis through interview and mid-level research which includes business justification, legal justifications, and industry specific justifications.
5. Security Auditing refers generally to a hands-on, privileged security inspection of the OS and Applications of a system or systems within a network or networks.
6. Ethical Hacking refers generally to a penetration test of which the goal is to discover trophies throughout the network within the predetermined project time limit.
7. Security Testing and it's military equivalent, the Posture Assessment, is a project-oriented risk assessment of systems and networks through the application of professional analysis on a security scan where penetration is often used to confirm false positives and false negatives as project time allows.

## Compliance

This manual was developed to satisfy the testing and risk assessment for personal data protection and information security in the following bodies of legislation. The tests performed provide the necessary information to analyze for data privacy concerns as per most governmental legislations and organizational best practices due to this manual's thorough testing stance. Although not all country statutes can be detailed herein, this manual has explored the various bodies of law to meet the requirements of strong examples of individual rights and privacy.

## Legislation

The tests in this manual have included in design the remote auditing and testing from the outside to the inside of the following:

### Austria

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

### United States of America

- U.S. Gramm-Leach-Bliley Act (GLBA)
- Clinger-Cohen Act
- Government Performance and Results Act
- Government Paperwork Elimination Act
- FTC Act, 15 U.S.C. 45(a), Section 5(a)
- Children's Online Privacy Protection Act (COPPA)
- ICANN Uniform Dispute Resolution Policy (UDRP)
- 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)
- 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]

### 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

### Spain

- Spanish LOPD Ley orgánica de regulación del tratamiento automatizado de los datos de carácter personal Art.15 LOPD - . Art. 5,
- LSSICE

### **Canada**

- Corporate Governance
- Provincial Law of Quebec, Canada Act Respecting the Protection of Personal Information in the Private Sector (1993).

### **United Kingdom**

- UK Data Protection Act 1998
- Corporate Governance

### **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 that 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.

## Best Practices

The tests in this manual have included in design the remote auditing and testing from the outside to the inside of the following:

### IT Information Library

Information available at <http://www.ogc.gov.uk/index.asp?id=2261> issued by the British Office for Government Commerce (OGC)

### Germany: IT Baseline Protection Manual (IT Grundschutzhandbuch)

Issued by Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security (BSI)) available at <http://www.bsi.de/gshb/english/menue.htm>

### German IT Systems

S6.68 (Testing the effectiveness of the management system for the handling of security incidents) and tests S6.67 (Use of detection measures for security incidents)

### 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 testing.

### GAO and FISCAM

This manual is in compliance to the control activities found in the US General Accounting Office's (GAO) Federal Information System Control Audit Manual (FISCAM) where they apply to network security.

### SET

This document incorporates the remote auditing test from the SET Secure Electronic Transaction(TM) Compliance Testing Policies and Procedures, Version 4.1, February 22, 2000

### NIST

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

- An Introduction to Computer Security: The NIST Handbook, 800-12
- Guidelines on Firewalls and Firewall Policy, 800-41
- Information Technology Security Training Requirements: A Role- and Performance-Based Model, 800-16
- DRAFT Guideline on Network Security Testing, 800-42
- 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

### MITRE

This manual is CVE compatible for Risk Assessment Values

## Rules Of Engagement

Those who are partners with ISECOM or publicly claim to use the OSSTMM for security testing must uphold the following rules of engagement. These rules define the ethical guidelines of acceptable practices in marketing and selling testing, performing testing work, and handling the results of testing engagements. Failure to comply with these rules may result in the inability to use the ISECOM seal on test results and the termination of the ISECOM partnership agreement.

### 1. Sales and Marketing

1. The use of fear, uncertainty and doubt 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 crime, facts, criminal or hacker profiling, and statistics.
2. The offering of free services for failure to penetrate or provide trophies from 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. Performing security tests against any network without explicit written permission from the appropriate authority is strictly forbidden.
5. The use of names of past clients who you have provided security testing for is forbidden even upon consent of said client. This is as much for the protection of the client's confidentiality as it is for the security testing organization.
6. It is required to provide truthful security advice even when the advice may be to advise giving the contract to another company. An example of this would be in explaining to a company that your security testers should not be verifying a security implementation your organization designed and installed rather it should be tested by an independent 3<sup>rd</sup> party.

### 2. Assessment / Estimate Delivery

1. Verifying possible vulnerable services without explicit written permission is forbidden.
2. The security testing of obviously highly insecure and unstable systems, locations, and processes is forbidden until the security has been put in place.

### 3. Contracts and Negotiations

1. With or without a Non-Disclosure Agreement contract, the security tester is ethically bound to confidentiality, non-disclosure of customer information, and security testing results.
2. The tester must always assume a limited amount of liability as per responsibility. Acceptable limited liability is equal to the cost of service. This includes both malicious and non-malicious errors and project mismanagement.
3. Contracts must clearly explain the limits and dangers of the security test.
4. In the case of remote testing, the contract must include the origin of the testers by telephone numbers and/or IP addresses.
5. Contracts must contain emergency contact persons and phone numbers.
6. The contract must include clear, specific permissions for tests involving survivability failures, denial of service, process testing, or social engineering.
7. Contracts must contain the process for future contract and statement of work (SOW) changes.

### 4. Scope

1. The scope must be clearly defined contractually before verifying vulnerable services.
2. The scope must clearly explain the limits of the security test.

### 5. Providing Test Plan

1. The test plan must include both calendar time and man hours.
2. The test plan must include hours of testing.

## 6. Providing the rules of engagement to the client.

1. No unusual or major network changes allowed by the client during testing.
2. To prevent temporary raises in security only for the duration of the test, the client should notify only 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, and security operations.
3. If necessary for privileged testing, the client must provide two, separate, access tokens whether they be logins and passwords, certificates, secure ID numbers, etc. and they should be typical to the users of the privileges being tested (no especially empty or secure accounts).
4. When performing a privileged test, the tester must first test without privileges in a black box environment and then test again with privileges.

## 7. Testing

1. The testers 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.
2. The exploitation of Denial of Service tests may only be done with explicit permission. An OSSTMM security test does not require one to exploit denial of service and survivability endangering type vulnerabilities in a test. The tester is expected to use gathered evidence only to provide a proper review of such security processes and systems.
3. Social engineering and process testing may only be performed in non-identifying statistical means against untrained or non-security personnel.
4. Social engineering and process testing may only be performed on personnel identified in the scope and may not include customers, partners, associates, or other external entities.
5. High risk vulnerabilities such as discovered breaches, vulnerabilities with known, high exploitation rates, vulnerabilities which are exploitable for full, unmonitored or untraceable access, or which may put immediate lives at risk, discovered during testing must be reported to the customer with a practical solution as soon as they are found.
6. Distributed Denial of Service testing over the Internet is forbidden.
7. Any form of flood testing where a person, network, system, or service, is overwhelmed from a larger and stronger source is forbidden.
8. Client notifications are required whenever the tester changes the testing plan, changes the source test venue, has high risk findings, previous to running new, high risk or high traffic tests, and if any testing problems have occurred. Additionally, the client should be notified with progress updates weekly.

## 8. Reporting

1. Reports must include practical solutions towards discovered security problems.
2. Reports must include all unknowns clearly marked as unknowns.
3. Reports must state clearly all states of security found and not only failed security measures.
4. Reports must use only qualitative metrics for gauging risks based on industry accepted methods. These metrics must be based on a mathematical formula and not on feelings of the analyst.

## 9. Report Delivery

1. The client must be notified when the report is being sent as to expect its arrival and to confirm receipt of delivery.
2. All communication channels for delivery of report must be end to end confidential.

## Process

The process of a security test concentrates on evaluating the following areas which in turn reflect upon the security presence which is the defined environment for security testing. These we refer to as the Security Dimensions:

### Visibility

Visibility is what can be seen, logged, or monitored in the security presence both with and without the aid of electronic devices. This includes, but is not limited to, radio waves, light beyond the visible spectrum, communication devices such as telephones, GSM, and e-mail, and network packets such as TCP/IP.

### Access

Access is an entry point into the security presence. An access point need not be physical barrier. This can include, but is not limited to, a web page, a window, a network connection, radio waves, or anything in which a location supports the definition of quasi-public or where a computer interacts with another computer within a network. Limiting access means denying all except what is expressly permitted financially and in best practices.

### Trust

Trust is a specialized pathway in regards to the security presence. Trust includes the kind and amount of authentication, non-repudiation, access control, accountability, confidentiality, and integrity between two or more factors within the security presence.

### Authentication

Authentication is the measure for which every interaction in the process is privileged.

### Non-repudiation

Limited or non-repudiation provides assurance that no person or system responsible for the interaction can deny involvement in the interaction.

### Confidentiality

Confidentiality is the assurance that only the intended systems or parties of specific communication in a process may have access to the privileged information contained in the process.

### Privacy

Privacy is that the process itself is known only between intended systems or parties.

### Authorization

Authorization is the assurance that the process has a reason or business justification and is managed by a responsible party providing privilege to systems or parties.

### Integrity

Integrity is the assurance that the process has finality and cannot be changed, continued, redirected, or reversed without it being known to the systems or parties involved.

### Safety

Safety is the means of which a process cannot harm other systems, parties or other processes even through complete failure.

### Alarm

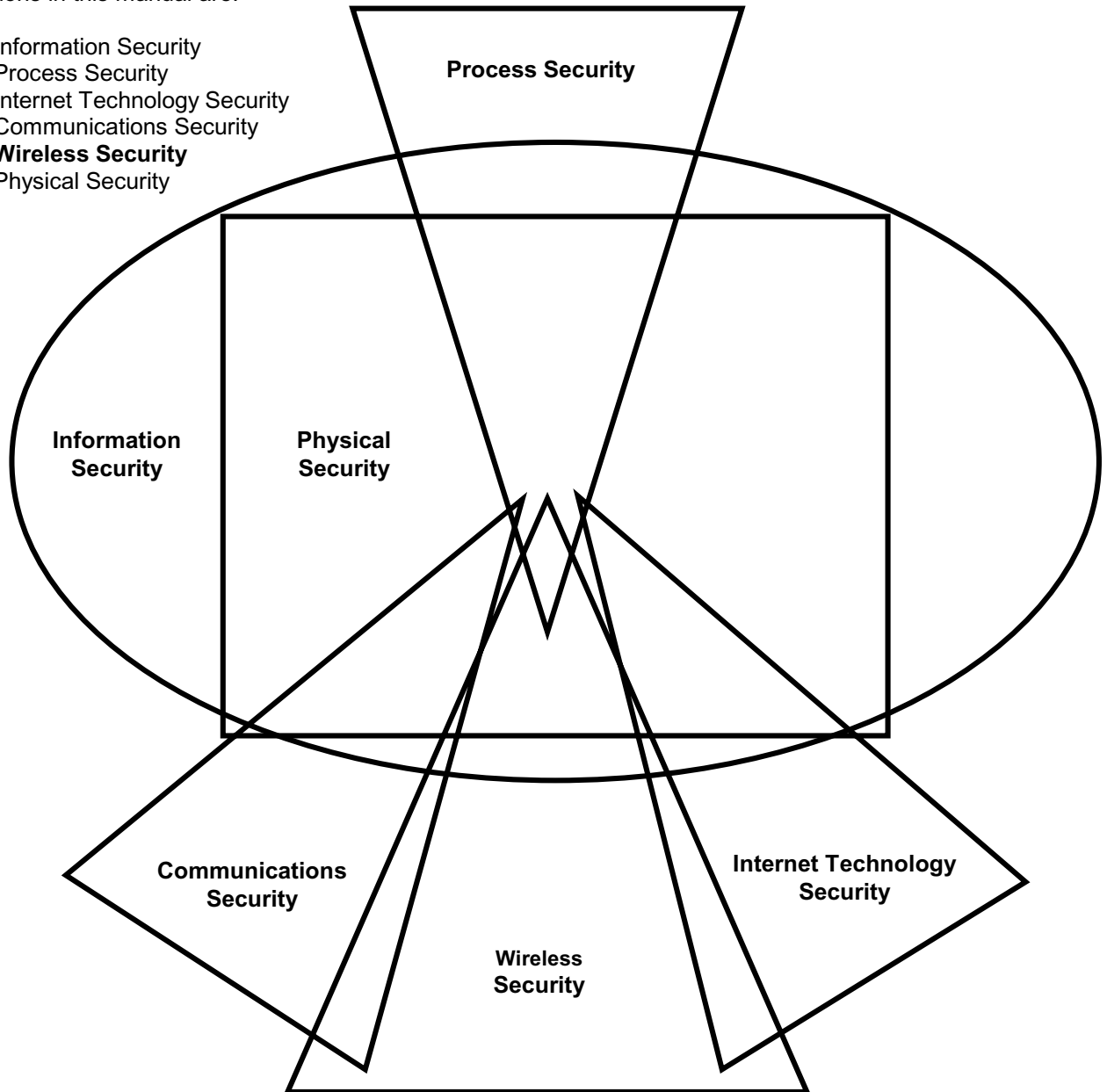
Alarm is the timely and appropriate notification of activities that violate or attempt to violate any of the other security dimensions. In most security breaches, alarm is often the single process which initiates further consequences.

## The Security Map

The security map is a visual display of the security presence. The security presence is the environment of a security test and is comprised of six sections which are the sections of this manual. The sections each overlap and contain elements of all other sections. Proper testing of any one section must include the elements of all other sections, direct or indirect.

The sections in this manual are:

1. Information Security
2. Process Security
3. Internet Technology Security
4. Communications Security
5. **Wireless Security**
6. Physical Security



## Security Map Module List

The module list of the security map are the primary elements of each section. Each module must further include all of the Security Dimensions which are integrated into tasks to be completed. To be said to perform an OSSTMM security test of a particular section, all the modules of that section must be tested and of that which the infrastructure does not exist for said Module and cannot be verified, will be determined as NOT APPLICABLE in the OSSTMM Data Sheet inclusive with the final report.

### **5. Wireless Security Testing**

1. Posture Review
2. Electromagnetic Radiation (EMR) Testing
3. 802.11 Wireless Networks Testing
4. Bluetooth Networks Testing
5. Wireless Input Device Testing
6. Wireless Handheld Testing
7. Cordless Communications Testing
8. Wireless Surveillance Device Testing
9. Wireless Transaction Device Testing
10. RFID Testing
11. Infrared Testing
12. Privacy Review

## Risk Assessment

Risk assessment is maintained by both the tester and the analyst for all data gathered to support a valid assessment through non-privileged testing. This implies that if too little or improper data has been gathered then it may not be possible to provide a valid risk assessment and the tester should therefore rely on best practices, the client's industry regulations, the client's business justifications, the client's security policy, and the legal issues for the client and the client's regions for doing business.

## Risk Evaluation

Risk means that limits in the security presence will have a detrimental effect on people, culture information, processes, business, image, intellectual property, legal rights, or intellectual capital. This manual maintains four dimensions in testing for a minimal risk state environment:

### 1. Safety

All tests must exercise concern for worst case scenarios at the greatest expenses. This requires the tester to hold above all else the regard for human safety in physical and emotional health and occupation.

### 2. Privacy

All tests must exercise regard for the right to personal privacy regardless of the regional law. The ethics and understanding for privacy are often more advanced than current legislation.

### 3. Practicality

All tests must be engineered for the most minimal complexity, maximum viability, and deepest clarity.

### 4. Usability

All tests must stay within the frame of usable security. That which is most secure is the least welcoming and forgiving. The tests within this manual are performed to seek a usable level of security (also known as practical security).

## “Perfect” Security

In risk assessment, the OSSTMM applies the technique of “Perfect Security”. In Perfect Security, the tester and analyst gauge the client as to what would be perfect security. This is countered with the Posture Review, which is best practices, the client’s industry regulations, the client’s business justifications, the client’s security policy, and the legal issues for the client and the client’s regions for doing business. The result is Perfect Security for that client. The tester and analyst then provide a gap analysis between the current state of security with Perfect Security.

Simple best practices as defined as a theoretical towards Perfect Security:

### Wireless

- Usability of security features should be a strength.
- Quarantine and verify all wireless devices before accepting.
- Assure business justifications for all wireless devices.
- Maintain established limits of wireless signal strength and distance.
- Limit trusts (to systems and users).
- Encrypt all traffic.
- Allow only accessibility with accountability.
- Layer the security.
- Treat wireless devices as separate networks from established ones.
- Trigger it to alarm on failed or duplicate account access.
- Monitor and log accessibility from all non-voice communication traffic.
- Disallow and limit unauthorized bridging from wireless to wired.
- Decentralize nodes.

### Internet Gateway and Services

- No unencrypted remote access.
- No unauthenticated remote access.
- Restrictions deny all and allow specifically.
- Monitor it all and log it.
- Decentralize.
- Limit Inter-system trust.
- Quarantine all inputs and validate them.
- Install only the applications / daemons necessary.
- Layer the security.
- Invisible is best- show nothing except the service itself.
- Simplicity prevents configuration errors.

### Mobile Computing

- Quarantine all incoming network and Internet traffic.
- No unencrypted remote access.
- No unauthenticated remote access.
- Encrypt accordingly.
- Install only the applications / daemons necessary.
- Invisible is best- no running services.
- BIOS passwords required.

- Security training for best practices and recognizing security issues is required for users and helpdesks.

### **Applications**

- Usability of security features should be a strength.
- Assure business justifications for all inputs and outputs in the application.
- Quarantine and validate all inputs.
- Limit trusts (to systems and users).
- Encrypt data.
- Hash the components.
- All actions occur on the server side.
- Layer the security.
- Invisible is best- show only the service itself.
- Trigger it to alarm.

### **People**

- Decentralized authority.
- Personal responsibility.
- Personal security and privacy controls.
- Accessible only through gateway personnel.
- Trained in defined legalities and ethics from security policies.
- Limited, need-to-know access to information and infrastructure.

## Risk Assessment Values

Integrated with each module are Risk Assessment Values (RAVs) which are defined as the degradation of security (or escalation of risk) over a specific life cycle based on best practices for periodic testing. The association of risk levels with cycles has proven to be an effective procedure for security metrics.

The concepts of security metrics in this manual are to:

- Establish a standard time cycle for testing and retesting to
- Maintain a measurable level of risk based on
- The degradation of security (escalation of risk) which occurs naturally, with time and
- The ability to measure risk with consistency and detail
- Both before and after testing.

Unlike conventional risk management, the RAVs operate purely on the application of security within an organization. They take into consideration the controls such as the processes, politics, and procedures by operating in parallel with the testing methodology. While the testing methodology does examine these controls sometimes in an indirect nature, the actual controls do not interest the tester rather it is the application of these controls that determine the results of a security test. A well written policy which is not followed will have no effect on actual security.

RAVs are determined mathematically by the following factors:

1. The degrees of degradation of each separate module from point of optimum health measured from a theoretical maximum of 100% for risk management purposes,
2. The cycle which determines the maximum length of time it takes for the degradation to degrade its full percentage value (degradation) based on security best practices and consensus,
3. The influence of other modules performed or not performed,
4. Weights established by the Security Dimensions,
5. The type of risk as designated by the OSSTMM Risk Types and whether the risk has been:
  - a. *Identified* but not investigated or investigation provided varied and unclear results,
  - b. *Verified* as in clearly positive or exploitable, or,
  - c. *Not applicable* in that it does not exist because the infrastructure or that security mechanism does not exist.

## Risk Types

Whereas the risk types appear to be subjective, the classification of risks to the following types is in actuality mostly objective when following the framework of the OSSTMM. Future versions will assure this is CVE compatible.

### Vulnerability

A flaw inherent in the security mechanism itself or which can be reached through security safeguards that allows for privileged access to the location, people, business processes, and people or remote access to business processes, people, infrastructure, and/or corruption or deletion of data.

A vulnerability may be a metal in a gate which becomes brittle below 0° C, a thumbprint reader which will grant access with rubber fingers, an infrared device that has no authentication mechanism to make configuration changes, or a translation error in a web server which allows for the identification of a bank account holder through an account number.

### Weakness

A flaw inherent in the platform or environment of which a security mechanism resides in, a misconfiguration, survivability fault, usability fault, or failure to meet the requirements of the Security Posture.

A weakness may be a process which does not save transaction data for the legal time limit as established by regional laws, a door alarm which does not sound if the door is left open for a given amount of time, a firewall which returns ICMP host unreachable messages for internal network systems, a database server that allows unfiltered queries, or an unlocked, unmonitored entrance into a otherwise secured building.

### **Information Leak**

A flaw inherent in the security mechanism itself or which can be reached through security safeguards which allow for privileged access to privileged or sensitive information concerning data, business processes, people, or infrastructure.

An information leak may be a lock with the combination available through audible signs of change within the lock's mechanisms, a router providing SNMP information about the target network, a spreadsheet of executive salaries for a private company, the private mobile telephone number of the marketing staff, or a website with the next review date of an organization's elevators.

### **Concern**

A security issue which may result from not following best practices however does not yet currently exist as a danger.

A concern may be FINGERD running on a server for an organization that has no business need for the FINGER service, a guarded doorway which requires the watchman to leave the door to apprehend a trespasser with no new guard to replace the one who left and maintain a presence at the door, or employees who sit with their monitors and whiteboards viewable from outside the perimeter security.

### **Unknowns**

An unidentifiable or unknown element in the security mechanism itself or which can be reached through security safeguards that currently has no known impact on security as it tends to make no sense or serve any purpose with the limited information the tester has.

An unknown may be an unexpected response possibly from a router in a network that is repeatable and may indicate network problems, an unnatural radio frequency emanating from an area within the secure perimeter however offers no identification or information, or a spreadsheet which contains private data about a competing company.

The following table provides the values for the Risk Assessment Values.

	<b>Verified</b>	<b>Identified</b>	<b>Not Applicable</b>
<b>Vulnerability</b>	3.2	1.6	0.4
<b>Weakness</b>	1.6	0.8	0.3
<b>Concern</b>	0.8	0.4	0.2
<b>Information Leak</b>	0.4	0.2	0.1
<b>Unknown</b>	0.2	0.1	--

## Sections and Modules

The methodology is broken down into *sections*, *modules* and *tasks*. The sections are specific points in the security map that overlap with each other and begin to dissect a whole that is much less than the sum of its parts. The modules are the flow of the methodology from one security presence point to the other. 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. Output may or may not be analyzed data (also known as intelligence) to serve as an input for another module. It may even be the case that the same output serves as the input for more than one module or section.

Some tasks yield no output; this means that modules will exist for which there is no input. Modules which have no input can be ignored during testing. Ignored modules do not necessarily indicate an inferior test; rather they may indicate superior security.

Modules that have no output as the result can mean one of three things:

- The tasks were not properly performed.
- The tasks were not applicable.
- The tasks revealed superior security.
- The task result data has been improperly analyzed.

It is vital that impartiality exists in performing the tasks of each module. Searching for something you have no intention of finding may lead to you finding exactly what you want. In this methodology, each module begins as an input and output exactly for the reason of keeping bias low. Each module gives a direction of what should be revealed to move further down the flow.

Time is relative. Larger test environments mean more time spent at each section, module and task. The amount of time allowed before returning with output data depends on the tester, the test environment, and the scope of the testing. Proper testing is a balance of time and energy where time is money and energy is the limit of man and machine power.

Identifying tasks that can be seen as “less than vital” and thereby “safely” trimmed from testing is vital when defining test modules for a target system, where project scope or restraints require. These omitted tasks however should be clearly documented and agreed prior to testing.

With the provision of testing as a service, it is highly important to identify to the commissioning party exactly what *has not or will not* be tested, thereby managing expectations and potentially inappropriate faith in the security of a system.

# Test Modules and Tasks

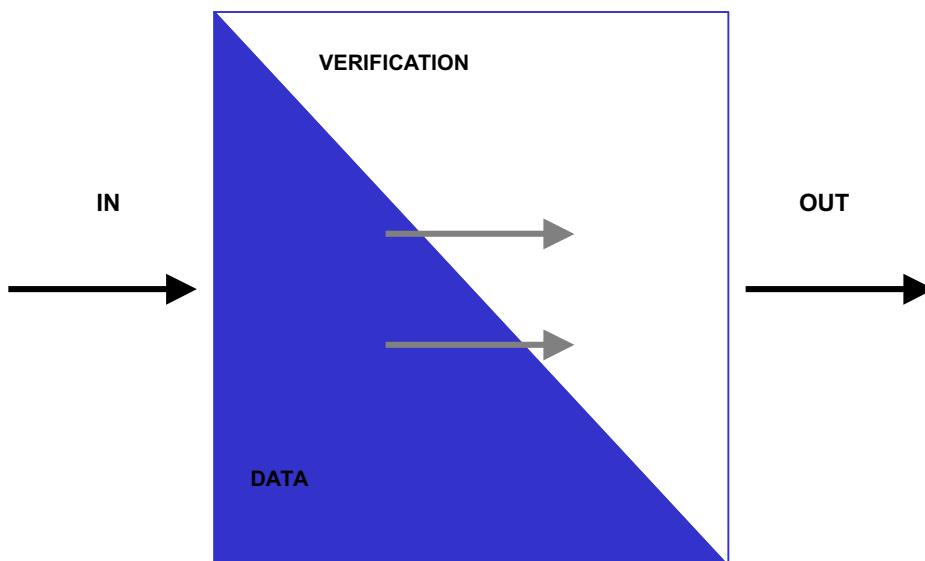
## Module Example

Module Name Description of the module.
<b>Expected Results:</b> Item Idea Concept Map
Group task description. Task 1 Task 2

## Methodology

The methodology flows from the initial module to the completion of the final module. The methodology allows for a separation between data collection and verification testing of and on that collected data. The flow may also determine the precise points of when to extract and when to insert this data.

In defining the methodology of testing, it is important to not constrict the creativity of the tester by introducing standards so formal and unrelenting that the quality of the test suffers. Additionally, it is important to leave tasks open to some interpretation where exact definition will cause the methodology to suffer when new technology is introduced.

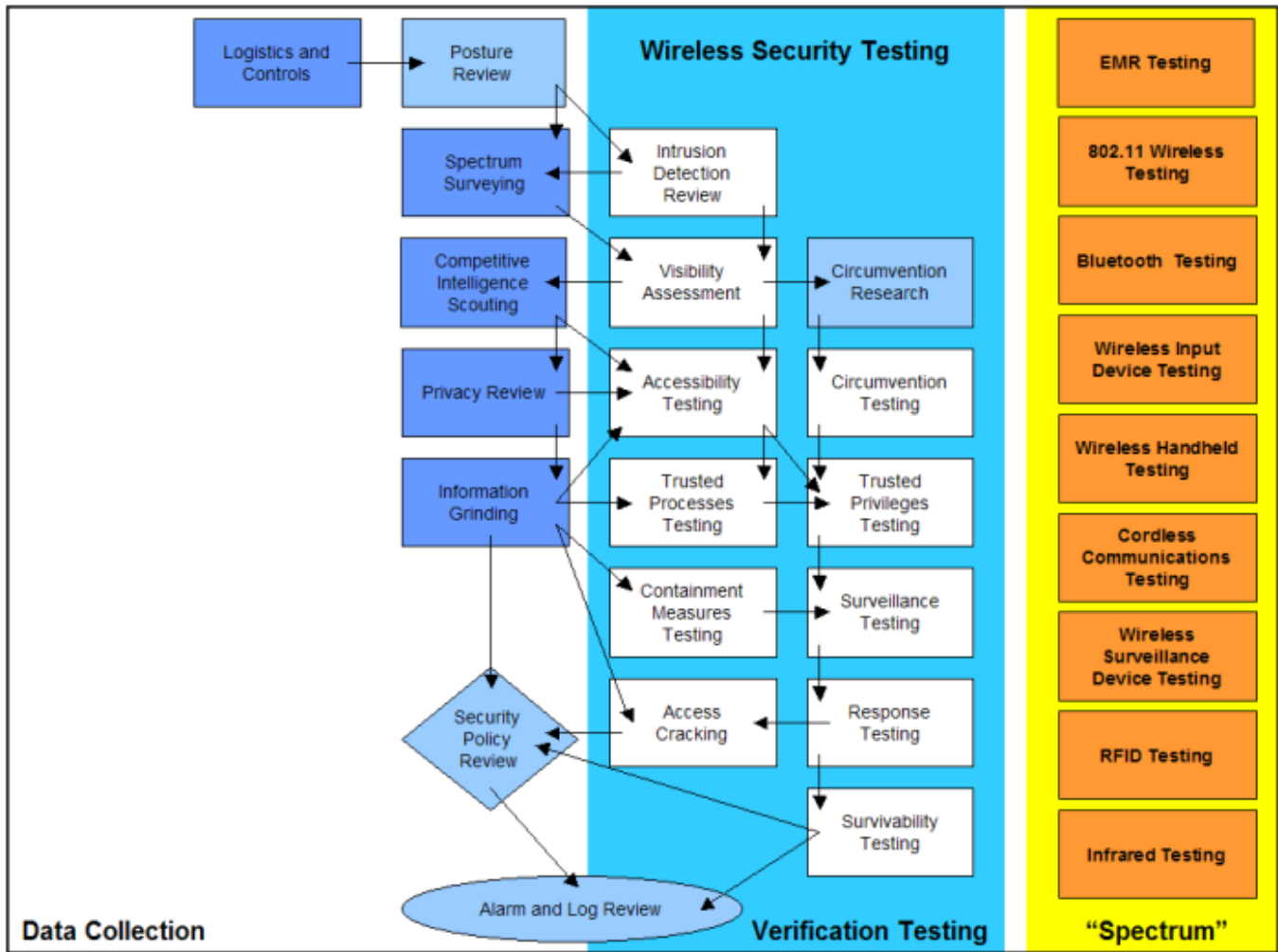


Each module has a relationship to the one before it and the one after it. Each section has inter-relational aspects to other modules and some inter-relate with all the other sections. Overall, security testing begins with an input that is ultimately the addresses of the systems to be tested. Security testing ends with the beginning of the analysis phase and the construction of the final report. This methodology does not affect the form, size, style, or content of the final report nor does it specify how the data is to be analyzed. That is left to the security tester or organization.

Sections are the whole security model divided into manageable, testable slices. Modules are the test variables in sections. The module requires an input to perform the tasks of the module and the modules of other sections. Tasks are the security tests to perform depending upon the input for the module. The results of the tasks may be immediately analyzed to act as a processed result or left raw. Either way, they are considered the output of the module. This output is often the input for a following module or in certain cases such as newly discovered hosts, may be the input for a previous module.

The whole security model can be broken up into manageable sections for testing. Each section can in turn be viewed as a collection of test modules, with each module being broken up into sets of tasks.

## Section E – Wireless Security



## Risk Assessment Values

Module	Cycle (days)	Degradation (%)	Influence (x)
Logistics and Controls	0	0	1.6
Posture Review	178	12	
Spectrum Surveying	25	2.3	
Intrusion Detection Review	25	2.3	
Competitive Intelligence Scouting	17	7.3	
Privacy Review	96	2.9	
Information Grinding	96	8.7	
Visibility Assessment	67	5.8	
Accessibility Testing	67	5.8	
Circumvention Research	2	3.6	
Circumvention Testing	3	3.6	
Trusted Processes Testing	42	4.1	
Trusted Privileges Testing	42	4.1	
Containment Measures Testing	96	3.9	
Surveillance Testing	178	9	
Access Cracking	96	3.9	
Response Testing	178	9	
Survivability Testing	25	2.3	
Security Policy Review	4	5.4	
Alarm and Log Review	124	6.7	
Spectrum	Cycle (days)	Degradation (%)	Influence (x)
EMR Testing			
802.11 Wireless Networks Testing			
Bluetooth Networks Testing			
Input Device Testing			
Handheld Testing			
Communications Testing			
Surveillance Device Testing			
Transaction Device Testing			
RFID Testing			
Infrared Testing			

## Modules

### 1. EMR (Electromagnetic Radiation) Testing

This is a method of testing Emissions Security (Emsec), and it pertains to remotely testing the electromagnetic radiation that is emitted from Information Technology devices. Electromagnetic radiation can be captured from devices, such as CRTs, LCDs, printers, modems, cell phones, and so on and used to recreate the data that is displayed on the screen, printed, transmitted... Exploiting this vulnerability is known as Van Eck phreaking.

Equipment for testing or exploiting this vulnerability can prohibitively expensive. However, there are some low cost solutions that incorporate a television receiver, a VCR tuner, synchronization equipment, and other parts. The main cost associated with this form of testing is the time involved. It can require a qualified person to sit for hours trying to find the EMR from the right source. Therefore, this form of testing is usually reserved for highly secure installations where protecting intellectual property is absolutely vital. Additionally, being as it is a given that this data can be obtained from any device that is known to emit EMR, it is best to test for this in implementations that are specifically designed to protect against it.

Protecting against this type of intrusion is usually done by purchasing "Tempest" rated equipment and placing the machines and all peripherals within a shielded room of some sort, such as a Faraday Cage and using only fiber, filtered, or coiled connections to all internal devices between each other and from the outside. Therefore, such protection can be cost prohibitive.

For low budget protection against this type of intrusion, PGP Security has a "Tempest" surveillance prevention option in its secure viewer (used when viewing encrypted text files). This is basically a low-contrast window in which text is viewed. It would probably obfuscate the text if viewed from a van. Also, white noise can be generated to make it much more difficult for intruders to get clean data.

\*Note – It is a common myth that CRTs are the biggest culprit in leaking information through EMR. This is not true. They do emit a significant amount of EMR, but it is not as powerful, nor as easily readable as that emitted by modems and printers. Moreover, to obtain usable data from CRTs, a highly trained individual would have to filter, reassemble, and organize the data. To obtain usable data from a modem or printer, you simply have to intercept it.

<b>Expected Results</b>	Level of electromagnetic radiation that is leaking from a secure room or site Distance EMR is readable from Type of data that is obtainable Ease of obtaining and reading EMR
-------------------------	--

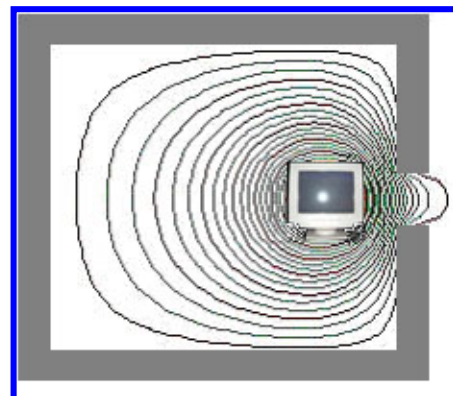
#### Evaluate Business Needs, Practices, Policies and Locations of Sensitive Areas

1. Verify that the organization has an adequate security policy in place to address EMR.
2. Verify that all personnel involved with sensitive areas are trained in methods of reducing EMR leakage and are familiar with the security policy.
3. Determine the level of acceptable EMR leakage based on institutional needs.
4. Determine individual Information Technology sites that must be isolated.
5. Verify that physical, perimeter security is in place to ensure that that access to sensitive areas is not easily obtainable by unauthorized parties.

#### Evaluate Hardware and Placement

6. Verify that all Information Technology devices that must be protected are located in a suitable Faraday Cage or metal-shielded room.

7. Verify that the hardware in place in the room is designed to emit low amounts of EMR and is compliant to the TEMPEST standard.
8. Verify strategic placement of items in the room to create the greatest protection against EMR emission.
9. Verify that the level of shielding is adequate to protect against emitted EMR.
10. Verify that the room is completely encased by proper shielding. Pay special attention to the door, floor, and ceiling.
11. Verify that the door to the room is kept closed at all times. Two shielded doors that cannot be open simultaneously are best to mitigate EMR leakage. A diagram for a suitable shielded room and what effect it has on EMR is shown below, note the need for containment at the entrance.
12. Verify that all peripheral devices (printers, modems...) that will be used by the protected computers are contained within the shielded room.



### Evaluate and Test Wiring and Emissions

13. Verify that all wiring feeds into and out of the shielded room are made of fiber, where possible.
14. Verify that all wiring feeds, especially those that are not made of fiber, are shielded and filtered (capacitors, coils...) in such a way to eliminate EMR from being carried within them out of the protected room.
15. Test for EMR leakage from outside of the protected room on all sides and at different distances.
16. Test all wiring coming from the protected room for EMR leakage.
17. Verify the distance that any leakage is detectable from.
18. Test all wiring that goes into and out of the building where the protected room is contained, to verify that there is no leakage.
19. Verify that there is no leakage in public access areas or areas of lesser security.
20. Determine the need for white noise generation to mask EMR emissions.

## 2. 802.11 Wireless Networks Testing

This is a method for testing access to 802.11 WLANs, which are becoming increasingly popular. However, some fairly alarming security problems are common when implementing these technologies. This is mainly because these networks are very quickly and easily thrown together, but security measures are not part of the default setup. There are some basic things that can be done to improve security and some more drastic measures that can be taken to make WLANs fairly secure.

### 802.11 Specifications:

<b>Physical Layer</b>	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), infrared (IR)
<b>Default encryption</b>	RC4-based stream encryption algorithm for confidentiality, authentication, and integrity. Limited Key management.
<b>Operating Range</b>	About 150 feet indoors and 1500 feet outdoors.

### Implementations:

#### 802.11a

- Operates in the 5GHz frequency range
- Not compatible with 802.11b or 802.11g hardware
- Maximum speed of 54Mbps

#### 802.11b

- Operates in the 2.4GHz frequency range
- Currently the most widely deployed standard
- Maximum speed of 11Mbps

#### 802.11g

- Operates in the 2.4 GHz frequency range
- Maximum speed of 54Mbps standard
- Expected to be backward compatible with the 802.11b hardware

<b>Expected Results</b>	Verify security policy and practices of the organization and users Identify the outer-most physical edge of the wireless network Identify the logical boundaries of the wireless network Enumerate access points into the network Identify IP-range (and possibly DHCP-server) of the wireless network Identify encryption methods used for data transfer Identify authentication methods of exploitable "mobile units" (clients) and users. Verify configuration of all devices Determine flaws in hardware or software that facilitate attacks
-------------------------	--

#### **Evaluate Business Needs, Practices, and Policies:**

1. Verify that the organization has an adequate security policy that addresses the use of wireless technology, including the use of 802.11.
2. Verify that all users are trained in the proper use and the dangers of wireless networking technology.
3. Perform a security risk assessment to determine the value of the assets in the organization that are exposed to the WLAN or that are exposed to devices that are ever exposed to the WLAN.
4. Verify that there are ongoing, random security audits to monitor and track devices.
5. Verify that a plan is in place to deal with the theft of wireless devices and that network passwords and keys are promptly changed.

#### **Evaluate Hardware, Firmware, and Updates.**

6. Perform a complete inventory of all wireless devices on the network.
7. Determine whether the wireless routers, client access points, and client NICs support firmware upgrades so that security patches can be deployed as they become available.
8. Verify that all of the latest patches and upgrades are applied to all wireless devices.
9. Verify that wireless patches and upgrades are deployed on a regular basis.
10. Verify that there are no devices on the network that compromise security through limitations in hardware or software design.
11. Verify that all devices are part of the planned implementation and were properly configured and that there are no rogue devices on the network that could jeopardize security by being confederate or merely improperly configured.
12. Review access logs and verify that no rogue devices are gaining access to the wireless network.

#### **Evaluate Access Control, Perimeter Security, and Ability to Intercept or Interfere with Communication:**

13. Determine the level of physical access controls to access points and devices controlling them (keyed locks, card badge readers, cameras...).
14. Perform a site survey to measure and establish the access point coverage for the organization.
15. Verify that wireless network devices do not interfere with other electronic devices on similar frequencies, such as cordless phones, in or next to the area of intended use.

16. Verify that all access points on the wireless network are at least five channels apart from each other and from access points on neighboring wireless networks to avoid possible denial of service problems caused by interference.
17. Determine the types of physical access controls (keyed locks, card badge readers, photo ID...) that are in place to control access to secure portions of the organization, including areas to which the wireless network extends.
18. Determine the locations where wireless communication extends beyond the physical boundaries of the organization and the distance which it extends.
19. Determine from how far access can be gained to the WLAN using common high-gain antennas.
20. Determine security measures that are in place where wireless communication does exceed physical boundaries (cameras, motion detection...).
21. If the intention is to restrict WLAN access to locations within buildings and not external areas, verify that access points are placed in the interior areas of the building and not near the exterior walls and windows.
22. Probe devices for possible DoS problems. Verify that wireless routers, access points and gateways are not vulnerable to denial of service attacks on PPTP, HTTP, or other ports on the internal interface.
23. Determine what type of intrusion detection system (IDS) is in use on the WLAN and areas that are accessible from it.
24. Test effectiveness of IDS system.

#### **Evaluate Administrative Access to Wireless Devices:**

25. Determine if access points are turned off during portions of the day when they will not be in use.
26. Verify that the reset function of access points is being used only by authorized personnel and only when absolutely needed.
27. Verify that access points are restored to the latest security settings after the reset feature is used.
28. Verify that management interfaces for the access points have user authentication.
29. Verify that all access points have strong administrative passwords.
30. Verify that all administrative passwords are changed regularly and stored safely.
31. Verify that wireless routers, gateways, and access points do not store the administrative password in plaintext in the default Management Information Base (MIB).
32. If the wireless router or access point allows remote (WAN side) configuration, verify that it is disabled.
33. If possible, verify that all web-driven configuration of the router or access point is disabled.
34. If it is not possible to disable web-driven configuration, verify that the administrative login cannot be circumvented by entering the specific URLs of the configuration pages.
35. For maximum security, verify that configuration of access points and wireless routers can only be performed through serial port access.
36. Verify that management traffic for access points is on a dedicated, wired subnet.
37. Verify that there are adequately robust community strings used for SNMP management traffic on the access points.
38. Verify that SNMP settings on the access points have been configured for least privilege (read only). Disable SNMP if it is not used.
39. For most secure use of SNMP, verify that access point management traffic is protected by SNMPv3 or equivalent cryptography.
40. Verify that access points will not allow remote attackers to cause a denial of service via a SNMP request with (1) a community string other than "public" or (2) an unknown OID, which causes the WAP to deny subsequent SNMP requests.
41. Verify that wireless routers, access points, and gateways do not use default SNMP community strings.
42. Verify that access points will not accept arbitrary community strings with requested MIB modifications, which allow remote attackers to obtain sensitive information such as WEP keys, cause a denial of service, or gain access to the network.

#### **Evaluate Configuration, Authentication and Encryption of Wireless Networks:**

43. Verify that the access point's default Service Set Identifier (SSID) has been changed.
44. Verify that the "broadcast SSID" feature has been disabled so that the client SSID must match that of the access point.
45. Verify that the SSID character string is not easy to guess and does not reflect anything about the company (name, location, function, products...).
46. Verify that the wireless router, access point or gateway does not use the 'Network Name' or SSID as the default Wired Equivalent Privacy (WEP) encryption key. Since the SSID occurs in the clear during communications, a remote attacker could determine the WEP key and decrypt traffic.
47. Verify that the WEP key is not stored in plaintext in a registry key on the client with weak permissions, which allows local users to decrypt network traffic by reading the WEP key from the registry key.
48. Determine if the broadcast beacon of the access point has been turned off for maximum security.
49. Verify that all insecure and unnecessary management protocols on the access points have been disabled.
50. Verify that all default parameters have been changed for the access points.
51. Verify that all security features of the WLAN products have been enabled, including the cryptographic authentication and WEP privacy feature.
52. Verify that encryption key sizes are at least 128 bits or as large as possible.
53. Verify that default shared keys are periodically replaced by more secure unique keys.
54. Ensure that a properly configured firewall has been installed between the wired infrastructure and the wireless network.
55. If installation requires maximum security, verify that sensitive parts of the wired network are in no way accessible from the wireless network and that no devices on the wireless network are ever on the sensitive portions of the wired network. The reason for this is that client devices on the wireless network are likely to be the easiest to compromise, and if certain types of spyware or trojans are loaded onto the wireless clients and they are later plugged into sensitive areas of the wired networks, security measures have been circumvented and sensitive data could be compromised.
56. Verify that layer 2 switched are used instead of hubs for access point connectivity.
57. Verify that all technology involved in the WLAN has all of the latest upgrades and security patches.
58. Verify that users are authenticated with username and password to WLANs and what type of authentication is used (local, RADIUS, Kerberos...).
59. Verify that network authentication is not susceptible to playback of previous authentications to gain access to network resources.
60. For improved security in instances where it is supported, verify that IPSec is used instead of the default (WEP) as the security protocol.
61. For improved security in instances where it is supported, verify that an authentication protocol, like 802.1x, is used on top of WEP.
62. If installation requires maximum security, verify that a more secure encryption algorithm than the default RC4 algorithm is in use (such as 3DES or AES).
63. If installation requires maximum security, verify that user authentication to the WLANs is gained through most secure methods (biometrics, smart cards, two-factor authentication, PKI, RSA...).
64. Determine whether static IP addressing is being used on the WLAN; this is more secure than DHCP.
65. Verify that DHCP is disabled if it is not totally necessary.
66. Verify that access is granted only to client machines with registered MAC addresses.
67. Verify that all possible security features that are provided by the architecture are in use.

#### **Evaluate Wireless Clients:**

68. Verify that all wireless clients have antivirus software installed.
69. Verify that all wireless clients have a firewall installed.
70. Verify that all wireless clients are up to date on patches and are configured for maximum security. As with VPNs, it is often easiest to gain access to a secured network through a poorly configured client.
71. If installation requires maximum security, verify that all wireless clients must use a Virtual Private Network (VPN) to gain access to any resources, including the Internet, on the WLAN.
72. Verify that VPNs have strong encryption, at least 3DES or better.

- 73. Verify that clients can't be forced to fall-back to plaintext-mode.
- 74. Verify that ad-hoc mode has been disabled unless the environment is such that the risk is tolerable.

### 3. Bluetooth Network Testing

This is a method for testing Bluetooth ad-hoc networks (piconets), which are popular for small, low bandwidth intensive wireless personal area networks (PANs). As with other wireless methods, there are inherent vulnerabilities that pose significant security problems.

#### Bluetooth Specifications:

Physical Layer	Frequency Hopping Spread Spectrum (FHSS)
Frequency Band	2.4 – 2.45 GHz (ISM band)
Hop Frequency	1,600 hops per second
Raw Data Rate	1Mbps
Throughput	Up to 720 Kbps
Data and Network Security	<ul style="list-style-type: none"> <li>• Three modes of security (none, link-level, and service-level)</li> <li>• Two levels of device trust and three levels of service security.</li> <li>• Stream encryption algorithm for confidentiality and authentication.</li> <li>• PIN derived keys and limited key management.</li> </ul>
Operating Range	About 10 meters (30 feet); can be extended to 100 meters (328 feet).

<b>Expected Results</b>	Verify security policy and practices of the organization and users Identify the outer-most physical edge of the wireless network Identify the logical boundaries of the wireless network and all of the connection points to wired and other wireless networks Identify encryption methods used for data transfer Identify use of PIN codes and key exchanges Verify correct configuration of all devices Determine flaws in hardware or software that facilitate attacks
-------------------------	---

#### Evaluate Business Needs, Practices, and Policies:

1. Verify that there is an organizational security policy that addresses the use of wireless technology, including Bluetooth technology.
2. Verify that all users are trained in the proper use and the dangers of Bluetooth wireless technology.
3. Verify that the wireless network is fully understood. Being as piconets form scatternets and have possible connections to 802.11 networks and connections to both wired and wireless wide area networks, it is imperative to begin with a comprehensive understanding of overall connectivity. Also, it is possible for a single device to have connections to multiple wireless networks.
4. Verify that there are ongoing, random security audits to monitor and track devices.
5. Verify that handheld Bluetooth devices are protected from theft.
6. Verify that all Bluetooth devices are turned off during all hours of the day that they are not in operation.
7. Verify that users understand that it is critical to secure the Bluetooth “bonding” environment from eavesdroppers during the initialization process where key exchanges occur.
8. Verify that handheld Bluetooth devices are stored securely when left unattended.
9. Verify that all handheld Bluetooth devices are labeled with the name of the owner, the organization, and contact info.
10. Verify that all users know what to do if a Bluetooth device is stolen.
11. Verify that plug-in or add-on modules are securely stored when not in use.

12. Verify that any data that is backed up on storage modules is done so in encrypted form.
13. Verify that some type of loss minimization is performed (physical locks, cables...).
14. Verify that the organization has proper password management (aging, complexity criteria...) for all handheld devices.
15. Verify that the organization has a practice of keeping up to date with applicable security notifications and deploying updates and patches on Bluetooth devices and the workstations that they mirror to.
16. Verify that users synchronize their handheld devices regularly with their PCs to avoid loss of data if the device is lost, stolen, or runs low on batteries.

#### **Evaluate Hardware, Firmware, and Updates.**

17. Perform a complete inventory of all Bluetooth enabled wireless devices.
18. Verify that all devices are part of the planned implementation and were properly configured and that there are no rogue devices on the network that could jeopardize security by being confederate or merely improperly configured.
19. Review access logs to verify that there are no rogue devices gaining access to the network.
20. Verify that all of the latest patches and upgrades are applied to all Bluetooth enabled devices.
21. Verify that Bluetooth patches and upgrades are deployed on a regular basis.

#### **Test for Common Vulnerabilities (especially in the Red-M 1050AP):**

22. Perform brute force attack against Bluetooth access point to discern the strength of password. Verify that passwords contain numbers and special characters. Bluetooth Access Points use case insensitive passwords, which makes it easier for attackers to conduct a brute force guessing attack due to the smaller space of possible passwords.
23. Perform buffer overflow test against Bluetooth access point management web interface to determine if it allows remote attackers to cause a denial of service and possibly execute arbitrary code via a long administration password.
24. Determine the ability for attackers to perform a brute force attack against the TFTP server on Bluetooth access points. In most current Bluetooth access points, the TFTP server cannot be disabled, which makes it easier for remote attackers to crack the administration password via brute force methods.
25. Determine the ability for unintended users to connect to the web management server for Bluetooth access points. The web management server for many Bluetooth access points does not use session-based credentials to authenticate users, which allows attackers to connect to the server from the same IP address as a user who has already established a session.
26. Determine the extent to which Bluetooth access points publicize their names, IP addresses, and other information in UDP packets to a broadcast address. This action allows any system on the network to obtain potentially sensitive information about the access point device by monitoring UDP port 8887.
27. Determine the extent that Bluetooth access point PPP servers allow bonded users to cause a denial of service and possibly execute arbitrary code via a long user names.

#### **Evaluate Access Control, Perimeter Security, and Ability to Intercept or Interfere with Communication:**

28. Verify the actual perimeter of the Bluetooth network.
29. Verify that external boundary protection is in place around the perimeter of the building or buildings of the organization.
30. Determine any spots where the Bluetooth network extends beyond the physical boundaries of the organization.
31. Determine the distance that the Bluetooth network can be reached with a high-gain antenna.
32. Determine the types of physical access controls (keyed locks, card badge readers, photo ID...) that are in place to control access to secure portions of the organization, including areas to which the Bluetooth network extends.
33. Determine security measures that are in place where Bluetooth networks do exceed physical boundaries (cameras, motion detection...).
34. For optimal security, verify that intrusion detection sensors are deployed on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.

35. Probe devices for possible DoS problems.

**Evaluate Device Configuration (Authentication, Passwords, Encryption...):**

36. Verify that Bluetooth devices are set to the lowest possible power setting to maintain sufficient operation that will keep transmissions within the secure boundaries of the organization.
37. Verify that users have chosen PIN codes that are as long and random as possible.
38. Verify that no Bluetooth device is defaulting to the zero PIN.
39. Verify that all Bluetooth devices are configured to delete PINs after initialization. This ensures that a PIN entry is required every time and not stored in memory.
40. For optimal security, verify that alternative methods of PIN code exchanges are in use, such as Diffie Hellman Key Exchange or certificate-based key exchange methods at the application layer. Use of these key exchange processes simplifies generation and distribution of longer PIN codes.
41. Verify that combination keys are in use, rather than unit keys.
42. Verify that link encryption is in use for all Bluetooth connections.
43. For optimal security, verify that smart card technology is in use to provide key management.
44. Verify that antivirus software is installed and in use on intelligent Bluetooth-enabled hosts.
45. For optimal security, verify that user authentication, such as biometrics, smart cards, two-factor authentication, or PKI are in use.
46. Verify that device mutual authentication is used for all accesses. This helps prevent man-in-the-middle attacks.
47. Verify that encryption (mode 3) is in use for all broadcast transmissions.
48. Verify that encryption key sizes are configured to the maximum allowable length.
49. Verify that users cannot be forced to fall back to unencrypted mode.
50. Verify that a "minimum key size" is required for any key negotiation processes.
51. Verify that network authentication is not susceptible to playback of previous authentications to gain access to network resources.
52. Verify that portable devices with Bluetooth interfaces are configured with a PIN or password to prevent unauthorized access if lost or stolen.
53. For optimal security, verify that application-level encryption and authentication (on top of the Bluetooth stack) is in use. For example IPsec VPN technology can be used to ensure the greatest amount of protection for highly sensitive transactions.

## 4. Wireless Input Device Testing

This section deals with wireless input devices, such as mice and keyboards. These devices are becoming very popular, but present profound vulnerabilities and compromises in privacy and security.

<b>Expected Results</b>	Verify security policy and practices of the organization and users Identify the outer-most physical edge of the wireless input device range Determine range Identify encryption methods used for data transfer Determine flaws in hardware or software that facilitate attacks
-------------------------	--

### Evaluate Business Needs, Practices, and Policies:

1. Analyze organizational security policy that addresses the use of wireless technology, such as wireless input devices.
2. Verify that users are trained in the proper use and the dangers of wireless input devices.
3. Perform a security risk assessment to determine the value of the assets in the organization that are exposed to the wireless input devices or that are exposed to devices that are ever exposed to the wireless input devices.
4. Verify that the organization is performing ongoing, random security audits to monitor and track wireless input devices.

### Evaluate Hardware, Firmware, and Updates:

5. Perform a complete inventory of all wireless input devices on the network.
6. Determine whether the wireless input devices support firmware upgrades so that security patches can be deployed as they become available.
7. Verify that all of the latest patches and upgrades are applied to all wireless input devices.
8. Verify that wireless input device patches and upgrades are deployed on a regular basis.
9. Verify that there are no wireless input devices on the network that compromise security through limitations in hardware or software design.
10. Verify that all devices are part of the planned implementation and were properly configured and that there are no rogue devices on the network that could jeopardize security by being confederate or merely improperly configured.

### Evaluate Access Control, Perimeter Security, and Ability to Intercept or Interfere with Communication:

11. Perform a site survey to measure and establish the service range of the wireless input devices for the organization.
12. Verify that wireless input devices do not interfere with other wireless input devices or electronic devices on similar frequencies, such as cordless phones, in or next to the area of intended use.
13. Determine the locations where the wireless input device range extends beyond the physical boundaries of the organization and the distance which it extends.
14. Determine from how far communication from wireless input devices can be intercepted, changed, or monitored using common high-gain antennas.
15. Verify ability to capture and recreate data transferred from wireless input devices.
16. Verify that encryption is in use, where applicable.
17. Verify that wireless input devices do not have a long 'synch' delay, which could allow a remote attacker to hijack connections via a man-in-the-middle attack.
18. Probe devices for possible denial of service problems.

## 5. Wireless Handheld Security Testing

Due to the incredible variety and ubiquity of handheld wireless devices, it is nearly impossible to address each type. This section is intended to incorporate all wireless devices in aggregate. There are basic measures that should be taken and tested across all wireless devices. The following steps provide a method of testing for security on all devices.

The most significant aspect in testing these devices lies not in the actual configuration of the device, but in the education of the user. Most of these steps test user knowledge regarding the most secure use of the device.

<b>Expected Results</b>	Verify security policy and practices of the organization and users Identify the outer-most physical edge of the wireless input device range Identify range Identify encryption methods used for data transfer Verify correct configuration of devices Identify use of PIN codes and key exchanges
-------------------------	--

### Evaluate Business Needs, Practices, and Policies:

1. Verify that there is an organizational security policy that addresses the use of all handheld devices.
2. Verify that users are trained in the proper use and the dangers of wireless handheld devices.
3. Perform a risk assessment to understand the value of the assets in the organization that need protection.
4. Verify that there are ongoing, random security audits to monitor and track devices.
5. Verify that devices are stored securely when left unattended.
6. Verify that all handheld devices are labeled with the name of the owner, the organization, and contact info.
7. Verify that all users know what to do if a device is stolen.
8. Verify that plug-in or add-on modules are securely stored when not in use.
9. Verify that any data that is backed up on storage modules is done so in encrypted form.
10. Verify that some type of loss minimization is performed (physical locks, cables...).
11. Verify that the organization has proper password management (aging, complexity criteria...) for all handheld devices.
12. Verify that the organization has a practice of keeping up to date with applicable security notifications and deploying updates and patches on handheld devices and the workstations that they mirror to.
13. Verify that users synchronize their handheld devices regularly with their PCs to avoid loss of data if the device is lost, stolen, or runs low on batteries.

### Evaluate Hardware, Firmware, and Updates:

14. Perform a complete inventory of all wireless devices on the network.
15. Determine whether the wireless routers, client access points, and client NICs support firmware upgrades so that security patches can be deployed as they become available.
16. Verify that all of the latest patches and upgrades are applied to all wireless devices.
17. Verify that wireless patches and upgrades are deployed on a regular basis.
18. Verify that there are no devices on the network that compromise security through limitations in hardware or software design.
19. Verify that all devices are part of the planned implementation and were properly configured and that there are no rogue devices on the network that could jeopardize security by being confederate or merely improperly configured.
20. Review access logs and verify that no rogue devices are gaining access to the wireless network.

### Evaluate Access Control, Perimeter Security, and Ability to Intercept or Interfere with Communication:

21. Verify that there is external boundary protection around the perimeter of the buildings, or wireless networks.
22. Verify that there are physical access controls (card badge readers, keyed locks, photo ID access...) to areas containing wireless devices or control equipment.
23. Determine any spots where the wireless network extends beyond the physical boundaries of the organization.

24. Determine the distance that the wireless network can be reached with a high-gain antenna.
25. Determine the types of physical access controls (keyed locks, card badge readers, photo ID...) that are in place to control access to secure portions of the organization, including areas to which the wireless network extends.
26. Determine security measures that are in place where wireless networks do exceed physical boundaries (cameras, motion detection...).
27. For optimal security, verify that intrusion detection sensors are deployed on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.
28. Probe devices for possible DoS problems.

**Evaluate Device Configuration (Authentication, Passwords, Encryption...):**

29. Verify that the devices use robust encryption to protect sensitive files and applications.
30. Verify that users always exchange data in encrypted form and that they cannot be forced to fall back to unencrypted mode.
31. Verify that wireless handheld devices use the strongest authentication methods possible.
32. Verify that network authentication is not susceptible to playback of previous authentications to gain access to network resources.
33. Verify that each device has a power-on password to protect data if the device is lost or stolen.
34. Verify that any desktop mirroring software is password protected.
35. Verify that all devices have a timeout mechanism that automatically prompts the user for a password after a period of inactivity.
36. Verify that users have the ability to authenticate securely locally as well as remotely.
37. Verify that sensitive data is archived to the PC and not stored on handheld devices longer than necessary.
38. Verify that infrared ports are turned off during periods of inactivity.
39. Verify that antivirus software is installed on handheld devices, if available.
40. Verify that PDAs are provided with secure authorization hardware/firmware.

## 6. Cordless Communications Testing

This is a method of testing cordless communications communication devices which may exceed the physical and monitored boundaries of an organization. This includes testing for interference between similar or differing wireless communication types within the organization and with neighboring organizations.

<b>Expected Results</b>	Map physical edge of the cordless communications. Map logical boundaries of the cordless communications. List of communication types List of frequencies emanating from the target List of vulnerabilities in the cordless communication present
-------------------------	--

**Evaluate Business Needs, Practices, and Policies:**

1. Verify that the organization has an adequate security policy that addresses the use of cordless communication technology.
2. Verify that users are trained in the proper use and the dangers of cordless communication technology.
3. Perform a security risk assessment to determine the value of the assets in the organization that are exposed to the cordless communication technology.
4. Verify that there are ongoing, random security audits to monitor and track devices.
5. Determine if there is a plan in place to deal with the theft of cordless communication technology devices and if access methods, passwords, and encryption can be promptly changed.

**Evaluate Hardware, Firmware, and Configuration:**

6. Perform an inventory of all cordless communication devices.

7. Verify that all cordless communication devices are part of the planned implementation and that there are no rogue devices that might exceed the intended range of the cordless communication infrastructure.
8. Verify that all necessary hardware and firmware upgrades have been installed.
9. Verify authentication-method of the clients, if they exist.
10. Verify that encryption is used, configured, and type used.
11. Verify that clients can't be forced to fall-back to non-encrypted mode if encryption is intended.

**Evaluate Access Control, Perimeter Security, and Ability to Intercept or Interfere with Communication:**

12. Verify the distance in which the cordless communication extends beyond the physical boundaries of the organization.
13. Verify that there is not interference between cordless communication types within the organization and with neighboring organizations.
14. Verify that cordless communication devices do not interfere with other electronic devices on similar frequencies, such as wireless networks, in or next to the area of intended use.
15. Verify potential to eavesdrop on wireless communications.
16. Verify ability to terminate or disrupt wireless communications.
17. Determine ability to gain unauthorized access to wireless communication channels to place unauthorized calls.
18. Probe network for possible DoS problems.

## 7. Wireless Surveillance Device Testing

This section pertains to the wireless surveillance devices that have recently begun to replace wired surveillance devices – such as cameras, microphones, etc. These devices enable companies to install monitoring equipment in areas where it was previously not feasible and at a lower cost. This monitoring equipment is often completely hidden, either by its very small size or by being disguised in another object, like a fire alarm, picture, or clock. Being as most of this equipment is wireless, it is more susceptible to interference, jamming, monitoring, and playback than its wired counterpart. Also, the security tester may be the last line of defense to ensure that this equipment is installed and operated appropriately.

<b>Expected Results</b>	Identify appropriateness of the devices installation Map the effectiveness of its concealment (if intended) Map the ability to intercept, jam, interfere, or playback the data transmitted Map level of encryption of data sent Identify quality of data sent and received.
-------------------------	---

**Evaluate Business Needs, Practices, and Policies:**

1. Verify that there is a company policy that effectively addresses wireless surveillance equipment.
2. Verify that surveillance equipment is not installed in an inappropriate place, such as a bathroom.
3. Verify that technology is not in conflict with local laws.
4. Verify that security personnel are trained in the proper use and the dangers of wireless surveillance device.

**Evaluate Devices and Placement:**

5. Verify that the surveillance equipment is truly disguised or not visible, if that is the intent of the equipment.
6. Determine if encryption is used to protect transmitted data and what kind.
7. Verify that the quality of images, audio, or data sent and received meets business needs.
8. Verify that devices have adequate power and that batteries are changed regularly (if not AC powered).
9. Verify that these devices meet all other requirements of wired physical security devices, where applicable.

**Evaluate Access Control, Perimeter Security, and Ability to Intercept or Interfere with Communication:**

10. Verify the actual perimeter of the wireless surveillance device transmissions.
11. Verify that external boundary protection is in place around the perimeter of the wireless surveillance transmissions.
12. Determine any spots where the wireless surveillance transmissions extend beyond the physical boundaries of the organization.
13. Determine the distance that the wireless surveillance transmissions can be reached with a high-gain antenna.
14. Determine the types of physical access controls (keyed locks, card badge readers, photo ID...) that are in place to control access to secure portions of the organization, including areas to which the wireless surveillance extends.
15. Verify that access controls (keyed locks, card badge readers, photo ID...) are in place on wireless surveillance device control and receiver equipment.
16. Determine security measures that are in place where wireless surveillance transmissions do exceed physical boundaries (cameras, motion detection...).
17. Probe devices for possible DoS problems.
18. Determine the ability of unintended third parties to intercept that images, audio, or other data that is sent from the wireless devices.
19. Determine the ability of unintended third parties to recreate and use the transmitted data that has been intercepted.
20. Determine the ability to interfere with or jam the transmissions sent from wireless surveillance equipment.
21. Determine the distance that data can be intercepted, jammed using a high gain antenna.
22. Determine the perimeter controls that are around the areas that transmissions can be intercepted.
23. Determine the ability for images or data to be recorded and played back at higher output, thereby overpowering the true signal and causing the receiver to display the recorded signal.
24. Verify that wireless surveillance equipment does not interfere with other wireless devices, such as cordless phones, wireless Internet, RFIDs, etc.

## 8. Wireless Transaction Device Testing

This section covers the wireless transaction devices that are in place in many stores. This equipment is currently being used to provide uplinks for cash registers and other point of sale devices, throughout the retail industries. This technology has proven to be a tremendous benefit and business enabler to companies, but is sometimes installed without thought to security and protection of confidential information.

<b>Expected Results</b>	Map ability interception and use or manipulation of transaction data Identify level of encryption used to safeguard data Map the distance that data can be intercepted
-------------------------	--

**Evaluate Business Needs, Practices, and Policies:**

1. Verify that there is a company policy that effectively addresses wireless transaction equipment.
2. Verify that all firmware, patches, and software are updated on a regular basis.
3. Verify that safeguards meet all local, state, and federal laws governing electronic transmission of data.
4. Verify that users are fully trained in the proper use and dangers of wireless transaction devices.

**Evaluate Hardware, Firmware, and Updates:**

5. Perform a full inventory of all wireless transaction devices.
6. Verify that all devices are accounted for and that there are no devices not included in the planned implementation.

7. Verify that there are no devices that compromise security, due to hardware limitations or improper configuration.
8. Verify that all devices have current patches, firmware, and software.

#### **Evaluate Device Configuration:**

9. Verify that the data being sent is encrypted and the level of encryption being used.
10. Verify that wireless transaction devices will not communicate with unauthenticated devices.
11. Verify that any keys used for encryption are not set to default values.
12. Verify that devices are set to the lowest possible power setting that enables them to effectively transmit.
13. Verify that transmitters and receivers are within proper range of one another.

#### **Evaluate Access Control, Perimeter Security, and Ability to Intercept or Interfere with Communication:**

14. Determine the ability of unintended third to intercept transmitted data.
15. Determine the distance that data can be intercepted around the organization using high gain antennas.
16. Determine the ability to interfere with or jam transmitted data.
17. Determine the ability to perform denial of service attacks against wireless transaction devices.
18. Determine the ability to gain access to devices through playback of authentication sequences.
19. Determine the ability to interject erroneous data by either replaying recorded transmissions or sending specially crafted data.

## 9. RFID Testing

RFID (Radio Frequency Identifier) tags are composed of an integrated circuit (IC), which is sometimes half the size of a grain of sand, and an antenna – usually a coil of wires. Information is stored on the IC and transmitted via the antenna. RFID tags can either be passive (no battery, it uses energy from tag-reader's RF transmission) or active (self-powered by battery). The data transmission speed and range depends on power output, antenna size, receiver sensitivity, frequency, and interference. RFID tags can be read-only, read-write, or a combination of the two, where some data is read-only (such as the serial number) and other data is changeable for later encoding or updates.

Additionally, RFID tags do not require line of sight to be read and can function under a variety of environmental conditions – some tags are water resistant and washable. Each tag contains a 64 bit unique identifier and varying amounts of memory – many have 1024 bits. Therefore, they provide a high level of functionality and data integrity.

Some tags provide security measures. Most tags that use encryption have a 40-bit hidden encryption key. Some RFID transponders integrate a digital signature encryption protocol that includes a challenge/response authentication. Depending on the design of the RFID tag and the transponder, the authentication can be either one sided or two sided.

The exact frequencies used in RFID systems may therefore vary by country or region, however, RFID systems typically utilize the following frequency ranges:

- Low frequency: 30 to 300 kHz frequency range, primarily the 125 kHz band;
- High frequency: 13.56 MHz frequency range;
- Ultra-high frequency (UHF): 300 MHz to 1 GHz frequency range; and
- Microwave frequency: frequency range above 1 GHz, primarily the 2.45 GHz and 5.8 GHz bands.

RFID tags are absolutely invaluable to logistics, but feared and doubted by privacy advocates, because of the quality and quantity of information that they provide. Therefore, steps need to be taken to ensure that full logistics needs are not impaired, while privacy constraints are not trampled upon.

There is impending legislation that could affect the way companies use RFID tags, and it is best to take a proactive, forward-thinking approach for best practices. To do this, verify that RFID tags can be read at every step along the logistics path, but are deactivated at their final destination (such as point-of-sale) and that they cannot be reactivated by any means. Deactivation at the final destination helps protect against future legislation, as well as against malicious intent.

However, it also needs to be ensured that RFID tags cannot be deactivated by those attempting to steal the items. Therefore, RFID tag deactivation should only be performed at cash registers or at other specific places to meet business needs.

<b>Expected Results</b>	Identify the security measures provided by the RFID system Identify whether level of security is appropriate for its intended use Identify weaknesses in tracking methods Map the organizations practices relating to handling of RFID tagged devices Identify level of customer confidentiality required in respective industry
-------------------------	--

#### **Evaluate Business Needs, Practices, and Policies:**

1. Verify that the organization has an adequate security policy that addresses the use of wireless RFIDs.
2. Verify that users are trained in the proper use and the dangers of RFIDs.
3. Perform a security risk assessment to determine the value of the assets in the organization that contain RFIDs.
4. Verify that there are ongoing, random security audits to monitor and track uses of RFIDs and devices that read them.
5. Verify that a plan is in place to deal with the theft of RFIDs, scanners, and associated equipment.
6. Ensure that RFID tags on purchased products are disabled. This will reduce the possibility that a passer-by with a powerful RFID tag scanner and receiver will be able to enumerate items containing RFID tags within a location. It also mitigates the possibility of future liability regarding privacy issues caused by active RFIDs.

#### **Evaluate RFID Attributes (Authentication, Encryption, Properties...):**

7. Verify that serial number on ID tag cannot be changed.
8. Verify that tags used for secure transactions (such as credit cards or other payment devices) use appropriate encryption and authentication – preferably a two-sided challenges/handshake type authentication where data is not exchanged until both sides are verified.
9. Verify that secure information is not kept on the tags themselves, but on a server back-end that is accessible only after validation of exchanged information between the RFID tag and the reader.
10. Verify that active tags are not broadcasting secure information.
11. Verify that RFID tags have a kill feature to disable tracking at point-of-sale.
12. Verify that kill feature is not easily engaged by non-intended parties – for instance, it should require authentication and encryption to activate the kill feature.
13. Verify that the kill feature cannot be activated by playback of previously recorded sessions.

#### **Evaluate Placement, Scanners, and Tracking Equipment:**

14. For complete tracking of tagged products in a warehouse or other storage environment, ensure that RFID tag readers are in place at all entrances and exits, not just at main freight arrival and departure locations. This will help to reduce shrinkage caused by employee theft.

15. For situations where an actual device must be tracked and customer confidentiality is not a concern, verify that tags are not easily removed from the device, such as being on the outside of the box. It is best that the actual device have the RFID tag embedded within it and that its removal would render the device useless.
16. Verify that RFID tag readers have adequate power and reception sensitivity and are positioned in close enough proximity to read all of the tags that pass by them.
17. Verify that items are stacked and packaged in such a way that RFID tags can still be read. For instance, if packaging or stacking places too much shielding (such as foil in packaging) around tagged items, it may reduce the distance that they can be effectively read, due to weakness in signal strength. This would result in tracking failures.
18. For situations where customer confidentiality is a concern, verify that RFID tags are placed in the packaging of the device, preferably on the inside of the box. This helps reduce the possibility of accidental or deliberate removal of the tag, but provides confidentiality to the customer and protects the company from future privacy legislation and possible recall expenditures.

**Evaluate Access Control, Perimeter Security, and Ability to Intercept or Interfere with Communication:**

19. Verify that RFID tag and reader transmissions do not interfere with wireless networks and communications equipment.
20. Verify that areas near RFID readers that handle secure transactions have appropriate security measures, such as CCTV, to monitor transactions.
21. Probe reader devices for possible DoS problems.
22. Record and analyze secure transaction communications and analyze data sent between RFIDs and readers to determine if inappropriate data is transmitted.
23. Verify that authentication scheme is not susceptible to playback of previously recorded sessions to reveal secure data or allow fraudulent transactions.

## 10. Infrared Systems Testing

This is a method of testing infrared communications communication devices which may exceed the physical and monitored boundaries of an organization.

Infrared communication is much less accessible from the outside an organization, compared to 802.11 or Bluetooth. However, security on infrared devices tends to be frequently overlooked, due to its relative inaccessibility.

<b>Expected Results</b>	Map outer-most physical edge of the infrared communications List of line-of-site areas into the target The logical boundaries of infrared communications List of communication types List of systems and applications emanating from the target List the ability to upload, download, or intercept data
-------------------------	--

**Evaluate Business Needs, Practices, Policies and Locations of Sensitive Areas:**

1. Verify that the organization has an adequate security policy that addresses the use of wireless technology, such as infrared devices.
2. Verify that all users are trained in the proper use and the dangers of infrared technology.
3. Perform a security risk assessment to determine the value of the assets in the organization that are exposed to infrared devices.
4. Verify that there are ongoing, random security audits to monitor and track infrared devices.
5. Verify that a plan is in place to deal with the theft of infrared devices and that network passwords and keys are promptly changed.

**Evaluate Hardware, Firmware, and Updates:**

6. Perform a complete audit of all infrared enabled devices.
7. Verify that all devices are part of the planned implementation and were properly configured and that there are no rogue devices that compromise security by being confederate or improperly configured.
8. Verify that all of the latest patches and upgrades are applied to all infrared devices.
9. Verify that infrared patches and upgrades are deployed on a regular basis.
10. Probe network for possible DoS problems.

**Evaluate Access Control, Perimeter Security, and Ability to Intercept or Interfere with Communication:**

11. Verify the distance that the infrared communication extends beyond the physical boundaries of the organization.
12. Determine vulnerabilities in infrared uses within the organization, such as unencrypted uses of it in public areas.
13. Determine ability to upload or download data unauthenticated.
14. Determine ability to intercept data.
15. Determine ability to playback recorded authentication transmissions to gain access to secure data.

**Evaluate Device Configuration (Authentication, Passwords, Encryption..):**

16. Verify authentication-method of the clients.
17. Verify that encryption is used, configured, and type used.
18. Verify that clients can't be forced to fall-back to non-encrypted mode.
19. Verify that devices require a password to alter settings.

# Open Methodology License (OML)

Copyright (C) 2002 Institute for Security and Open Methodologies (ISECOM).

## PREAMBLE

A methodology is a tool that details WHO, WHAT, WHICH, and WHEN. A methodology is intellectual capital that is often protected strongly by commercial institutions. Open methodologies are community activities which bring all ideas into one documented piece of intellectual property which is freely available to everyone.

With respect the GNU General Public License (GPL), this license is similar with the exception for the right for software developers to include the open methodologies which are under this license in commercial software. This makes this license incompatible with the GPL.

The main concern this license covers for open methodology developers is that they will receive proper credit for contribution and development as well as reserving the right to allow only free publication and distribution where the open methodology is not used in any commercially printed material of which any monies are derived from whether in publication or distribution.

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 copyright holder saying it is protected under the terms of this Open Methodology License.
2. The Methodology refers to any such methodology or 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 copyright law which applies to a work containing the Methodology or a portion of it, either verbatim or with modifications and/or translated into another language.
3. All persons may copy and distribute verbatim copies of the Methodology as are received, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and 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 copyright holder.
4. No persons may sell this Methodology, charge for the distribution of this Methodology, or any medium of which this Methodology is apart of without explicit consent from the copyright holder.
5. All persons may include this Methodology in part or in whole in commercial service offerings, private or internal (non-commercial) use, or for educational purposes without explicit consent from the copyright holder providing the service offerings or personal or internal use comply to points 3 and 4 of this License.
6. No persons may modify or change this Methodology for republication without explicit consent from the copyright holder.
7. All persons may utilize the Methodology or any portion of it to create or enhance commercial or free software, and copy and distribute such software under any terms, provided that they also meet all of these conditions:

- a) Points 3, 4, 5, and 6 of this License are strictly adhered to.
  - b) Any reduction to or incomplete usage of the Methodology in the software must strictly and explicitly state what 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 an appropriate copyright notice and 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 or for any other reason (not limited to patent issues), conditions are imposed on any person (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If said person cannot satisfy simultaneously his obligations under this License and any other pertinent obligations, then as a consequence said person may not use, copy, modify, or distribute the Methodology at all. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.
9. If the distribution and/or use of the Methodology is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that 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. The Institute for Security and Open Methodologies may publish revised and/or new versions of the Open Methodology License. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

**NO WARRANTY**

11. BECAUSE THE METHODOLOGY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE METHODOLOGY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE METHODOLOGY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE IN USE OF THE METHODOLOGY IS WITH YOU. SHOULD THE METHODOLOGY PROVE INCOMPLETE OR INCOMPATIBLE YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY USE AND/OR REDISTRIBUTE THE METHODOLOGY UNMODIFIED AS PERMITTED HEREIN, BE LIABLE TO ANY PERSONS FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE METHODOLOGY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY ANY PERSONS OR THIRD PARTIES OR A 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.