

OSSTMM 3

OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL

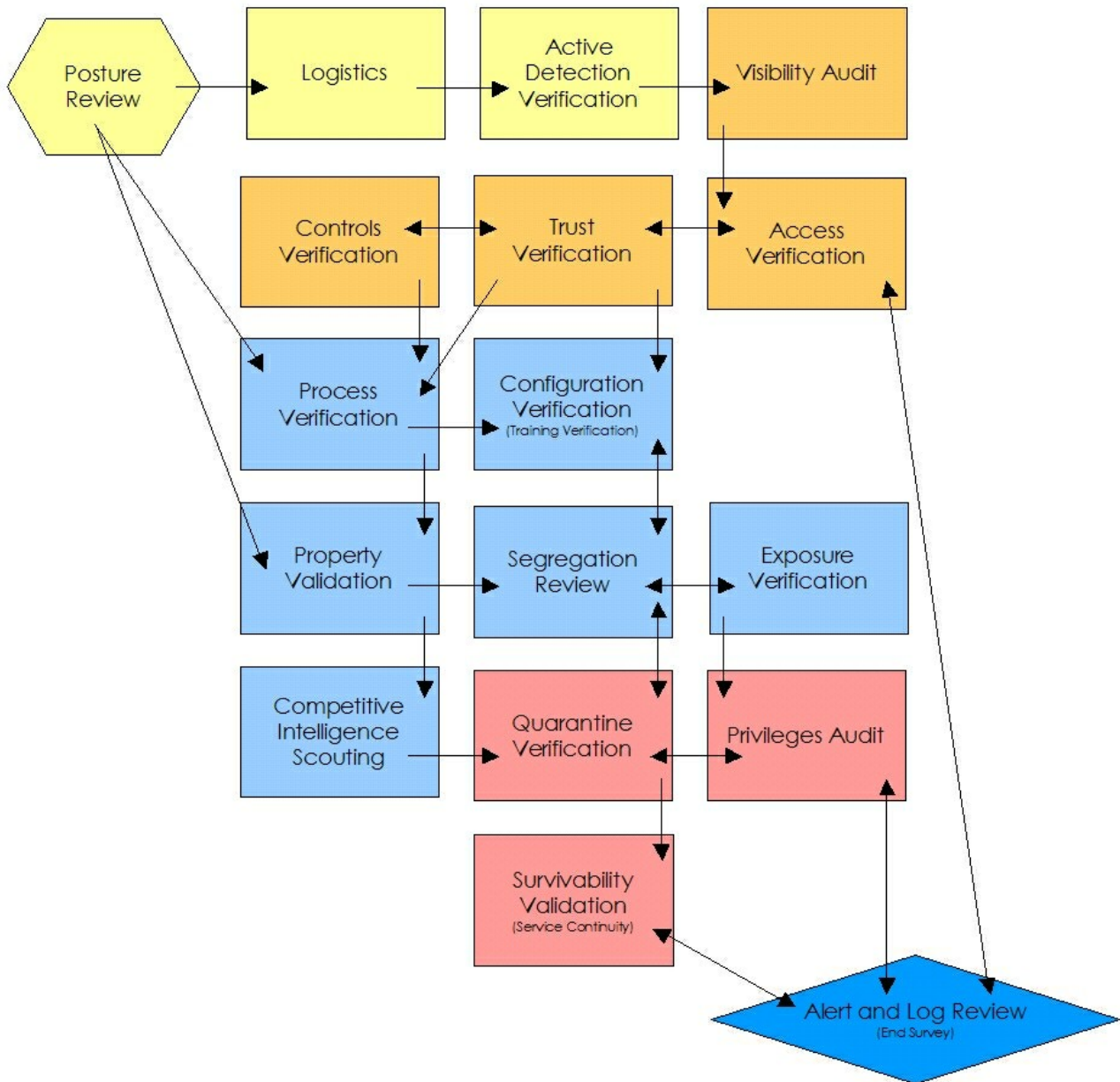
HUMAN SECURITY DRAFT

Release Candidate
Pending Peer Review and Final Review

Created by Pete Herzog

Table of Contents

Chapter 7 - Human Security.....	4
PHYSSEC – HUMSEC - PSYOPS.....	4
Considerations.....	4
1.1 Posture Review.....	5
1.2 Logistics.....	5
1.3 Active Detection Verification.....	6
1.4 Visibility Audit.....	6
1.5 Controls Verification	7
1.6 Trust Verification	7
1.7 Access Verification	8
1.8 Process Verification.....	9
1.9 Training Verification.....	9
1.10 Property Validation.....	10
1.11 Segregation Review.....	10
1.12 Exposure Verification.....	11
1.13 Competitive Intelligence Scouting.....	11
1.14 Quarantine Verification.....	12
1.15 Privileges Audit.....	12
1.16 Service Continuity.....	13
1.17 End Survey.....	13
Chapter 12 - Open Methodology License (OML).....	15



Chapter 7 - Human Security

PHYSSEC – HUMSEC - PSYOPS

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

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

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

Competent auditors will require both diligent people skills and critical thinking skills to assure factual data collection creates factual results through correlation and analysis.

Considerations

1. In personam: Scope restrictions are to target those personnel who are under direct legal contract with the scope owner and therefore legal responsibility for their security awareness and obligations.
2. Plausible Deniability: No direct personnel security testing will take place for personnel who have not been trained, informed, or can be said to possess having security awareness experience or obligations due to job responsibility requirements.
3. Human Rights: Where personnel to be tested are randomly chosen and/or are not said to have job responsibilities directly related to gate keeping, security, or safety, the auditor will refrain from personally identifying the person and report solely on a statistical basis.

1.1 Posture Review

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

1.1.1 Policy

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

1.1.2 Legislation

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

1.1.3 Culture

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

1.1.4 Relationships

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

1.1.5 Regional Culture

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

1.1.6 Economics

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

1.2 Logistics

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

1.2.1 Communications Equipment

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

1.2.2 Communications

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

1.2.3 Time

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

1.3 Active Detection Verification

Determination of active and passive controls to detect intrusion to filter or deny test attempts must be made prior to testing or risk creating false positives and negatives in the test result data as well as changing the alarm status of monitoring personnel or agents.

1.3.1 Channel Monitoring

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

1.3.2 Channel Moderating

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

1.3.3 Supervision

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

1.3.4 Operator Assistance

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

1.4 Visibility Audit

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

1.4.1 Access Identification

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

1.4.2 Personnel Enumeration

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

1.5 Controls Verification

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

1.5.1 Non-repudiation

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

1.5.2 Confidentiality

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

1.5.3 Privacy

Enumerate and test for use of or inadequacies from all segments of communication with personnel within the scope over a channel and/or properties transported using specific, individual signatures, personal identification, or "quieted" or "closed room" personal interactions to protect the privacy of the interaction and the process of providing property only to those within the proper security clearance for that process, information, or physical property.

1.5.4 Integrity

Enumerate and test for inadequacies in all segments of communication with personnel within the scope over a channel and/or assets transported over a channel using a documented process, signatures, encryption, hash, or markings to protect to assure that the

information or physical property cannot be changed, continued, redirected, or reversed without it being known to parties involved.

1.6 Trust Verification

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

1.6.1 Misrepresentation

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

1.6.2 Fraud

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

1.6.3 Misdirection

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

1.6.4 Phishing

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

1.6.5 Resource Abuse

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

1.7 Access Verification

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

personnel in their private life.

1.7.1 Access Process

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

1.7.2 Authority

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

1.7.3 Authentication

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

1.8 Process Verification

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

1.8.1 Maintenance

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

1.8.2 Misinformation

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

1.8.3 Due Diligence

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

1.8.4 Indemnification

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

1.9 Training Verification

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

1.9.1 Education Mapping

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

1.9.2 Policy Disruption

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

1.9.3 Awareness Mapping

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

1.9.4 Awareness Hijacking

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

1.10 Property Validation

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

1.10.1 Sharing

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

1.10.2 Black Market

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

1.10.3 Sales Channels

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

1.11 Segregation Review

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

1.11.1 Privacy Containment Mapping

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

1.11.2 Evident Information

Enumerate and map from individual gateway personnel their information such as names, race, sex, religion, vacation days, personal home pages, published resumes, personal affiliations, directory inquiries, bank branch, electoral register, and any particular personal information stated implicitly as private in regulations and policy.

1.11.3 Disclosure

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

1.11.4 Limitations

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

1.12 Exposure Verification

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

1.12.1 Exposure Mapping

Enumerate and map personnel information regarding the organization such as organization charts, key personnel titles, job descriptions, personal and work telephone numbers, mobile

phone numbers, business cards, shared documents, resumes, organizational affiliations, private and public e-mail addresses, logins, login schemes, passwords, back-up methods, insurers, or any particular organizational information stated implicitly as confidential in regulations and policy.

1.12.2 Profiling

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

1.13 Competitive Intelligence Scouting

Tests for scavenging property that can be analyzed as business intelligence. While competitive intelligence as a field is related to marketing, the process here includes any form of competitive intelligence gathering, including but not limited to economic and industrial espionage.

1.13.1 Business Grinding

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

1.13.2 Business Environment

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

1.13.3 Organizational Environment

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

1.14 Quarantine Verification

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

1.14.1 Containment Process Identification

Identify and examine quarantine methods and process at the gateways in all channels for

aggressive and hostile contacts such as sales people, head-hunters, grifters, journalists, competitors, job seekers, job candidates, and disruptive persons.

1.14.2 Containment Levels

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

1.15 Privileges Audit

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

1.15.1 Identification

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

1.15.2 Authorization

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

1.15.3 Escalation

Verify and map access to property through the use of privileges to gain higher privileges to that of gatekeepers.

1.15.4 Discrimination

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

1.15.5 Subjugation

Enumerate and test for inadequacies from all channels the personnel who communicate assets to use or enable loss controls not available by default such as insecure e-mail or public telephone conversations.

1.16 Service Continuity

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

1.16.1 Resilience

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

1.16.2 Continuity

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

1.16.3 Safety

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

1.17 End Survey

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

1.17.1 Alarm

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

1.17.2 Storage and Retrieval

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

Chapter 12 - Open Methodology License (OML)

Creative Commons 2.5 Attribution-NonCommercial-NoDerivs 2005, ISECOM

PREAMBLE

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

With respect to 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 (ie. 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 a part of without explicit consent from the copyright holder.
5. All persons may include this Methodology in part or in whole in commercial service offerings, private or internal (non-commercial) use, or for educational purposes without explicit consent from the copyright holder providing the service offerings or personal or internal use comply to points 3 and 4 of this License.
6. No persons may modify or change this Methodology for republication without explicit consent from the copyright holder.

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

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

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

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

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

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

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

NO WARRANTY

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

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