INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OSSTMM 2.1.

Open-Source Security Testing Methodology Manual

Created by Pete Herzog

CURRENT VERSION:	OSSTMM 2.1
NOTES:	The sections and modules are based on the 2.0 model still. However, with this version the OSSTMM is bridging to the new 3.0 structure. After a year and a half, we have collected more than enough information to ensure better and more thorough security testing however the current format did not suffice for the collected information. The newer format will ensure that the new material will best accommodate maximum knowledge transfer. **All updated material until 2.5 will only be released only to subscribers.**
CHANGES:	The following changes are included: readability, document structure, all 6 methodologies have been updated, updated laws and best practices, rules of engagement structure, rules of thumb, ISECOM rules of ethics, and RAVs.
DATE OF CURRENT VERSION:	Saturday, August 23, 2003
DATE OF ORIGINAL VERSION:	Monday, December 18, 2000

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.

CREATED BY:	Pete Herzog	Managing Director of ISECOM - pete<at>isecom.org
KEY CONTRIBUTORS:	Marta Barceló Robert E. Lee Rick Tucker Nigel Hedges Colby Clark Tom O'Connor Andrea Barisani Gary Axten Marco Ivaldi Raoul Chiesa	*Assistant Director of ISECOM* - marta<at>isecom.org *co-Chairman of the Board of ISECOM* - robert<at>isecom.org *Board Advisor of ISECOM* - rick<at>isecom.org nigel.hedges<at>ca.com colby<at>isecom.org tom91<at>elivefree.net lcars<at>infis.univ.trieste.it gary.axten<at>lineone.net raptor<at>mediaservice.net raoul<at>mediaservice.net
KEY ASSISTANCE:	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	*Manager of the OPRP of ISECOM* - 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 nouchn<at>net2s.com scocat<at>remingtonltd.com leoloro<at>microsoft.com calcolea<at>menta.net claudia.kottmann<at>gmx.net
KEY SUPPORTERS:	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

PREVIOUS CONTRIBUTORS AND ASSISTANCE:	Rafael Ausejo Prieto Debbie Evans Daniel R. Walsh Juan Antonio Cerón Jordi Martinez Barrachina Michael S. Hines Miguel Angel Dominguez Torres Rich Jankowski Manuel Fernando Muiños Gómez Kevin Timm Sacha Faust Angel Luis Uruñuela Jose Luis Martin Mas Vincent Ip Anders Thulin Marcus M. Andersson	rafael.ausejo<at>dvc.es Debbie.Evans<at>dsnuk.com daniel.walsh<at>Total-Trust.com ja_ceron<at>terra.es jordi<at>security.gft.com mshines<at>purdue.edu mdominguez<at>security.gft.com richj<at>lucent.com mmuinos<at>dsecurity.net ktimm<at>var-log.com sacha<at>severus.org alum<at>phreaker.net jose.l.martin<at>dvc.es vincentiptingpong<at>hotmail.com anders.x.thulin<at>telia.se marcus.m.andersson<at>telia.se

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.

Previous Contributors and Assistance: This designation is for all individuals who's ideas and work still remains within the updated versions of the OSSTMM but are no longer regular contributors. Those who have asked to no longer be affiliated for government or corporate reasons have been removed.

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

Contributors 2
Foreword 4
Introduction 9
Scope 10
  Intended Audience 10
  Accreditation 10
  End Result 11
  Analysis 11
  Internet and Network Related Terms 11
  Compliance 15
    Legislation 15
    Best Practices 17
Rules Of Engagement 18
Rule of Thumb 20
Process 21
The Security Map 22
  Security Map Module List 23
Risk Assessment 25
  Risk Evaluation 25
  Perfect Security 25
  Risk Assessment Values 27
  Risk Types 27
Sections and Modules 29
Test Modules and Tasks 30
  Module Example 30
Methodology 31
Section A – Information Security 32
  Risk Assessment Values 33
  Modules 34
    1. Competitive Intelligence Review 34
    2. Privacy Review 35
    3. Document Grinding 36
Section B – Process Security 37
  Risk Assessment Values 38
  Modules 39
    1. Request Testing 39
    2. Guided Suggestion Testing 40
    3. Trusted Persons Testing 41
Section C – Internet Technology Security 42
  Risk Assessment Values 43
  Protocol Subsets 43
  Map Making 44
  Modules 45
    1. Logistics and Controls 45
    2. Network Surveying 46
    3. System Services Identification 47
    4. Competitive Intelligence Review 49
    5. Privacy Review 50
    6. Document Grinding 51
    4. Vulnerability Research and Verification 52
    5. Internet Application Testing 53

6. Routing ... 55
7. Trusted Systems Testing ... 56
8. Access Control Testing ... 57
9. Intrusion Detection System Testing ... 59
10. Containment Measures Testing ... 60
11. Password Cracking ... 61
12. Denial of Service Testing ... 62
13. Security Policy Review ... 63
Section D – Communications Security ... 64
Risk Assessment Values ... 65
Modules ... 66
1. PBX Testing ... 66
2. Voicemail Testing ... 67
3. FAX Review ... 68
4. Modem Testing ... 69
Section E – Wireless Security ... 70
Risk Assessment Values ... 71
Modules ... 72
1. Electromagnetic Radiation (EMR) Testing ... 72
2. [802.11] Wireless Networks Testing ... 73
3. Bluetooth Network Testing ... 75
4. Wireless Input Device Testing ... 76
5. Wireless Handheld Security Testing ... 77
6. Cordless Communications Testing ... 78
7. Wireless Surveillance Device Testing ... 79
8. Wireless Transaction Device Testing ... 80
9. RFID Testing ... 81
10. Infrared Systems Testing ... 83
11. Privacy Review ... 84
Section F – Physical Security ... 85
Risk Assessment Values ... 86
Modules ... 87
1. Perimeter Review ... 87
2. Monitoring Review ... 88
3. Access Controls Testing ... 89
4. Alarm Response Review ... 90
5. Location Review ... 91
6. Environment Review ... 92
Report Requirements Templates ... 93
Network Profile Template ... 94
Server Information Template ... 95
Firewall Analysis Template ... 96
Advanced Firewall Testing Template ... 98
IDS Test Template ... 99
Social Engineering Target Template ... 101
Social Engineering Telephone Attack Template ... 102
Social Engineering E-mail Attack Template ... 103
Trust Analysis Template ... 104
Privacy Review Template ... 105
Containment Measures Review Template ... 106
E-Mail Spoofing Template ... 107
Competitive Intelligence Template ... 108
Password Cracking Template ... 109

Denial of Service Template 110
Document Grinding Template 111
Social Engineering Template 119
Legal Penetration Testing Checklist 121
Test References 125
sap 27 125
Protocols 126
Open Methodology License (OML) 127

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

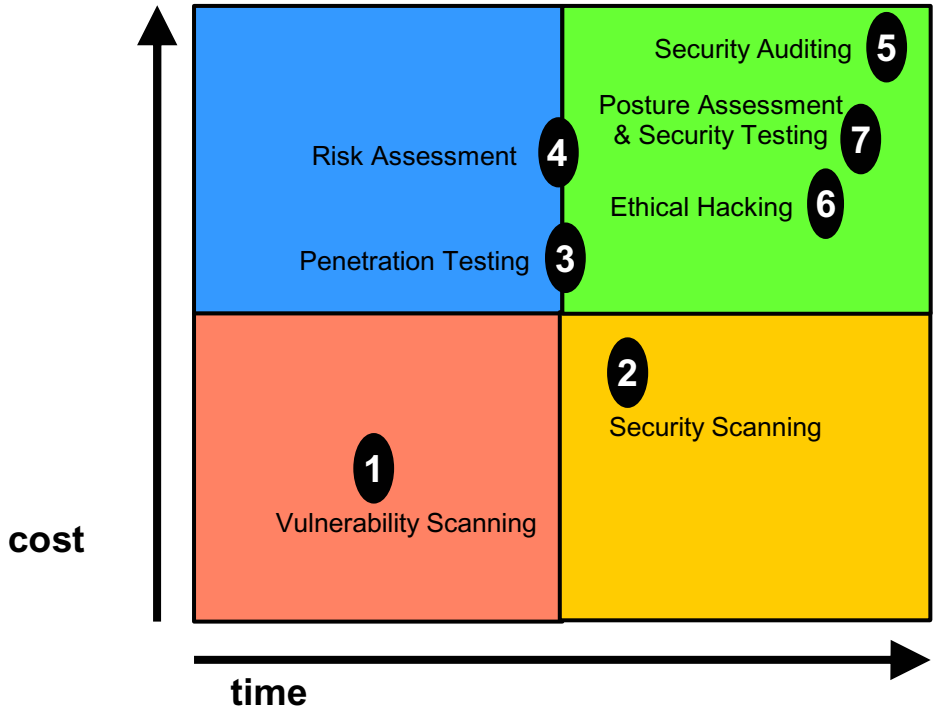
Throughout this manual we refer to words and terms that may be construed with other intents or meanings. This is especially true through international translations. For definitions not associated within this table below, see the reference of the OUSPG Vulnerability Testing Terminology glossary available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

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

Containment Measures	A process for quarantine and validation
Customer	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.
Environment	The interactive, co-dependent state of the network in operation. Also known as the setting
Estimate	A document of the time and man hours required for a test and may include price
Ethical Hacking	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
Expected Results	The findings from a specific module
Firewall	The software or hardware tool for imposing an Access Control List (ACL) on a system or network
Goal	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
Gray Box	The tester has some prior knowledge of the test elements or environment
Gray Hat	A hacker who is chaotic and anarchistic but does not break the law, however the actions often lack integrity or ethics
Hacker	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
Intrusion Detection System (IDS)	Either passive or active, host-based or network based, this tool is designed to monitor and sometimes stop attacks in action
Liability	The financial assurance of diligence and responsibility.
Location	The physical location.
Man Hours	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
Manual Testing	A test which requires a person to input data throughout the testing process and monitor the outcome to provide analysis
Man Weeks	This is the amount of work one person can do in one work week of 40 hours
Modules	These are viewpoints based in business security for individual OSSTMM sections
Network Scope	This refers to what a tester may legally test
Non Disclosure Agreement	A legal contract to stop the spread of information beyond the need to know basis of those sharing the NDA
PBX	Stands for Phone Exchange and is the central server in an organization for handling phone lines
Penetration Test	A security test with a defined goal which ends when the goal is achieved or time runs out
Plan	A calendar of tasks to be systematically completed in a test
Posture Assessment	The U.S. Military term for a security test
Practical	Defines security which is usable and applies to business justification
Privileges Testing	Tests where credentials are supplied to the user and permission is granted for testing with those credentials
Privileges	Credentials and permission
RAV	Risk Assessment Values. This is the de facto risk assessment tool of the OSSTMM which relies on cycles and degradation factors in the modules
Remote Access	This is defined as access from outside the location
Risk Assessment	In the OSSTMM this is used to describe security degradation as a comparison marker which can quantify a level of security over time
Router	A software or hardware device for routing packets
Scope	A description of what is permitted in a security test
Scouting	Document grinding for new or unique business information and trends
Sections	In the OSSTMM, these are used to define general security viewpoints. The

	OSSTMM uses 6 viewpoints; IT, Information, Wireless, Communications, Physical and Process
Security Audit	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.
Security Presence	How security is applied to all six security sections of an organization
Security Scope	Another term for scope
Security Test	A test for the security presence. May be specified by section
Social Engineering	An active attack against processes
Tasks	Specific security tests in a module to achieve one or more of the defined Expected Results
Time	Physical time - the fourth dimension - 24 hours a day
Usability	A step to making security understandable and efficient so as not to be intentionally bypassed for any legitimate reason
Verification Test	A follow-up security test after all the fixes have been fixed
Visibility	Components of the security presence which can be remotely discerned
Vulnerability Test	A test for services, open ports and known vulnerabilities
White Box	The tester has full prior knowledge of the test elements or environment
White Hat	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 (Cth) (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 3rd 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.

Rule of Thumb

These are the rules of thumb for security testing and gauging testing time.

Enumeration rule of thumb:

2 days for a class C <= 12 hops over a 64k digital line

- Add an additional hour per class C for every hop over 12.
- More bandwidth will decrease scanning time proportionally.
- Does not count for systems protected by an active IDS or application-level firewall.

OSSTMM test rule of thumb:

Complete OSSTMM testing rule of thumb includes enumeration.

3 man-weeks for 10 live systems in a class C <= 12 hops over 64k ISDN

- Add an additional 1/2 man hour per live system for every hop over 12.
- More bandwidth will decrease testing time proportionally up to 1Mb.
- Increasing the number of testers will decrease testing time proportionally. Analysis and reporting will become more complicated and take longer with more than 5 testers.
- Does not count for systems protected by an active IDS or application-level firewall.

Additional security testing rule of thumb calculations:

- In planning a security test, be sure to reserve approximately 2 man days per person per calendar week for research and development which includes system maintenance and verifying new testing tools.
- Total testing time should never exceed 3 months for a single test.
- Analysis can begin early but not before half the initial machine time for enumeration has lapsed.
- 1/2 the time spent testing is needed for reporting.
- The report should be delivered 3 days minimum before the workshop.
- The security testing organization should not outnumber the invited attendees at the workshop with the exception of if there is only 1 attendee then there may be two representatives from the testing organization.
- Of the number of attendees from the security testing organization at a workshop, one should always be the actual tester and one other should always be a commercial (sales) person.

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.

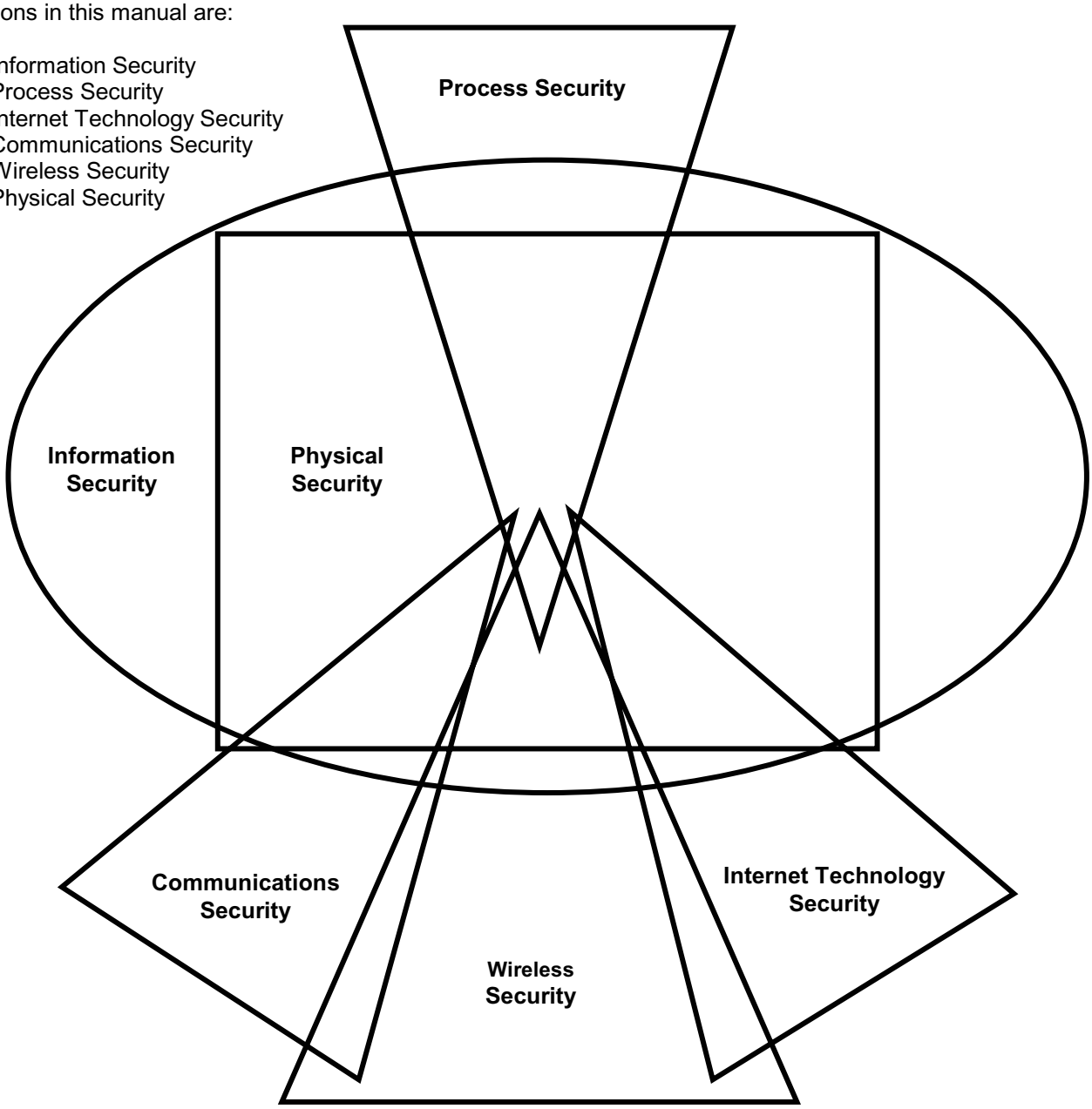
Alarm
Alarm is the timely and appropriate notification of activities that violate or attempt to violate any of the other security dimensions. In most security breaches, alarm is often the single process which initiates further consequences.

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.

1. **Information Security Testing**
    1. Posture Assessment
    2. Information Integrity Review
    3. Intelligence Survey
    4. Internet Document Grinding
    5. Human Resources Review
    6. Competitive Intelligence Scouting
    7. Privacy Controls Review
    8. Information Controls Review

2. **Process Security Testing**
    1. Posture Review
    2. Request Testing
    3. Reverse Request Testing
    4. Guided Suggestion Testing
    5. Trusted Persons Testing

3. **Internet Technology Security Testing**
    1. Logistics and Controls
    2. Posture Review
    3. Intrusion Detection Review
    4. Network Surveying
    5. System Services Identification
    6. Competitive Intelligence Scouting
    7. Privacy Review
    8. Document Grinding
    9. Internet Application Testing
    10. Exploit Research and Verification
    11. Routing
    12. Trusted Systems Testing
    13. Access Control Testing
    14. Password Cracking
    15. Containment Measures Testing
    16. Survivability Review
    17. Denial of Service Testing
    18. Security Policy Review
    19. Alert and Log Review

4. **Communications Security Testing**
    1. Posture Review
    2. PBX Review
    3. Voicemail Testing
    4. FAX Testing
    5. Modem Survey
    6. Remote Access Control Testing
    7. Voice over IP Testing
    8. X.25 Packet Switched Networks Testing

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

6. **Physical Security Testing**
    1. Posture Review
    2. Access Controls Testing
    3. Perimeter Review
    4. Monitoring Review
    5. Alarm Response Review
    6. Location Review
    7. Environment 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 then 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:

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 0º 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.

	Verified	Identified	Not Applicable
Vulnerability	3.2	1.6	0.4
Weakness	1.6	0.8	0.3
Concern	0.8	0.4	0.2
Information Leak	0.4	0.2	0.1
Unknown	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

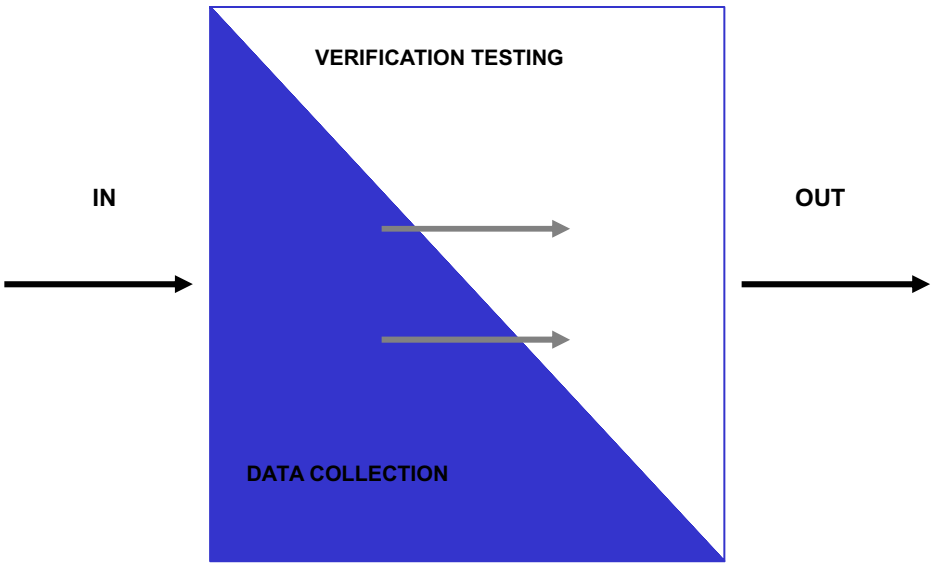
Module Name
Description of the module.

Expected Results:	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.



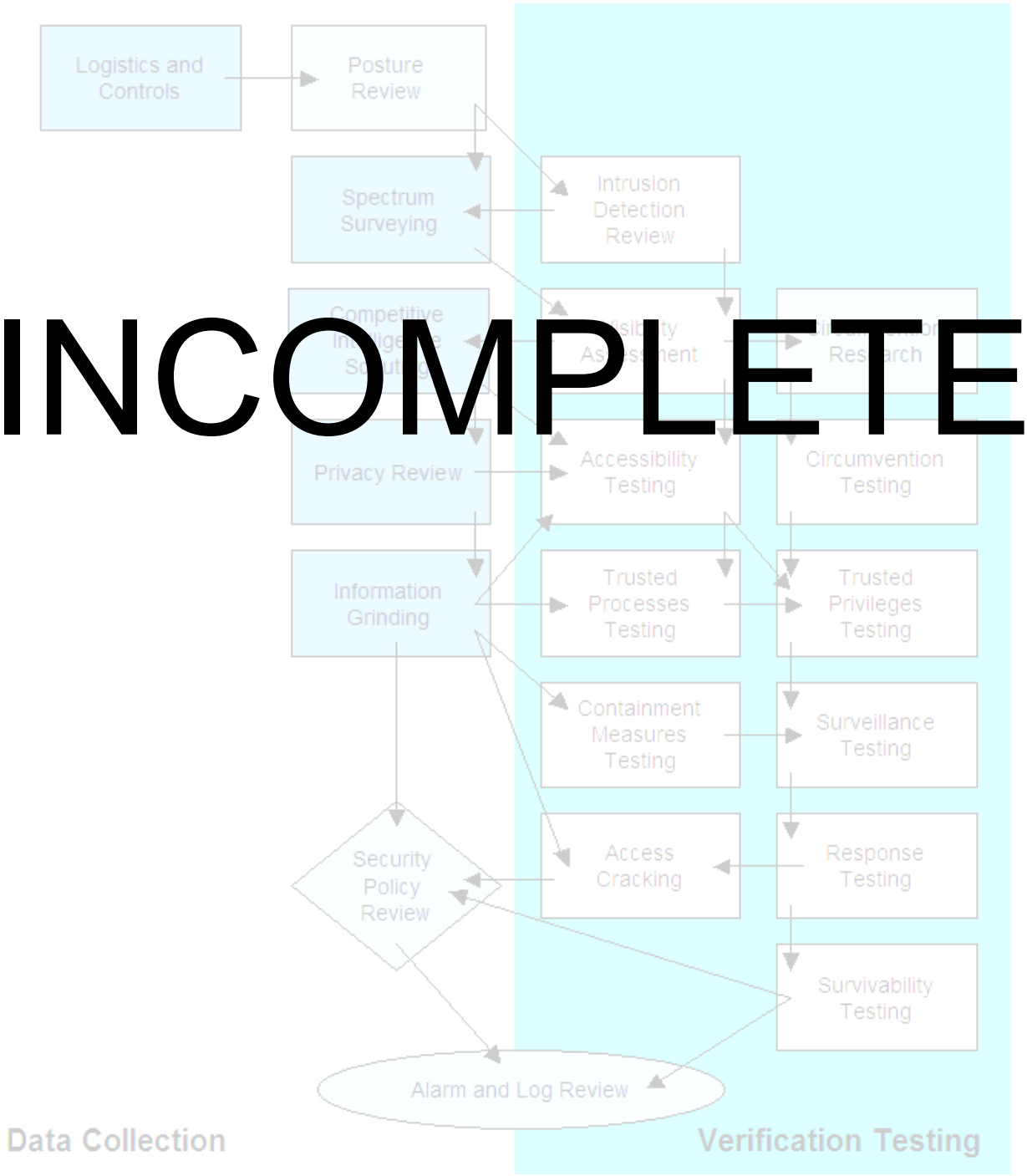
In defining the methodology of testing, it is important to not constrict the creativity of the tester by introducing standards so formal and unrelenting that the quality of the test suffers. Additionally, it is important to leave tasks open to some interpretation where exact definition will cause the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



INCOMPLETE

Risk Assessment Values

Module	Cycle (days)	Degradation (%)	Influence (x)
Posture Assessment	Unavailable	Unavailable	Unavailable
Information Integrity Review	Unavailable	Unavailable	Unavailable
Intelligence Survey	Unavailable	Unavailable	Unavailable
Internet Document Grinding	Unavailable	Unavailable	Unavailable
Human Resources Review	Unavailable	Unavailable	Unavailable
Competitive Intelligence Review	Unavailable	Unavailable	Unavailable
Privacy Controls Review	Unavailable	Unavailable	Unavailable
Information Controls Review	Unavailable	Unavailable	Unavailable

Modules

1. Competitive Intelligence Review

CI Scouting is the scavenged information from an Internet presence that can be analyzed as business intelligence. Different than the straight-out intellectual property theft found in industrial espionage or hacking, CI tends to be non-invasive and much more subtle. It is a good example of how the Internet presence extends far beyond the hosts in the DMZ. Using CI in a penetration test gives business value to the components and can help in finding business justifications for implementing various services.

Expected Results:	A measurement of the organization's network business justifications Size and scope of the Internet presence A measurement of the security policy to future network plans

1. Map and measure the directory structure of the web servers
2. Map the measure the directory structure of the FTP servers
3. Examine the WHOIS database for business services relating to registered host names
4. Determine the IT cost of the Internet infrastructure based on OS, Applications, and Hardware.
5. Determine the cost of support infrastructure based on regional salary requirements for IT professionals, job postings, number of personnel, published resumes, and responsibilities.
6. Measure the buzz (feedback) of the organization based on newsgroups, web boards, and industry feedback sites
7. Record the number of products being sold electronically (for download)
8. Record the number of products found in P2P sources, wares sites, available cracks up to specific versions, and documentation both internal and third party about the products

2. Privacy Review

The privacy review is the focal point of the legal and ethical storage, transmission, and control of data based on employee and customer privacy. The use of this data is a concern to many private persons and legislation is unveiling specific rules regarding privacy. Although some of these laws are local, all of them apply to the Internet and therefore affect security testers internationally.

Expected Results:	List any disclosures List compliance failures between public policy and actual practice List systems involved in data gathering List data gathering techniques List data gathered

1. Compare publicly accessible policy to actual practice
2. Compare actual practice to regional fraud and privacy laws or compliancy
3. Identify database type and size for storing data
4. Identify data collected by the organization
5. Identify storage location of data
6. Identify cookie types
7. Identify cookie expiration times
8. Identify information stored in cookie
9. Verify cookie encryption methods
10. Identify server location of web bug(s)
11. Identify web bug data gathered and returned to server

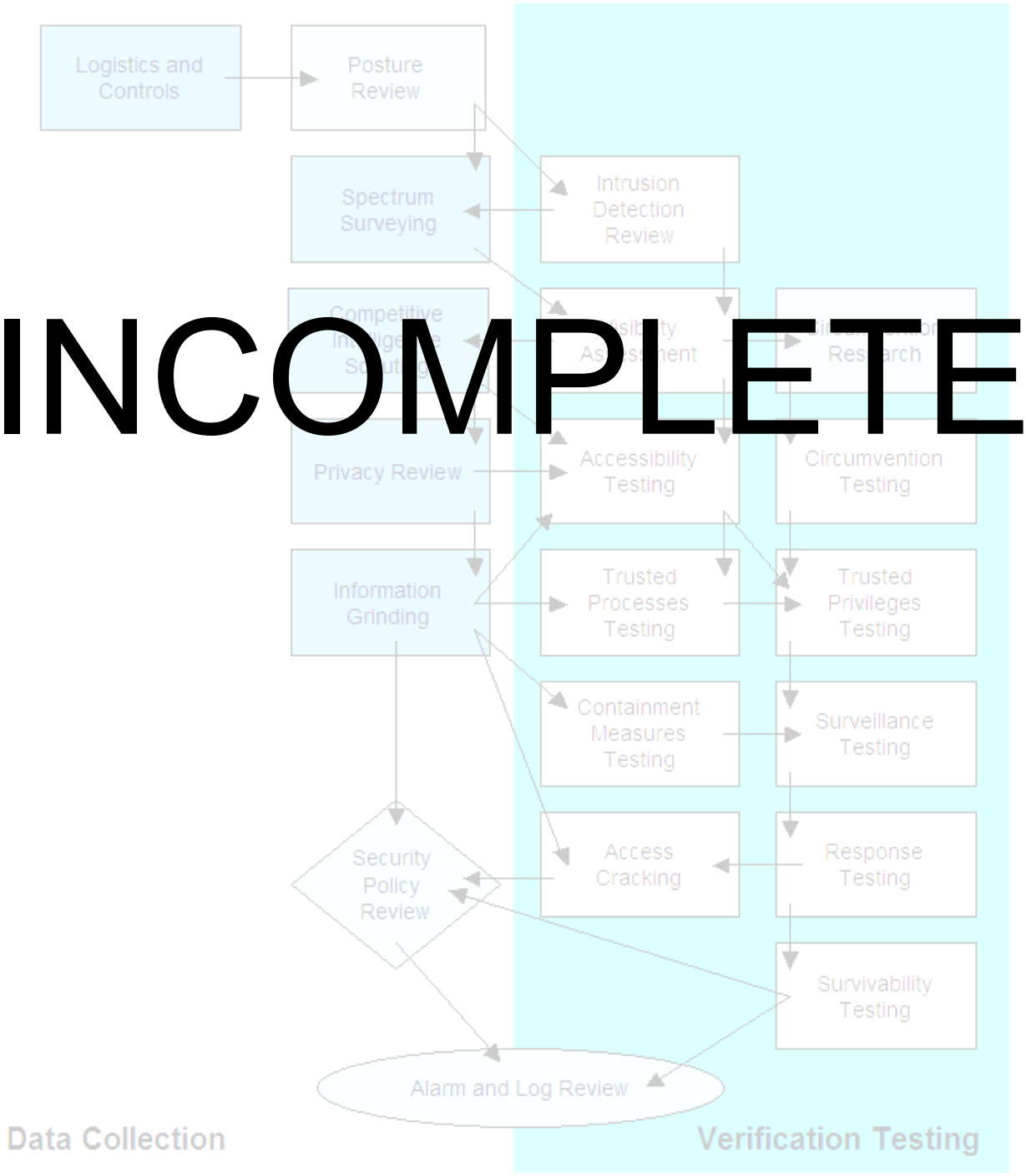
3. Document Grinding

The module here is important in the verification of much of the tested information and pertains to many levels of what is considered information security. The amount of time granted to the researching and extraction of information is dependent upon the size of the organization, the scope of the project, and the length of time planned for the testing. More time however, does not always mean more information but it can eventually lead to key pieces of the security puzzle.

Expected Results:	A profile of the organization A profile of the employees A profile of the organization's network A profile of the organization's technologies A profile of the organization's partners, alliances, and strategies

1. Examine web databases and caches concerning the target organization and key people.
2. Investigate key persons via personal homepages, published resumes, organizational affiliations, directory enquiries, companies house data, and electoral register.
3. Compile e-mail addresses from within the organization and personal e-mail addresses from key people.
4. Search job databases for skill sets technology hires need to possess in the target organization.
5. Search newsgroups for references to and submissions from within the organization and key people.
6. Search documents for hidden codes or revision data.
7. Examine P2P networks for references to and submissions from within the organization and key people.

Section B – Process Security



INCOMPLETE

Risk Assessment Values

Module	Cycle (days)	Degradation (%)	Influence (x)
Posture Review	Unavailable	Unavailable	Unavailable
Request Testing	Unavailable	Unavailable	Unavailable
Reverse Request Testing	Unavailable	Unavailable	Unavailable
Guided Suggestion Testing	Unavailable	Unavailable	Unavailable
Trusted Persons Testing	Unavailable	Unavailable	Unavailable

Modules

1. Request Testing

This is a method of gaining access privileges to an organization and its assets by querying gateway personnel over communications medium such as telephone, e-mail, chat, bulletin boards, etc. from a fraudulent “privileged” position. Gateway personnel are those who themselves have the authority to grant access privileges to others.

Expected Results:	List of access code methods List of valid codes Names of gateway persons Methods of obtaining this information List of information obtained

1. Select a gateway person from information already gained about personnel
2. Examine the contact methods for gateway person from the target organization
3. Gather information about gateway person (position, habits, preferences)
4. Contact gateway person and request information from an authority or privileged position
5. Gather information from gateway person
6. Enumerate amount of privileged information disclosed.

2. Guided Suggestion Testing

This is a method of enumeration and privileged access points enumeration to an organization and its assets by inviting internal personnel over communications medium such as telephone, e-mail, chat, bulletin boards, etc. to an outside location from a fraudulent “privileged” position. This invitation technique requires a “location” for the person to be invited to such as a web page, e-mail account,

Expected Results:	List of access points List of internal IP addresses Methods of obtaining this information List of information obtained

1. Select a person or persons from information already gained about personnel
2. Examine the contact methods for the people from the target organization
3. Invite the people to use / visit the location
4. Gather information from the visitors
5. Enumerate the type and amount of privileged information disclosed.

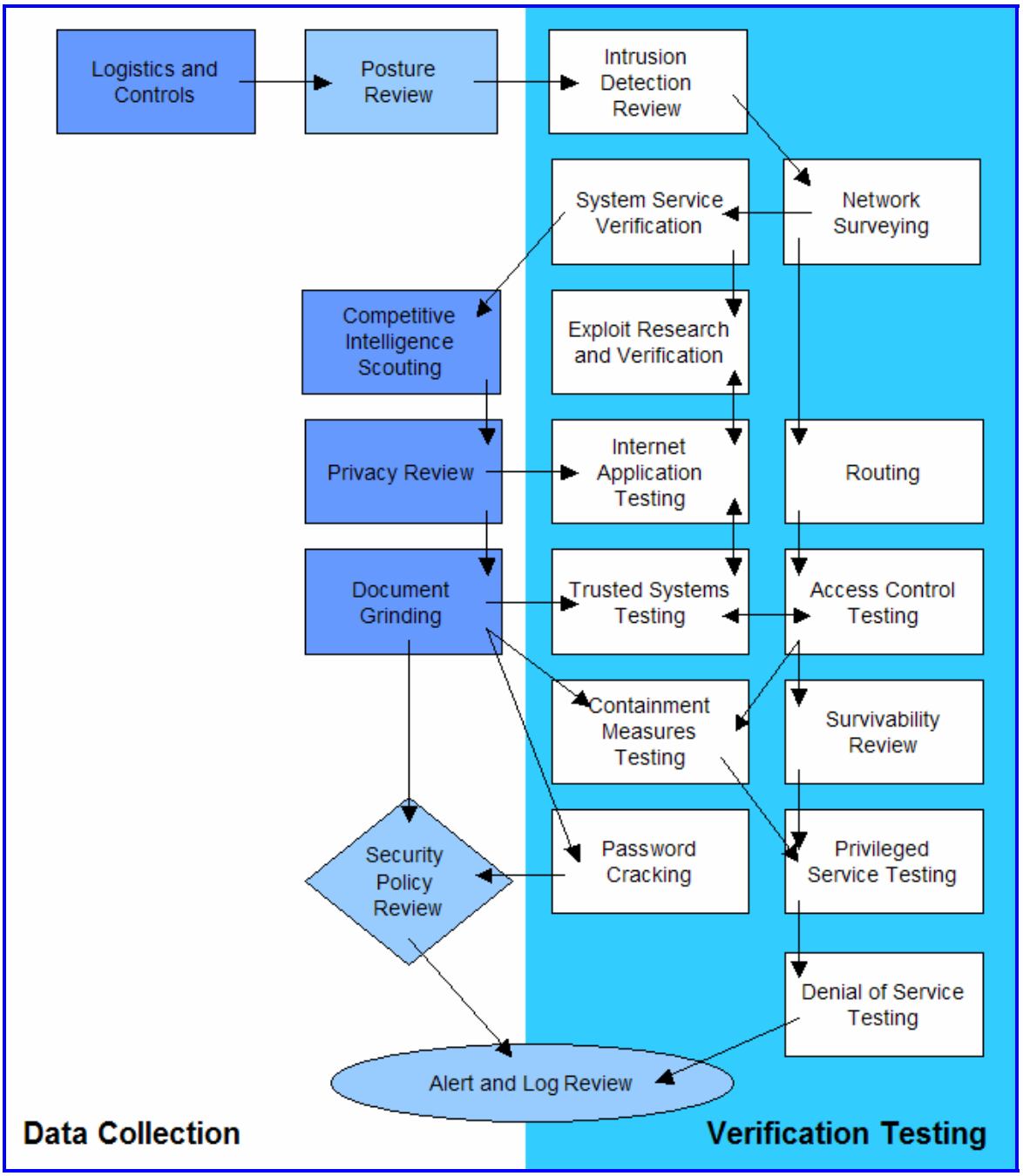
3. Trusted Persons Testing

This is a method of using a trusted position of such as that of an employee, vendor, partner, or daughter company employee to subvert the internal person into disclosing information concerning the target organization. This module may be performed through any communication means or in person.

Expected Results:	List of trusted persons List of trusted positions Methods of obtaining this information List of information obtained

1. Select a person or persons from information already gained about personnel
2. Examine the contact methods for the people from the target organization
3. Contact the internal person from a position of trust
4. Gather information from the internal person
5. Enumerate the type and amount of privileged information disclosed.

Section C – Internet Technology Security



Risk Assessment Values

Module	Cycle (days)	Degradation (%)	Influence (x)
Logistics and Controls	0	0	1.6
Posture Review	178	12	
Intrusion Detection Review	25	2.3	
Network Surveying	30	3	
System Services Identification	7,19,54	1.7,3.9,2.15	
Comp Intel Scouting	17	7.3	
Privacy Review	96	2.9	
Document Grinding	96	8.7	
Internet Application Testing	67	5.8	
Exploit Research & Verification	3	3.6	
Routing	34	3.2	
Trusted Systems Testing	42	4.1	
Access Control Testing	34	2.9	
Password Cracking	21	7.8	
Containment Measures Testing	96	3.9	
Survivability Review	178	9	
Privileged Service Testing	25	2.3	
Denial of Service Testing	4	5.4	
Security Policy Review	124	6.7	
Alert and Log Review	0	0	

Protocol Subsets

Protocol	Subset A	Subset B
TCP	1,21,22,23,25,53,80,110,111,161,443	1,7,19,21,22,23,25,53,80,110, 111,137,139,161,389,443,445, 1433,1434,10001,12001,33580, 65535
UDP	1,20,53,65,67,68,69,139,161,445,1433,1434	1,7,13,19,20,53,65,67,68,69,139,161 ,445,1433,1434,1812,10001,12001,3 3580,65535
ICMP	0/0,3/3,3/4,8/0,11/0,13/0,15/0	0/0,3/0,3/1,3/2,3/3,3/4,3/5,3/6,3/7,4/0 ,8/0,11/0,13/0,15/0,30,33,34,40/1
IPv4	Unavailable	Unavailable
IPv6	Unavailable	Unavailable
OSPF	Unavailable	Unavailable
ISAKMP	Unavailable	Unavailable
IPSec	Unavailable	Unavailable
BGP	Unavailable	Unavailable
RTP	Unavailable	Unavailable
RSVP	Unavailable	Unavailable
IGMP	Unavailable	Unavailable
IOTP	Unavailable	Unavailable
L2TP	Unavailable	Unavailable

Map Making

Routing
Trusts
Access points
Alarm ID segments
Services
Access Control
Survivability

INCOMPLETE

Modules

1. Logistics and Controls

The purpose of this module is to reduce false positives and false negatives by assuring proper adjustments are made to all testing tools.

Expected Results:	The testing bandwidth discrepancies Packet loss for TCP Packet loss for UDP Packet loss for ICMP Network routing problems ISPs routing traffic and Transit Sellers

Error Checking

1. Examine the route to the target network for packet loss using TCP
2. Examine the route to the target network for packet loss using UDP
3. Examine the route to the target network for packet loss using ICMP
4. Measure the rate of packet round-trip time using TCP
5. Measure TCP latency through TCP connections
6. Measure the rate of packet acceptance and response on the target network
7. Measure the amount of packet loss or connection denials at the target network

Routing

8. Examine the routing path to the targets from the attack system.
9. Examine the routing path for the target's ISPs.
10. Examine the routing path for the target ISPs primary Transit Sellers.
11. Examine the use of IPv6 to each live host in the network.

2. Network Surveying

A network survey serves often as an introduction to the systems to be tested. It is best defined as a combination of data collection, information gathering, and policy control. Although it is often advisable from a legal standpoint to define contractually exactly which systems to test if you are a third-party auditor or even if you are the system administrator, you may not be able to start with concrete system names or IP addresses. In this case you must survey and analyze. The point of this exercise is to find the number of reachable systems to be tested without exceeding the legal limits of what you may test. Therefore the network survey is just one way to begin a test; another way is to be given the IP range to test. In this module, no intrusion is being performed directly on the systems except in places considered a quasi-public domain.

In legal terms, the quasi-public domain is a store that invites you in to make purchases. The store can control your access and can deny certain individuals entry but for the most part is open to the general public (even if it monitors them). This is the parallel to an e-business or web site.

Although not truly a module in the methodology, the network survey is a starting point. Often more hosts are detected during actual testing. Please bear in mind that the hosts discovered later may be inserted in the testing as a subset of the defined testing and often only with permission or collaboration with the target organization's internal security team.

Expected Results:	Domain Names Server Names IP Addresses Network Map ISP / ASP information System and Service Owners Possible test limitations

Name server responses.

1. Examine Domain registry information for servers.
2. Find IP block owned.
3. Question the primary, secondary, and ISP name servers for hosts and sub domains.
4. Find IPv6 IP blocks in use though DNS queries.

Examine the outer wall of the network.

5. Use multiple traces to the gateway to define the outer network layer and routers.

Examine tracks from the target organization.

6. Search web logs and intrusion logs for system trails from the target network.
7. Search board and newsgroup postings for server trails back to the target network.

Information Leaks

8. Examine target web server source code and scripts for application servers and internal links.
9. Examine e-mail headers, bounced mails, and read receipts for the server trails.
10. Search newsgroups for posted information from the target.
11. Search job databases and newspapers for IT positions within the organization relating to hardware and software.
12. Search P2P services for connections into the target network and data concerning the organization.

3. System Services Identification

Port scanning is the invasive probing of system ports on the transport and network level. Included here is also the validation of system reception to tunneled, encapsulated, or routing protocols. This module is to enumerate live or accessible Internet services as well as penetrating the firewall to find additional live systems. The small sample of protocols here is for clarity of definition. Many protocols are not listed here. Testing for different protocols will depend on the system type and services it offers. For a more complete list of protocols, see the Test References section.

Each Internet enabled system has 65,536 TCP and UDP possible ports (incl. Port 0). However, it is not always necessary to test every port for every system. This is left to the discretion of the test team. Port numbers that are important for testing according to the service are listed with the task. Additional port numbers for scanning should be taken from consensus intrusion database project sites such as www.dshield.org.

Once open ports have been identified, it is necessary to conduct an active examination of the application listening behind the service. In certain cases more than one application exists behind a service where one application is the listener and the others are considered components of the listening application. A good example of this is PERL installed for use in a Web application. In that case the listening service is the HTTP daemon and the component is PERL.

After service identification, the next step is to identify the system through the active probing of a system for responses that can distinguish its operating system and version level.

Expected Results:	Open, closed or filtered ports IP addresses of live systems Internal system network addressing List of discovered tunneled and encapsulated protocols List of discovered routing protocols supported Active services Service Types Service Application Type and Patch Level OS Type Patch Level System Type List of live systems Internal system network addressing Network Map

Enumerate Systems

1. Collect broadcast responses from the network
2. Probe past the firewall with strategically set packet TTLs (Firewalking) for all IP addresses.
3. Use ICMP and reverse name lookups to determine the existence of all the machines in a network.
4. Use a TCP source port 80 and ACK on ports 3100-3150, 10001-10050, 33500-33550, and 50 random ports above 35000 for all hosts in the network.
5. Use TCP fragments in reverse order with FIN, NULL, and XMAS scans on ports 21, 22, 25, 80, and 443 for all hosts in the network.
6. Use a TCP SYN on ports 21, 22, 25, 80, and 443 for all hosts in the network.
7. Use DNS connect attempts on all hosts in the network.
8. Use FTP and Proxies to bounce scans to the inside of the DMZ for ports 22, 81, 111, 132, 137, and 161 for all hosts on the network.

Enumerating Ports

9. Use TCP SYN (Half-Open) scans to enumerate ports as being open, closed, or filtered on the default TCP testing ports for all the hosts in the network.
10. Use TCP full connect scans to scan all ports up to 1024 on all hosts in the network.
11. Use TCP fragments in reverse order to enumerate ports and services for the subset of ports on the default Packet Fragment testing ports in Appendix B for all hosts in the network.
12. Use UDP scans to enumerate ports as being open or closed on the default UDP testing ports if UDP is NOT being filtered already. [Recommended: first test the packet filtering with a small subset of UDP ports.]

Verifying Various Protocol Response

13. Verify and examine the use of traffic and routing protocols.
14. Verify and examine the use of non-standard protocols.
15. Verify and examine the use of encrypted protocols.
16. Verify and examine the use of TCP and ICMP over IPv6.

Verifying Packet Level Response

17. Identify TCP sequence predictability.
18. Identify TCP ISN sequence numbers predictability.
19. Identify IPID Sequence Generation predictability.
20. Identify system up-time.

Identifying Services

21. Match each open port to a service and protocol.
22. Identify server uptime to latest patch releases.
23. Identify the application behind the service and the patch level using banners or fingerprinting.
24. Verify the application to the system and the version.
25. Locate and identify service remapping or system redirects.
26. Identify the components of the listening service.
27. Use UDP-based service and Trojan requests to all the systems in the network.

Identifying Systems

28. Examine system responses to determine operating system type and patch level.
29. Examine application responses to determine operating system type and patch level.
30. Verify the TCP sequence number prediction for each live host on the network.
31. Search job postings for server and application information from the target.
32. Search tech bulletin boards and newsgroups for server and application information from the target.
33. Match information gathered to system responses for more accurate results.

4. Competitive Intelligence Review

CI Scouting is the scavenged information from an Internet presence that can be analyzed as business intelligence. Different than the straight-out intellectual property theft found in industrial espionage or hacking, CI tends to be non-invasive and much more subtle. It is a good example of how the Internet presence extends far beyond the hosts in the DMZ. Using CI in a penetration test gives business value to the components and can help in finding business justifications for implementing various services.

Expected Results:	A measurement of the organization's network business justifications Size and scope of the Internet presence A measurement of the security policy to future network plans

Business Intelligence

1. Map and measure the directory structure of the web servers
2. Map the measure the directory structure of the FTP servers
3. Examine the WHOIS database for business services relating to registered host names
4. Determine the IT cost of the Internet infrastructure based on OS, Applications, and Hardware.
5. Determine the cost of support infrastructure based on regional salary requirements for IT professionals, job postings, number of personnel, published resumes, and responsibilities.
6. Measure the buzz (feedback) of the organization based on newsgroups, web boards, and industry feedback sites
7. Record the number of products being sold electronically (for download)
8. Record the number of products found in P2P sources, wares sites, available cracks up to specific versions, and documentation both internal and third party about the products
9. Identify the business partners
10. Identify the customers from organizations to industry sectors
11. Verify the clarity and ease of use of the merchandise purchasing process
12. Verify the clarity and ease of use for merchandise return policy and process
13. Verify that all agreements made over the Internet from digital signature to pressing a button which signifies acceptance of an end-user agreement can be repudiated immediately and for up to 7 days.

5. Privacy Review

The privacy review is the focal point of the legal and ethical storage, transmission, and control of data based on employee and customer privacy. The use of this data is a concern to many private persons and legislation is unveiling specific rules regarding privacy. Although some of these laws are local, all of them apply to the Internet and therefore affect security testers internationally.

In these tests, it is required to understand the difference between personal and private information: Private information is information which is generally only known to the persons themselves and the authority who collected that data. This could be university transcripts, amount of money given to the church, names of ex-girlfriends or ex-boyfriends, and perhaps an embarrassing childhood memory. Personal information is information that describes a person or a person's lifestyle such as birth date, hair color, age, names of members in the family, the bank they use, their pets' names, gender, sexual preferences, religion, or favorite color.

Additionally, personally identifiable information is information that a person's identity can be derived from whether alone or in aggregate. This could be a person's name or government ID number.

Expected Results:	List any disclosures List compliance failures between public policy and actual practice List systems involved in data gathering List data gathering techniques List data gathered

Policy

1. Identify public privacy policy
2. Identify web-based forms
3. Identify database type and location for storing data
4. Identify data collected by the organization
5. Identify storage location of data
6. Identify cookie types
7. Identify cookie expiration times
8. Identify information stored in cookie
9. Verify cookie encryption methods
10. Identify the clarity of opt-out information
11. Identify the ease of use for opt-out
12. Identify beacon gifs (web bugs) in web services and e-mails
13. Identify server location of beacon gifs
14. Identify web bug data gathered and returned to server

False Light and Defamation

15. Identify fictionalized persons, organizations, institutions with real persons.
16. Identify persons or organizations portrayed in a negative manner.

Appropriation

17. Identify persons, organizations, or materials which as themselves or of a likeness thereof which is used for commercial reasons as in web sites or advertisements.

Disclosure of Private Facts

18. Identify information about employees persons, organizations, or materials which contain private information.

6. Document Grinding

The module here is important in the verification of much of the tested information and pertains to many levels of what is considered information security. The amount of time granted to the researching and extraction of information is dependent upon the size of the organization, the scope of the project, and the length of time planned for the testing. More time however, does not always mean more information but it can eventually lead to key pieces of the security puzzle.

Expected Results:	A profile of the organization A profile of the employees A profile of the organization's network A profile of the organization's technologies A profile of the organization's partners, alliances, and strategies

1. Examine web databases and caches concerning the target organization and key people.
2. Investigate key persons via personal homepages, published resumes, organizational affiliations, directory enquiries, companies house data, and electoral register.
3. Compile e-mail addresses from within the organization and personal e-mail addresses from key people.
4. Search job databases for skill sets technology hires need to possess in the target organization.
5. Search newsgroups for references to and submissions from within the organization and key people.
6. Search documents for hidden codes or revision data.
7. Examine P2P networks for references to and submissions from within the organization and key people.

4. Vulnerability Research and Verification

The focus of this module is in the identification, understanding, and verification of weaknesses, misconfigurations and vulnerabilities within a host or network.

Research involved in finding vulnerabilities is necessary up until the delivery of the report. This involves searching online databases and mailing lists specific to the systems and network being tested. Do not confine yourself to the web, consider using IRC, Newsgroups, and underground FTP sites.

Testing for vulnerabilities using automated tools is an efficient way to determine existing holes and system patch level. Although many automated scanners are currently on the market and in the underground, it is important for the tester to identify and incorporate the current underground scripts/exploits into this testing. However, manual verification is necessary for eliminating false positives, expanding the hacking scope, and discovering the data flow in and out of the network. Manual testing refers to a person or persons at the computer using creativity, experience, and ingenuity to test the target network.

Expected Results:	Type of application or service by vulnerability Patch levels of systems and applications List of possible denial of service vulnerabilities List of areas secured by obscurity or visible access List of actual vulnerabilities minus false positives List of Internal or DMZ systems List of mail, server, and other naming conventions Network map

1. Integrate the currently popular scanners, hacking tools, and exploits into the tests.
2. Measure the target organization against the currently popular scanning tools.
3. Attempt to determine vulnerability by system and application type.
4. Attempt to match vulnerabilities to services.
5. Attempt to determine application type and service by vulnerability.
6. Perform redundant testing with at least 2 automated vulnerability scanners.
7. Identify all vulnerabilities according to applications.
8. Identify all vulnerabilities according to operating systems.
9. Identify all vulnerabilities from similar or like systems that may also affect the target systems.
10. Verify all vulnerabilities found during the exploit research phase for false positives and false negatives.
11. Verify all positives (be aware of your contract if you are attempting to intrude or might cause a denial of service).

5. Internet Application Testing

An Internet application test employs different software testing techniques to find "security bugs" in server/client applications of the system from the Internet. In this module, we refer the server/client applications to those proprietarily developed by the system owners serving dedicate business purposes and the applications can be developed with any programming languages and technologies. E.g. web application for business transactions is a target in this module. "Black box" and/or "White box" testing can be used in this module.

Expected Results:	List of applications List of application components List of application vulnerabilities List of application system trusts

Re-Engineering

1. Decompose or deconstruct the binary codes, if accessible.
2. Determines the protocol specification of the server/client application.
3. Guess program logic from the error/debug messages in the application outputs and program behaviors/performance.

Authentication

4. Find possible brute force password guessing access points in the applications.
5. Find a valid login credentials with password grinding, if possible.
6. Bypass authentication system with spoofed tokens.
7. Bypass authentication system with replay authentication information.
8. Determine the application logic to maintain the authentication sessions - number of (consecutive) failure logins allowed, login timeout, etc.
9. Determine the limitations of access control in the applications - access permissions, login session duration, idle duration.

Session Management

10. Determine the session management information - number of concurrent sessions, IP-based authentication, role-based authentication, identity-based authentication, cookie usage, session ID in URL encoding string, session ID in hidden HTML field variables, etc.
11. Guess the session ID sequence and format
12. Determine the session ID is maintained with IP address information; check if the same session information can be retried and reused in another machine.
13. Determine the session management limitations - bandwidth usages, file download/upload limitations, transaction limitations, etc.
14. Gather excessive information with direct URL, direct instruction, action sequence jumping and/or pages skipping.
15. Gather sensitive information with Man-In-the-Middle attacks.
16. Inject excess/bogus information with Session-Hijacking techniques.
17. Replay gathered information to fool the applications.

Input Manipulation

18. Find the limitations of the defined variables and protocol payload - data length, data type, construct format, etc.
19. Use exceptionally long character-strings to find buffer overflows vulnerability in the applications.
20. Concatenate commands in the input strings of the applications.
21. Inject SQL language in the input strings of database-tired web applications.

22. Examine "Cross-Site Scripting" in the web applications of the system.
23. Examine unauthorized directory/file access with path/directory traversal in the input strings of the applications.
24. Use specific URL-encoded strings and/or Unicode-encoded strings to bypass input validation mechanisms of the applications.
25. Execute remote commands through "Server Side Include".
26. Manipulate the session/persistent cookies to fool or modify the logic in the server-side web applications.
27. Manipulate the (hidden) field variable in the HTML forms to fool or modify the logic in the server-side web applications.
28. Manipulate the "Referrer", "Host", etc. HTTP Protocol variables to fool or modify the logic in the server-side web applications.
29. Use illogical/illegal input to test the application error-handling routines and to find useful debug/error messages from the applications.

Output Manipulation

30. Retrieve valuable information stored in the cookies
31. Retrieve valuable information from the client application cache.
32. Retrieve valuable information stored in the serialized objects.
33. Retrieve valuable information stored in the temporary files and objects.

Information Leakage

34. Find useful information in hidden field variables of the HTML forms and comments in the HTML documents.
35. Examine the information contained in the application banners, usage instructions, welcome messages, farewell messages, application help messages, debug/error messages, etc.

6. Routing

The Screening Router is a defense often found on a network that restricts the flow of traffic between the enterprise network and the Internet. It operates on a security policy and uses ACL's (Access Control Lists) to accept or deny packets. This module is designed to assure that only that which should be expressly permitted be allowed into the network; all else should be denied. The screen may also be designed to restrict the outflow of certain types of traffic as well. Routers are becoming more and more complex and some may have features unknown to the tester and often the target organization. The tester's role is in part to determine the role of the router in the DMZ.

Expected Results:	Router type and features implemented Information on the router as a service and a system Outline of the network security policy by the ACL List of the types of packets which may enter the network Map of router responses to various traffic types List of live systems found

Router and feature identification

1. Verify the router type with information collected from intelligence gathering.
2. Verify if the router is providing network address translation (NAT)
3. Verify the penetrations from strategically determined packet TTL settings (Firewalking) completed in the Port Scanning module.

Verifying router ACL configuration

4. Test the ACL against the written security policy or against the "Deny All" rule.
5. Verify that the router is egress filtering local network traffic
6. Verify that the router is performing address spoof detection
7. Verify the penetrations from inverse scanning completed in the Port Scanning module.
8. Test the router outbound capabilities from the inside.
9. Measure the ability of the router to handle very small packet fragments
10. Measure the ability of the router to handle over-sized packets
11. Measure the ability of the router to handle overlapped fragments such as that used in the TEARDROP attack

7. Trusted Systems Testing

The purpose of testing system trusts is to affect the Internet presence by posing as a trusted entity of the network. The testing scenario is often more theory than fact and does more than blur the line between vulnerability testing and Firewall/ACL testing, it is the line.

Expected Results:	Map of systems dependent upon other systems Map of applications with dependencies to other systems Types of vulnerabilities which affect the trusting systems and applications

1. Verify possible relationships determined from intelligence gathering, application testing, and services testing.
2. Test the relationships between various systems through spoofing or event triggering.
3. Verify which systems can be spoofed.
4. Verify which applications can be spoofed.

8. Access Control Testing

The firewall controls the flow of traffic between the enterprise network, the DMZ, and the Internet. It operates on a security policy and uses ACL's (Access Control Lists). This module is designed to assure that only that which should be expressly permitted be allowed into the network, all else should be denied. Additionally, the tester is to understand the configuration of the firewall and the mapping it provides through to the servers and services behind it.

Reviewing the server logs is needed to verify the tests performed on the Internet presence especially in cases where results of the tests are not immediately visible to the tester. Many unknowns are left to the analyst who has not reviewed the logs.

Expected Results:	Information on the firewall as a service and a system Information on the features implemented on the firewall Outline of the network security policy by the ACL List of the types of packets which may enter the network List of the types of protocols with access inside the network List of live systems found List of packets which entered the network by port number List of protocols which entered the network List of unmonitored paths into the network

Firewall and features identification

1. Verify the router type with information collected from intelligence gathering.
2. Verify if the router is providing network address translation (NAT)
3. Verify the penetrations from strategically determined packet TTL settings (Firewalking) completed in the Port Scanning module.

Verifying firewall ACL configuration

4. Test the ACL against the written security policy or against the "Deny All" rule.
5. Verify that the firewall is egress filtering local network traffic
6. Verify that the firewall is performing address spoof detection
7. Verify the penetrations from inverse scanning completed in the Port Scanning module.
8. Test the firewall outbound capabilities from the inside.
9. Determine the success of various packet response fingerprinting methods through the firewall
10. Verify the viability of SYN stealth scanning through the firewall for enumeration
11. Measure the use of scanning with specific source ports through the firewall for enumeration
12. Measure the ability of the firewall to handle overlapped fragments such as that used in the TEARDROP attack
13. Measure the ability of the firewall to handle tiny fragmented packets
14. Test the firewall's ability to manage an ongoing series of SYN packets coming in (flooding).
15. Test the firewall's response to packets with the RST flag set.
16. Test the firewall's management of standard UDP packets.
17. Verify the firewall's ability to screen enumeration techniques using ACK packets.
18. Verify the firewall's ability to screen enumeration techniques using FIN packets.
19. Verify the firewall's ability to screen enumeration techniques using NULL packets.
20. Verify the firewall's ability to screen enumeration techniques measuring the packet window size (WIN).
21. Verify the firewall's ability to screen enumeration techniques using all flags set (XMAS).

22. Verify the firewall's ability to screen enumeration techniques using IPIDs.
23. Verify the firewall's ability to screen enumeration techniques using encapsulated protocols.
24. Measure the robustness of firewall and it's susceptibility to denial of service attacks with sustained TCP connections.
25. Measure the robustness of firewall and it's susceptibility to denial of service attacks with temporal TCP connections.
26. Measure the robustness of firewall and it's susceptibility to denial of service attacks with streaming UDP.
27. Measure the firewall's response to all types of ICMP packets.

Reviewing firewall logs

28. Test the firewall logging process.
29. Verify TCP and UDP scanning to server logs.
30. Verify automated vulnerability scans.
31. Verify services' logging deficiencies.

9. Intrusion Detection System Testing

This test is focused on the performance and sensitivity of an IDS. Much of this testing cannot be properly achieved without access to the IDS logs. Some of these tests are also subject to attacker bandwidth, hop distance, and latency that will affect the outcome of these tests.

Reviewing the server logs is needed to verify the tests performed on the Internet presence especially in cases where results of the tests are not immediately visible to the tester. Many unknowns are left to the analyst who has not reviewed the logs and alerts.

Expected Results:	Type of IDS Note of IDS performance under heavy load Type of packets dropped or not scanned by the IDS Type of protocols dropped or not scanned by the IDS Note of reaction time and type of the IDS Note of IDS sensitivity Rule map of IDS List of IDS false positives List of IDS missed alarms List of unmonitored paths into the network

IDS and features identification

1. Verify the IDS type with information collected from intelligence gathering.
2. Determine its sphere of protection or influence.
3. Test the IDS for alarm states.
4. Test the signature sensitivity settings over 1 minute, 5 minutes, 60 minutes, and 24 hours.

Testing IDS configuration

5. Test the IDS for configured reactions to multiple, varied attacks (flood and swarm).
6. Test the IDS for configured reactions to obfuscated URLs and obfuscated exploit payloads.
7. Test the IDS for configured reactions to speed adjustments in packet sending.
8. Test the IDS for configured reactions to random speed adjustments during an attack.
9. Test the IDS for configured reactions to random protocol adjustments during an attack.
10. Test the IDS for configured reactions to random source adjustments during an attack.
11. Test the IDS for configured reactions to source port adjustments.
12. Test the IDS for the ability to handle fragmented packets.
13. Test the IDS for the ability to handle specific system method attacks.
14. Test the effect and reactions of the IDS against a single IP address versus various addresses.

Reviewing IDS logs and alerts

15. Match IDS alerts to vulnerability scans.
16. Match IDS alerts to password cracking.
17. Match IDS alerts to trusted system tests.

10. Containment Measures Testing

The containment measures dictate the handling of traversable, malicious programs and egressions. The identification of the security mechanisms and the response policy need to be targeted. It may be necessary to request first a new test mail account or desktop system that the administrator can monitor.

Expected Results:	Define Anti-Trojan Capabilities Define Anti-Virus Capabilities Identify Desktop Containment Measures Identify Desktop Containment Weaknesses List containment resources

1. Measure the minimum resources that need to be available to this subsystem in order for it to perform its task.
2. Verify the resources available to this subsystem that it does not need to perform its tasks, and what resources are shielded from use by this subsystem.
3. Verify the detection measures present for the detection of attempted access to the shielded resources.
4. Verify unneeded resources
5. Verify the features of the containment system.
6. Verify detection measures are present for detection of 'unusual' access to the 'needed' resources
7. Measure the response and process against the “sap 27” (see page 123 for the list).
8. Measure the configuration of the system.

11. Password Cracking

Password cracking is the process of validating password strength through the use of automated password recovery tools that expose either the application of weak cryptographic algorithms, incorrect implementation of cryptographic algorithms, or weak passwords due to human factors. This module should not be confused with password recovery via sniffing clear text channels, which may be a more simple means of subverting system security, but only due to unencrypted authentication mechanisms, not password weakness itself. [Note: This module could include manual password guessing techniques, which exploits default username and password combinations in applications or operating systems (e.g. Username: System Password: Test), or easy-to-guess passwords resulting from user error (e.g. Username: joe Password: joe). This may be a means of obtaining access to a system initially, perhaps even administrator or root access, but only due to educated guessing. Beyond manual password guessing with simple or default combinations, brute forcing passwords for such applications as Telnet, using scripts or custom programs, is almost not feasible due to prompt timeout values, even with multi-connection (i.e. simulated threading) brute force applications.]

Once gaining administrator or root privileges on a computer system, password cracking may assist in obtaining access to additional systems or applications (thanks to users with matching passwords on multiple systems) and is a valid technique that can be used for system leverage throughout a security test. Thorough or corporate-wide password cracking can also be performed as a simple after-action exercise and may highlight the need for stronger encryption algorithms for key systems storing passwords, as well as highlight a need for enforcing the use of stronger user passwords through stricter policy, automatic generation, or pluggable authentication modules (PAMs).

Expected Results:	Password file cracked or uncracked List of login IDs with user or system passwords List of systems vulnerable to crack attacks List of documents or files vulnerable to crack attacks List of systems with user or system login IDs using the same passwords

1. Obtain the password file from the system that stores usernames and passwords
   - For Unix systems, this will be either /etc/passwd or /etc/shadow
   - For Unix systems that happen to perform SMB authentication, you can find NT passwords in /etc/smbpasswd
   - For NT systems, this will be /winnt/repair/Sam._ (or other, more difficult to obtain variants)
2. Run an automated dictionary attack on the password file
3. Run a brute force attack on the password file as time and processing cycles allow
4. Use obtained passwords or their variations to access additional systems or applications
5. Run automated password crackers on encrypted files that are encountered (such as PDFs or Word documents) in an attempt to gather more intelligence and highlight the need for stronger document or file system encryption.
6. Verify password aging.

12. Denial of Service Testing

Denial of Service (DoS) is a situation where a circumstance, either intentionally or accidentally, prevents the system from functioning as intended. In certain cases, the system may be functioning exactly as designed however it was never intended to handle the load, scope, or parameters being imposed upon it.

It is very important that DoS testing receives additional support from the organization and is closely monitored. Flood and Distributed (DDoS) attacks are specifically not tested and forbidden to be tested as per this manual. Well resourced floods and DDoS attacks will ALWAYS cause certain problems and often not just to the target but also to all routers and systems between the tester and the target.

Expected Results:	List weak points in the Internet presence including single points of failure Establish a baseline for normal use List system behaviors to heavy use List DoS vulnerable systems

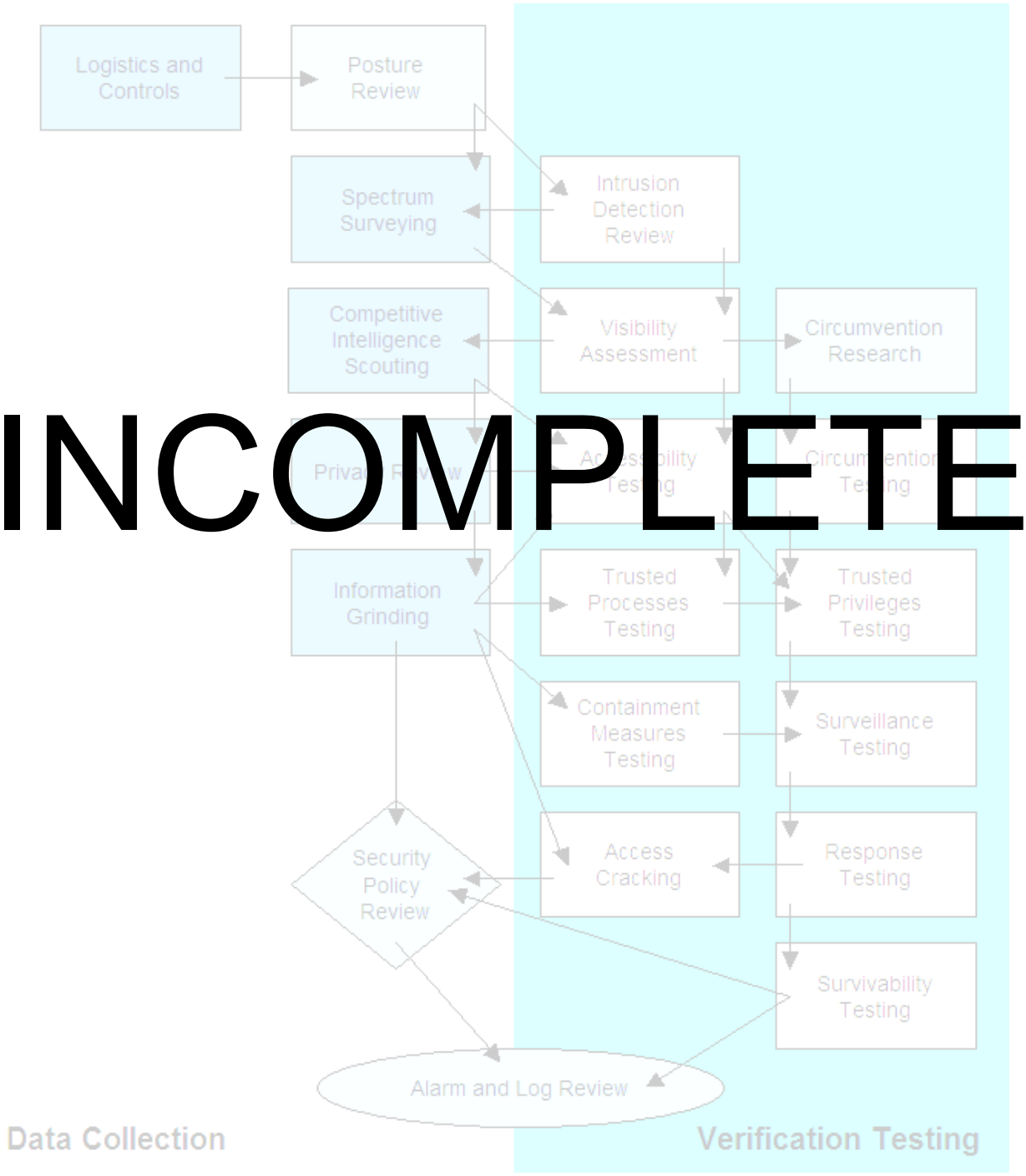
1. Verify that administrative accounts and system files and resources are secured properly and all access is granted with "Least Privilege".
2. Check the exposure restrictions of systems to non-trusted networks
3. Verify that baselines are established for normal system activity
4. Verify what procedures are in place to respond to irregular activity.
5. Verify the response to SIMULATED negative information (propaganda) attacks.
6. Test heavy server and network loads.

13. Security Policy Review

The security policy noted here is the written human-readable policy document outlining the mitigated risks an organization will handle with the use of specific types of technologies. This security policy may also be a human readable form of the ACL's. There are two functions to be performed: first, the testing of the written against the actual state of the Internet presence and other non internet related connections; and second, to assure that the policy exists within the business justifications of the organization, local, federal and international legal statutes, with particular respect to employer's and employee's rights and responsibilities and personal privacy ethics.
These tasks require that the testing and verification of vulnerabilities is completely done and that all other technical reviews have been performed. Unless this is done you can't compare your results with the policy that should be met by measures taken to protect the operating environment.

1. Measure the security policy points against the actual state of the Internet presence.
2. *Approval from Management* -- Look for any sign (e.g. signature) that reveals that the policy is approved by management. Without this approval the policy is useless because staff is not required to meet the rules outlined within. From a formal point of view you could stop investigating the policy if it is not approved by management. However, testing should continue to determine how effective the security measures are on the actual state of the internet presence.
3. Assure that the documentation is stored appropriately- electronically or otherwise, that the policy has been read and accepted by people before they are able to gain any access to the computer systems.
4. Identify incident handling procedures, to ensure that breaches are handled by the correct individual(s) and that they are reported in an appropriate manner.
5. *Inbound connections* -- Check out any risks mentioned on behalf of the Internet inbound connections (internet->DMZ, internet -> internal net) and measures which may be required to be implemented to reduce or eliminate those risks. These risks could be allowed on incoming connections, typically SMTP, POP3,HTTP, HTTPS, FTP, VPNs and the corresponding measures as authentication schemes, encryption and ACL. Specifically, rules that deny any stateful access to the internal net are often not met by the implementation.
6. *Outbound connections* -- Outbound connections could be between internal net and DMZ, as well as between internal net and the Internet. Look for any outbound rules that do not correspond to the implementation. Outbound connections could be used to inject malicious code or reveal internal specifics.
7. *Security measures* **--** Rules that require the implementation of security measures should be met. Those could be the use of AVS, IDS, firewalls, DMZs, routers and their proper configuration/implementation according to the outlined risks to be met.
8. Measure the security policy points against the actual state of non-Internet connections.
9. *Modems* -- There should be a rule indicating that the use of modems that are not specially secured is forbidden or at least only allowed if the modems are disconnected when not in use, and configured to disallow dial- in. Check whether a corresponding rule exists and whether the implementation follows the requirements.
10. *Fax machines* -- There should be a rule indicating that the use of fax machines which can allow access from the outside to the memory of the machines is forbidden or at least only allowed if the machines are powered down when not in use. Check whether a corresponding rule exists and whether the implementation follows the requirements.
11. *PBX* -- There should be a rule indicating that the remote administration of the PBX system is forbidden or at least only allowed if the machines are powered down when not in use. Check whether a corresponding rule exists and whether the implementation follows the requirements.
12. Measure the security policy against containment measures and social engineering tests based on the organization's employees' misuse of the Internet according to business justification and best security practices.

Section D – Communications Security



INCOMPLETE

Risk Assessment Values

Module	Cycle (days)	Degradation (%)	Influence (x)
Posture Review	Unavailable	Unavailable	Unavailable
PBX Review	Unavailable	Unavailable	Unavailable
Voicemail Testing	Unavailable	Unavailable	Unavailable
FAX Testing	Unavailable	Unavailable	Unavailable
Modem Survey	Unavailable	Unavailable	Unavailable
Remote Access Control Testing	Unavailable	Unavailable	Unavailable
Voice over IP Testing	Unavailable	Unavailable	Unavailable
X.25 Packet Switched Networks Testing	Unavailable	Unavailable	Unavailable

Modules

1. PBX Testing

This is a method of gaining access privileges to the telephone exchange of a target organization.

Expected Results:	Find PBX Systems that are allowing remote administration List systems allowing world access to the maintenance terminal List all listening and interactive telephony systems.

1. Review call detail logs for signs of abuse.
2. Ensure administrative accounts don't have default, or easily guessed, passwords.
3. Verify that OS is up-to-date and patched.
4. Check for remote maintenance access to system.
5. Test dial-in authentications.
6. Verify remote dial-in authentication.

2. Voicemail Testing

This is a method of gaining access privileges to the voicemail systems of the target organization and internal personnel.

Expected Results:	List of voice mailboxes that are world accessible List of voicemail dial-in codes and PINs

1. Verify PIN size and frequency of change
2. Identify user and organizational information
3. Check for remote maintenance access to system.
4. Test dial-in authentications.
5. Verify remote dial-in authentication.

3. FAX Review

This is a method of enumerating FAX machines and gaining access privileges to the systems which may host them.

Expected Results:	List of FAX systems List of FAX systems types and possible operating programs Compilation of information stored in memory of FAX machines Map of FAX usage protocol within the organization

1. Ensure administrative accounts don't have default, or easily guessed, passwords.
2. Test for FAX poling.
3. Check for remote maintenance access to system.
4. Test dial-in authentications.
5. Verify remote dial-in authentication.

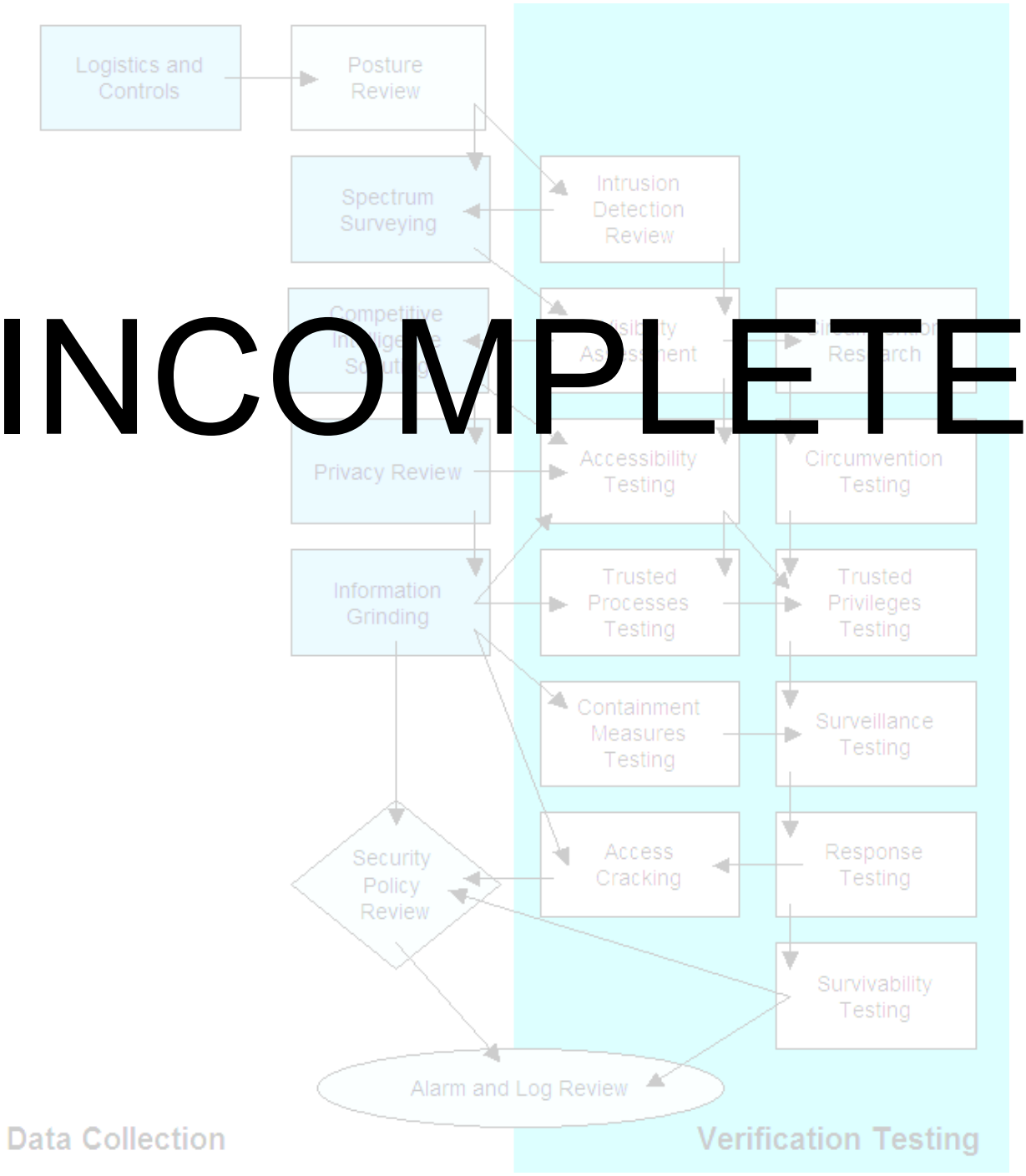
4. Modem Testing

This is a method of enumerating modems and gaining access privileges to the modem-enabled systems of a target organization.

Expected Results:	List of systems with listening modems List of modem types and operating programs List of modem authentication schemes List of modem logins and passwords Map of modem usage protocol within the organization

1. Scan the exchange for modems
2. Ensure accounts don't have default, or easily guessed, passwords.
3. Make sure OS and modem application is up-to-date and patched.
4. Check for remote maintenance access to system.
5. Test dial-in authentications.
6. Verify remote dial-in authentication.

Section E – Wireless Security



INCOMPLETE

Risk Assessment Values

Module	Cycle (days)	Degradation (%)	Influence (x)
Posture Review			
Electromagnetic Radiation (EMR) Testing	This should be performed on a new installation or whenever a new device is added to an existing, secure configuration.		
802.11 Wireless Networks testing	28 days	1.3%	
Bluetooth Networks Testing	28 days	1.3%	
Wireless Input Device Testing	60 days	2.8%	
Wireless Handheld Testing	60 days	2.8%	
Cordless Communications Testing	60 days	2.8%	
Wireless Surveillance Device Testing	This should be performed on a new installation or whenever a new device is added to an existing, secure configuration.		
Wireless Transaction Device Testing	This should be performed on a new installation or whenever a new device is added to an existing, secure configuration.		
RFID Testing	365 days		
Infrared Testing	120 days	.6%	
Privacy Review	70 days	2.1%	

Modules

1. Electromagnetic Radiation (EMR) 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 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.

Expected Results:	

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

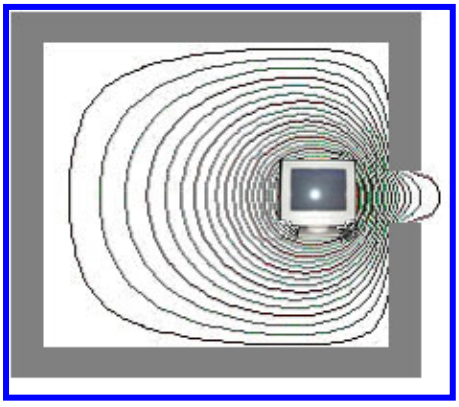
1. Verify that the organization has an adequate security policy in place to address EMR.

Evaluate Hardware and Placement

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

Evaluate and Test Wiring and Emissions

3. Verify that all wiring feeds into and out of the shielded room are made of fiber, where possible.



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:

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

Implementations:

802.11a
- Operates in the 5GHz frequency range
- Not compatible with 802.llb 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

Expected Results:	

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.

Evaluate Hardware, Firmware, and Updates.

6. Perform a complete inventory of all wireless devices on the network.

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

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

Evaluate Administrative Access to Wireless Devices:

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

Evaluate Configuration, Authentication and Encryption of Wireless Networks:

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

Evaluate Wireless Clients:

10. Verify that all wireless clients have antivirus software installed.

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	• Three modes of security (none, link-level, and service-level) • Two levels of device trust and three levels of service security. • Stream encryption algorithm for confidentiality and authentication. • PIN derived keys and limited key management.
Operating Range	About 10 meters (30 feet); can be extended to 100 meters (328 feet).

Expected Results:	

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.

Evaluate Hardware, Firmware, and Updates.

2. Perform a complete inventory of all Bluetooth enabled wireless devices.

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

3. 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.

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

4. Verify the actual perimeter of the Bluetooth network.

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

5. 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.

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.

Expected Results:	

Evaluate Business Needs, Practices, and Policies:

1. Analyze organizational security policy that addresses the use of wireless technology, such as wireless input devices.

Evaluate Hardware, Firmware, and Updates:

2. Perform a complete inventory of all wireless input devices on the network.

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

3. Perform a site survey to measure and establish the service range of the wireless input devices for the organization.

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.

Expected Results:	

Evaluate Business Needs, Practices, and Policies:

1. Verify that there is an organizational security policy that addresses the use of all handheld devices.

Evaluate Hardware, Firmware, and Updates:

2. Perform a complete inventory of all wireless devices on the network.

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

3. Verify that there is external boundary protection around the perimeter of the buildings, or wireless networks.

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

4. Verify that the devices use robust encryption to protect sensitive files and applications.

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.

Expected Results:	

Evaluate Business Needs, Practices, and Policies:

1. Verify that the organization has an adequate security policy that addresses the use of cordless communication technology.

Evaluate Hardware, Firmware, and Configuration:

2. Perform an inventory of all cordless communication devices.

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

3. Verify the distance in which the cordless communication extends beyond the physical boundaries of the organization.

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.

Expected Results:	

Evaluate Business Needs, Practices, and Policies:

1. Verify that there is a company policy that effectively addresses wireless surveillance equipment.

Evaluate Devices and Placement:

2. Verify that the surveillance equipment is truly disguised or not visible, if that is the intent of the equipment.

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

3. Verify the actual perimeter of the wireless surveillance device transmissions.

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.

Expected Results:	

Evaluate Business Needs, Practices, and Policies:

1. Verify that there is a company policy that effectively addresses wireless transaction equipment.

Evaluate Hardware, Firmware, and Updates:

2. Perform a full inventory of all wireless transaction devices.

Evaluate Device Configuration:

3. Verify that that the data being sent is encrypted and the level of encryption being used.

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

4. Determine the ability of unintended third to intercept transmitted 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. TFID 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.

Expected Results:	

Evaluate Business Needs, Practices, and Policies:

1. Verify that the organization has an adequate security policy that addresses the use of wireless RFIDs.

Evaluate RFID Attributes (Authentication, Encryption, Properties…):

2. Verify that serial number on ID tag cannot be changed.

Evaluate Placement, Scanners, and Tracking Equipment:

3. 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.

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

4. Verify that RFID tag and reader transmissions do not interfere with wireless networks and communications equipment.

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.

Expected Results:	

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.

Evaluate Hardware, Firmware, and Updates:

2. Perform a complete audit of all infrared enabled devices.

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

3. Verify the distance that the infrared communication extends beyond the physical boundaries of the organization.

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

4. Verify authentication-method of the clients.

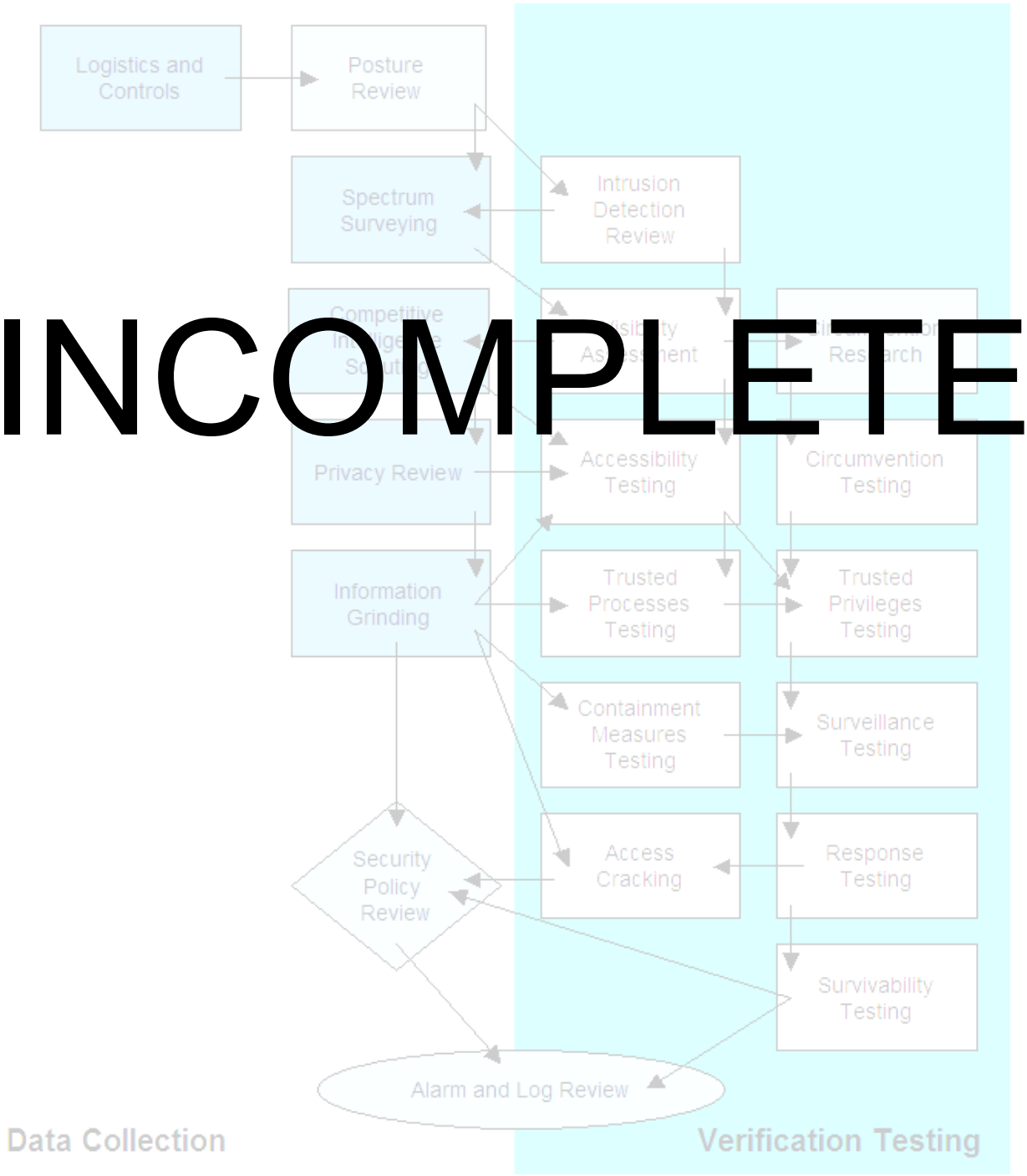
11. Privacy Review

The privacy of wireless communication devices may exceed the physical and monitored boundaries of an organization. The privacy review is the focal point of the legal and ethical storage, transmission, and control of data based on employee and customer privacy. The use of this data is a concern to many private persons and legislation is unveiling specific rules regarding privacy. Although some of these laws are local, all of them apply to the Internet and therefore affect security testers internationally.

Expected Results:	List any disclosures List compliance failures between public policy and actual practice List wireless communication involved in data gathering List data gathering techniques List data gathered

1. Verify authentication-method of the clients
2. Verify that appropriately strong passwords are in use
3. Verify that that there is a password expiration policy
4. Verify that encryption is used and properly configured
5. Verify that clients can't be forced to fall-back to none-encrypted mode
6. Compare publicly accessible policy to actual practice
7. Compare actual practice to regional fraud and privacy laws or compliancy
8. Identify database type and size for storing data
9. Identify data collected by the organization
10. Identify storage location of data
11. Identify data expiration times

Section F – Physical Security



INCOMPLETE

Risk Assessment Values

Module	Cycle (days)	Degradation (%)	Influence (x)
Posture Review	Unavailable	Unavailable	Unavailable
Access Controls Testing	Unavailable	Unavailable	Unavailable
Perimeter Review	Unavailable	Unavailable	Unavailable
Monitoring Review	Unavailable	Unavailable	Unavailable
Alarm Response Review	Unavailable	Unavailable	Unavailable
Location Review	Unavailable	Unavailable	Unavailable
Environment Review	Unavailable	Unavailable	Unavailable

Modules

1. Perimeter Review

This is a method of testing the physical security of an organization and its assets by reviewing is its physical perimeter security measures.

Expected Results:	Map of physical perimeter Types of physical protective measures List of unprotected / weakly protected areas

1. Map physical perimeter
2. Map physical protective measures (fences, gates, lights, etc)
3. Map physical access routes / methods
4. Map unmonitored areas

2. Monitoring Review

This is a method of discovering monitored access points to an organization and its assets through discovery of guard and electronic monitoring.

Expected Results:	List of monitored access points Types of monitoring List of unmonitored standard and privileged access points List of alarm triggers

1. Enumerate monitoring devices
2. Map guarded locations and routes traveled
3. Map unmonitored areas to monitored areas
4. Test monitoring devices for limitations and weaknesses
5. Test monitoring devices for denial of service attacks

3. Access Controls Testing

This is a method of testing access privileges to an organization and its assets through physical access points.

Expected Results:	List of physical access points Types of authentication Types of alarm systems List of alarm triggers

1. Enumerate access control areas
2. Examine access control devices and types
3. Examine alarm types
4. Determine the level of complexity in an access control device
5. Determine the level of privacy in an access control device
6. Test access control devices for vulnerabilities and weaknesses
7. Test access control devices against Denial of Service

4. Alarm Response Review

This is a method of discovering alarm procedure and equipment in an organization through discovery of guard and electronic monitoring.

Expected Results:	List of alarm types List of alarm triggers Map of alarm procedure List of persons involved in alarm procedure List of containment measures and safety precautions triggered by alarm

1. Enumerate alarm devices
2. Map alarm trigger procedures
3. Map alarm activated security reflexes
4. Discover persons involved in an alarm procedure
5. Test alarm escalation
6. Test alarm enablement and disablement
7. Test alarm devices for limitations and weaknesses
8. Test alarm devices for denial of service attacks
9. Test alarm procedures for Denial of Service attacks

5. Location Review

This is a method of gaining access to an organization or its assets through weaknesses in its location and protection from outside elements.

Expected Results:	Map of physical locations of assets List of physical location access points List of vulnerable access points in location List of external 3rd parties accessing locations

1. Enumerate visible areas into the organization (line of sight)
2. Enumerate audible areas into the organization (laser or electronic ear)
3. Test location areas for vulnerabilities and weaknesses to supply delivery
4. List supply delivery persons and organizations
5. List cleaning staff and organizations
6. List hours and days in delivery cycles
7. List hours and days in visitor cycles

6. Environment Review

This is a method of gaining access to or harming an organization or its assets through weaknesses in its environment.

Expected Results:	Map of physical locations of assets List of vulnerable locations List of local laws, customs, and ethics List of operational laws, customs, and ethics

1. Examine natural disaster conditions for the region
2. Examine political environmental conditions
3. Examine back-up and recovery procedures
4. Identify weaknesses and vulnerabilities in back-up and recovery procedures
5. Identify Denial of Service attacks in back-up and recovery procedures
6. Examine physical and electronic handicaps in various weather patterns
7. Compare operational procedures with regional laws, customs, and ethics

Report Requirements Templates

The following templates are an small example of the report requirements as per what should be displayed in a report to qualify for a certified OSSTMM compliancy stamp. Restrictions of applicability and scope apply.

Network Profile Template

IP ranges to be tested and details of these ranges

Domain information and configurations

Zone Transfer Highlights

SERVER LIST

IP Address	Domain Name(s)	Operating System

Server Information Template

IP Address	domain name

Port	Protocol	Service	Service Details

BANNER(S):

Port	Protocol	Banner

TCP SEQUENCING:

TCP Sequence Prediction
TCP ISN Seq. Numbers
IPID Sequence Generation
Uptime

CONCERNS AND VULNERABILITIES:

Concern or Vulnerability
Example
Solution

Firewall Analysis Template

fingerprinting
This test is to determine the success of various packet response fingerprinting methods through the firewall.

Method	Result

stealth
This determines the viability of SYN stealth scanning through the firewall for enumeration.

Result

source port control
This test measures the use of scanning with specific source ports through the firewall for enumeration.

Protocol	Source	Result
UDP	53	
UDP	161	
TCP	53	
TCP	69	

overlap
This test measures the ability of the firewall to handle overlapped fragments such as that used in the TEARDROP attack.

Protocol	Result

fragments
This test measures the ability of the firewall to handle tiny fragmented packets.

IP	Result

syn flood
This tests the firewall's ability to manage an ongoing series of SYN packets coming in.

IP	Result

rst flag
This test exacts the firewall's response to packets with the RST flag set.

IP	Result

udp
This tests the firewall's management of standard UDP packets.

IP	Result

ack
This test is to discover the firewall's ability to screen enumeration techniques using ACK packets.

IP	Result

fin
This test is to discover the firewall's ability to screen enumeration techniques using FIN packets.

IP	Result

null
This test is to discover the firewall's ability to screen enumeration techniques using NULL packets.

IP	Result

win
This test is to discover the firewall's ability to screen enumeration techniques using WIN packets.

IP	Result

xmas
This test is to discover the firewall's ability to screen enumeration techniques using packets with all flags set.

IP	Result

Advanced Firewall Testing Template

Sustained TCP Connections
This test is to measure the robustness of firewall and it's susceptibility to denial of service attacks.

connection	description	max connects	max idle time

Fleeting TCP Connections
This test is to measure the robustness of firewall and it's susceptibility to denial of service attacks.

connection	description	max connects	max idle time

Streaming UDP Throughput
This test is to measure the robustness of firewall and it's susceptibility to denial of service attacks.

connection	description	max connects

ICMP Responses
This test is to measure the firewall's response to various types of ICMP packets.

type	type description	response	RTT

Spoof Responses
This test is to measure the firewall's Access Control List rules by IP address.

connection	response description	from	to

Protocol
This test is to discover the firewall's ability to screen packets of various protocols.

Protocol	Result

IDS Test Template

IDS type
This test is to determine the IDS type and sphere of protection or influence.

IDS type	protection range by IP

Flood Attack
This test is to measure the IDS´s response capabilities in the event of many attacks of various priorities coming through at once.

flood type	description of attack	duration	result

Obfuscated URLs
This test addresses the IDS's ability to address disguised URLs for attacking web servers.

encoding type	URL sent	result

Speed Adjustments
This test measures the IDS's sensitivity to scans over definitive time periods.

	packet description	delay	result
1 minute			
5 minutes			
60 minutes			
24 hours			

Behavior Attacks
This test measures the IDS's sensitivity to many scans of a random nature.

	description	result
random speed attack		
random protocol attack		
random source attack		

Method Matching
This test measures the IDS's sensitivity to web server scans of unknown methods.

	result
HEAD	
POST	
PUT	
DELETE	
PATCH	
PROPFIND	
PROPPATCH	
MKCOL	
COPY	
MOVE	
LOCK	
UNLOCK	

Source Port Control
This test measures the use of scanning with specific source ports through the IDS without alarm.

Protocol	Source	Result
UDP	53	
UDP	161	
TCP	443	
TCP	22	

Spoof Responses
This test is to measure the firewall's Access Control List rules by IP address.

connection	response description	from	to

Fragments
This test measures the ability of the IDS to handle tiny fragmented packets.

Result

Social Engineering Target Template

Target Definition

Name	E-mail	Telephone	Description

Social Engineering Telephone Attack Template

Attack Scenario	
Telephone #	
Person	
Description	
Results	

Attack Scenario	
Telephone #	
Person	
Description	
Results	

Social Engineering E-mail Attack Template

Attack Scenario	
Email	
Person	
Description	
Results	

Attack Scenario	
Email	
Person	
Description	
Results	

Trust Analysis Template

IP Address	Domain Name
Description of Trust	

IP Address	Domain Name
Description of Trust	

IP Address	Domain Name
Description of Trust	

Privacy Review Template

IP Address	Domain Name
Privacy Policy	
Privacy Violations	

IP Address	Domain Name
Privacy Policy	
Privacy Violations	

Containment Measures Review Template

IP Address	Domain Name
Server Anti-virus / Anti-Trojan Mechanisms	
Server Response to “SAP 27” and 42.zip	

Desktop Anti-virus / Anti-Trojan Mechanisms

Desktop Mail Client Types
Desktop Mail Client Vulnerabilities

Desktop Browser Client Types
Desktop Browser Client Vulnerabilities

E-Mail Spoofing Template

Attempts

Internal Connect

Show the results of a telnet to the mail server and sending a mail from one internal address to another internal address.

Egression

Show the results of sending a mail from one internal address to another internal address using an external, third-party pop server.

External Relaying

Show the results of sending a mail from one external address to another external address using the target mail server.

Internal Relaying

Show the results of sending a mail from one internal address to an external address using the target mail server.

Competitive Intelligence Template

IP Address	
Domain Names	
Similar Domain Names	
Total Content Size	
Number of Documents	
Number of Products	
Product List	
Number of Services	
Services List	
Method of Sales	
Restricted Areas	

Password Cracking Template

Protected File

File name	
File type	
Crack time	
User name	
Password	

Encoded Password File

IP Address	
Service Port	
Service Type	
Protocol	
File name	
File type	
Crack time	
Login Names	
Passwords	

Protected Online Service

IP Address	
Service Port	
Service Type	
Protocol	
Login Names	
Passwords	

Denial of Service Template

System Testing

IP Address	
Service Port	
Service Type	
Protocol	
Test Description	
Test Response	

IP Address	
Service Port	
Service Type	
Protocol	
Test Description	
Test Response	

Process Testing

Process	
Persons	
Location	
Time / Date	
Test Description	
Test Response	

Process	
Persons	
Location	
Time / Date	
Test Description	
Test Response	

Document Grinding Template

Primary Contacts	
Method of Contact	

Organizational Information	
Business Name	
Business Address	
Business Telephone	
Business Fax	
Hierarchy Model	
Office Hierarchy	
Line of Business	
Operations	
Legal Structure	
Year Started	
Company History	
Departments and Responsibilities	
Telecommunications Information	
Noted Business Phone Numbers	

Phone Number Block	
Phone Number Type	
Number of Modems	
Modem Phone Numbers	
Modem Connect Speeds	
Number of Fax Machines	
Fax Phone Numbers	
Unusual Phone Numbers	

Employee Data	
Employee Names and Positions	
Employee Personal Pages	
Employee Information	

Outsourcers	
Web Designers	
Email	
Tech Support	
Firewall	
Intrusion Detection System	

Help Desk	
Partners	
Resellers	
Internet Service Providers	
Application Service Providers	

IP Information	
Domain Names	
Network Blocks	
Network Block Owner	
Records Created	
Records Last Updated	

Internal Network Information	
Number of Network Accounts	
Network Account Standard	
Network Account Creation Standard	
Web Clients Used	
Screen Size	
Security Settings in Browser	

Internal System Information	
Number of Systems	
System Names Standard	
System Names	
Types of Systems	
Operating Systems	
Services provided	

Email Information	
Email Server Address	
Email Server Type	
Email Clients	
Email System	
Email Address Standard	
E-mail Footer	
Encryption / Standard	
Bounced mails	
SMTP server path	
Automatic Vacation Returns	
Mailing Lists	

Web Information	
Website Address	
Web Server Type	
Server Locations	
Dates Listed	
Date Last Modified	
Web Links Internal	
Web Site Searchability	
Web Links External	
Web Server Directory Tree	
Technologies Used	
Encryption standards	
Web-Enabled Languages	
Form Fields	
Form Variables	
Method of Form Postings	
Keywords Used	

Company contactability	
Meta Tags	
Comments Noted	
e-commerce Capabilities	
Services Offered on Net	
Products Offered on Net	
Features	
Search Engines Identified	
Search Engine Ranking	
Daily/Weekly/Monthly Hits	
Link Popularity	
Link Culture	

File Management Information	
FTP Server Address	
SMB Server Address	
Server Location	
Server Type	
Directory Tree	

Files Sitting	

Name Services	
Primary (Authoritative) Name Server	
Secondary	
Last Update	
Additional Name Servers	

Firewall Information	
Firewall Address	
Firewall Type	
IDS system	

Routing Information	
Router Addresses	
Router Types	
Router Capabilities	

Virtual Private Network Information	
VPN Capabilities	
VPN Type	

Network Services	
Network Services Noted	

Internet Presence Information	
Newsgroup Postings	
Bulletin Board Postings	
Business Wire Postings	

Help Wanted Ads	
P2P Files	
Cracks Found	
Serial Numbers Found	

Competitive Intelligence	
Customer List	
Target Market	
Product List	

Social Engineering Template

Company	
Company Name	
Company Address	
Company Telephone	
Company Fax	
Company Webpage	
Products and Services	
Primary Contacts	
Departments and Responsibilities	
Company Facilities Location	
Company History	
Partners	
Resellers	
Company Regulations	
Company Info security Policy	
Company Traditions	
Company Job Postings	
Temporary Employment Availability	
Typical IT threats	

People	
Employee Information	
Employee Names and Positions	
Employee Place in Hierarchy	
Employee Personal Pages	
Employee Best Contact Methods	
Employee Hobbies	
Employee Internet Traces (Usenet, forums)	
Employee Opinions Expressed	
Employee Friends and Relatives	
Employee History (including Work History)	
Employee Character Traits	
Employee Values and Priorities	
Employee Social Habits	
Employee Speech and Speaking Patterns	
Employee Gestures and Manners	

Equipment	
Equipment Used	
Servers, Number and Type	
Workstations, Number and Type	
Software used (with versions)	
Hostnames Used	
Network Topology	
Anti-virus Capabilities	
Network Protection Facilities Used (with software versions)	
Remote Access Facilities Used (including Dial-up)	
Routers Used (with software versions)	
Physical Access Control Technology Used	
Location of Trash Disposal Facilities	

Legal Penetration Testing Checklist

FEATURES TO CONSIDER	APPLICABLE LAW
PRIVACY AND PROTECTION OF INFORMATION	
Obtaining and Using Personal Information. • Personal information about living people should only be obtained and used if is necessary for the purposes of a security test and it is legally permissible. • Certain conditions may need to be satisfied where personal information is obtained and used; these conditions will vary from country to country and could include: - obtaining the consent from the individual whose information is being obtained and used; - or the information is necessary for the prevention and detection of a crime.	International variations exist in relation to obtaining and processing personal data. There is a level of consistency between countries from the European Community, who have implemented Directive 95/46/EC of the European Parliament and of the Council on the protection of personal data with regard to the processing of personal data and of the free movement of such data (OJ [1995] L281/31). The UK's Data Protection Act 1998, which was partly based upon the Directive 95/46/EC expressly requires that personal data shall only be obtained and processed fairly and lawfully. A range of conditions need to be satisfied to demonstrate compliance with the Data Protection Act.
Copying, Storing, Retention and Destruction of Information. • Information belonging to others should only be copied and retained by the Security Testers where it is relevant and necessary for analysis and reporting purposes; unless such activities are expressly prohibited by the contract or by law. • Information belonging to others should only be kept for as long as is necessary for the purposes of testing and reporting. • Information that was legally obtained and deemed necessary for the purposes of the test should be destroyed in an appropriate manner when it is no longer required.	The legal requirements for handling information vary from country to country. Consistency exists between countries from the European Community who are subject to Directive 95/46/EC. - The UK's Data Protection Act 1998, which was partly based upon the Directive 95/46/EC expressly requires that personal data should not be kept for longer than is necessary and that adequate and appropriate security measures should be used to protect personal information. - Where a US company wishes to share personal information with a company subject to Directive 95/46/EC, the US company must adhere to the safe harbor requirements.
Disclosure of Information. • Information should not be disclosed to unauthorized individuals. • The Security Tester should ensure that an individual's privacy rights are respected, where necessary. • A Security Tester must not act in any manner which could result in a breach of confidentiality or contravention of any law or contract.	There are various rules that exist to protect information from unauthorized disclosed. These rules may be necessary to protect commercial confidentiality or an individual's privacy. - The European Community countries have adopted the European Convention of Human Rights in to their national laws. - The UK's Human Rights Act 1998 incorporates the Convention right of privacy, article 8. The Data Protection Act 1998

	requires that a minimum level of protection is used. - The United Nations Declaration of Human Rights at article 12, states that every individual has a right to privacy.

INFORMATION AND SYSTEM INTEGRITY	
Unauthorized interference with information systems. • Security Testers must not intentionally cause interference to the operation of their customer's information system, unless they are permitted by law or their customer. • Written consent may be required from the customer prior to performance of the Security Test.	Interference with information systems may be governed by a range of different laws internationally. Although it is a feature that may be incorporated as a contractual term. In the UK it is necessary to closely scrutinize the act of the perpetrator, who may be punished under range of legislation such as the Computer Misuse Act, the Theft Act or the Criminal Damages Act.
Damage and Modification of information or information systems • Security Testers should take care not to alter or damage any information or information systems during testing; except where permissible by law or the contracting party.	The alteration, modification or damage of information by the Security Testers may be a either a criminal or civil offence or both depending on the country. - In the UK, it is governed by the Computer Misuse Act and the Criminal Damages Act.
Unauthorized use of information or information systems. • There should be no unauthorized use of information or systems; except where permissible by law.	Information and the information systems may need to be protected from others for a wide range of reasons; such as maintaining client confidentiality or protecting companies research and development.

COMMUNICATION AND AUTHORISATION	
Notification of intention and actions. • Appropriate notices should be provided to the customer and any others with a legal right to know about the impact of a Security Test; • The Security Testers must provide the customer with the necessary detail of the actions that will be taken as part of the Test; • If any hackers are discovered on the customer's system during the Security Test, then the Testers should inform the customer as soon as it is possible.	It may be a legal requirement in some countries to receive notification of intentions and actions in relation to the Security Test. In the UK Security Testers may be liable for a variety of reasons if they fail to provide the appropriate notifications. They could breach a contractual requirement, be deemed negligent or infringe legislation such as the Computer Misuse Act 1990.

• All parties that may be effected by the Internet Security Test have been informed of the nature of the Test where legally necessary.	
Notification of Responsibilities • The Security Testers should ensure that their customers are aware of their responsibilities, which include: - taking back ups of information prior to the test; - and informing employees who need to know, for legal or operational purposes.	This is a general due diligence requirement, which may apply internationally.
Authorization • Written permission may be necessary from the customer before the Security Test is undertaken; • Consent may be required from individuals or organizations other than the customer before the Security Test is performed;	Conducting a Security Test written the appropriate authorization could be a criminal or civil offence depending on the country or countries of the test. - it is the Computer Misuse Act 1990 in the UK which makes it an offence to access a system without authority.
Suspension of the Security Test • If an intruder is discovered on the customer's information system during the Security Test, then the test should be suspended and the incident reported to the customer. Following suspension, the Security Test should only be re-commenced with the agreement of the customer.	Any Security Tester needs to act with caution otherwise they could be liable for a range of misdemeanors. In particular care needs to be exercised when intruders are discovered as the Security Tester does not want to be blamed for the actions of the intruder.

CONTRACT	
Contract formation and terms and conditions • Ensure that contracts are formed in compliance with the law; • The terms and conditions for the provision of Security Testing should be sufficiently detailed to reflect the rights and responsibilities of the tester and customer.	The use of contracts is an internationally accepted practice. There are differences between countries with contract law and these should be addressed if contracting with organizations from other countries. - In the UK guidance on contractual formation can be taken from legislation such as the Supply of Goods and Services Act 1982. This Act provides for the existence of implied terms in contracts such as the implied term that a service will be carried out with reasonable care and skill.

Liability • Ensure appropriate and legally acceptable clauses limiting liability exist in a contract. - For example a clause should exist that states that the Security Tester will not accept responsibility or liability for any damage or loss incurred as a result of the customer's failure to implement the appropriate safeguards to protect the information systems or any connected part of it.	There are international variations with the content of liability clauses. - With issues of liability the UK is subject to legislation such as the Unfair Contract Terms Act 1977.
Contents • It may be necessary to ensure that specific information necessary for the test is included with any contractual documents such as: - a list of all the assigned IP addresses which must be expressed as an individual IP address and as a range.	Providing details of the scope and parameters of the Security Test protects the customer and the Tester.

Test References

The following are key references for use with this manual in testing.

sap 27

The sap or “sucker” 27 are various extensions which are used in the wild for attempting to move groaned code in through e-mail systems and browsers.

EXT.	DESCRIPTION
.ade	Microsoft Access Project extension
.adp	Microsoft Access Project
.bat	Batch file
.chm	Compiled HTML Help file
.cmd	Microsoft Windows NT Command script
.com	Microsoft MS-DOS program
.cpl	Control Panel extension
.crt	Security Certificate
.eml	Outlook Express Mail
.exe	Program
.hlp	Help file
.hta	HTML program
.inf	Setup Information
.ins	Internet Naming Service
.jpg	JPEG image
.isp	Internet Communication Settings
.js	JScript file
.jse	JScript Encoded Script file
.mdb	Microsoft Access program
.mde	Microsoft Access MDE database
.msc	Microsoft Common Console document
.msi	Microsoft Windows Installer package
.msp	Microsoft Windows Installer patch
.mst	Microsoft Visual Test source files
.pcd	Photo CD Image, MS Visual compiled script
.pif	Shortcut to MS-DOS program
.reg	Registration entries
.scr	Screen Saver
.sct	Windows Script Component
.shb	Shell Scrap Object
.shs	Shell Scrap Object
.url	HTML page
.vb	VBScript file
.vbe	VBScript Encoded Script file
.vbs	VBScript file
.wav	Sound File
.wsc	Windows Script Component
.wsf	Windows Script file
.wsh	Windows Script Host Settings file

Protocols

An extension of the original OSSTMM Internet protocols list, the OPRP is a single resource for information on Internet and network protocols, transport information, and specifications. This resource is essential to thorough security testing.

This can be found on the ISECOM website at the following URL:

http://www.isecom.org/projects/protocolresource.htm

Open Methodology License (OML)

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 PESONS 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.