



INSTITUTE FOR SECURITY AND OPEN
METHODOLOGIES

BSTA 1.0

Business Security Testing and Analysis Workbook

Created by Pete Herzog

CREATED BY:	Pete Herzog	pete@isecom.org
PROJECT LEAD:	Pete Herzog	pete@isecom.org
CONTRIBUTORS	Javier Fernandez-Sanguino Juanjo Losada	jfernandez@germinus.com juanjo@securityxperts.es

CURRENT VERSION: v1.0
NOTES:
CHANGES:
DATE OF CURRENT VERSION: November 6, 2003
DATE OF ORIGINAL VERSION: November 6, 2003

1.	BSTA Workbook	3
1.1	Introduction.....	3
1.2	Goals of Workbook	3
2.	Business Benefits of Testing	3
2.1	Introduction	3
2.2	Terminology	3
2.3	Types of Testing.....	3
2.4	Legal Requirements	3
2.5	Internal/External Requirements	3
2.6	Frequency of Testing.....	3
2.7	Selecting a Test	3
2.8	Summary	3
3.	The Security Team.....	3
3.1	Introduction	3
3.2	Internal vs. External	3
3.3	Team Skills	3
3.4	Testing Methodology	3
3.5	Ethics.....	3
3.6	Team Recruiting.....	3
3.7	Skill Refinement.....	3
3.8	Information Sources	3
3.9	Tools Used.....	3
3.10	Assurance Measures	3
3.11	Security Metrics.....	3
3.12	Sample Work	3
3.13	Summary	3
4.	Testing Planning	4
4.1	Introduction	4
4.2	Developing Testing Scope.....	4
4.3	Project Handling.....	4
4.4	Timelines and Schedule	4
4.5	Testing Goals.....	4
4.6	Testing Limits.....	4
4.7	Communications	4
4.8	Testing Checklist.....	4
4.9	Authorization	4
4.10	Testing Scope Changes	4
4.11	RFP	4
4.12	Summary	4
5.	Testing Deliverables	4
5.1	Introduction	4
5.2	Report.....	4
5.3	Supplementary Deliverables.....	4
5.4	Workshop.....	4
5.5	Summary	4
	Open Methodology License (OML)	5

1. BSTA Workbook

1.1 Introduction

The BSTA (Business Security Testing and Analysis) is a peer-reviewed paper and workbook on implicit expectations, deliverables, and requirements for a security test. This document is suited for management and describes the various natures of tests, frequency, and risk as well as the legalities and ethics in hiring a security-consulting firm or developing an internal team.

1.2 Goals of Workbook

2. Business Benefits of Testing

2.1 Introduction

2.2 Terminology

2.3 Types of Testing

2.4 Legal Requirements

2.5 Internal/External Requirements

2.6 Frequency of Testing

2.7 Selecting a Test

2.8 Summary

3. The Security Team

3.1 Introduction

3.2 Internal vs. External

3.3 Team Skills

3.4 Testing Methodology

3.5 Ethics

3.6 Team Recruiting

3.7 Skill Refinement

3.8 Information Sources

3.9 Tools Used

3.10 Assurance Measures

3.11 Security Metrics

3.12 Sample Work

3.13 Summary

4. Testing Planning

- 4.1 Introduction
- 4.2 Developing Testing Scope
- 4.3 Project Handling
- 4.4 Timelines and Schedule
- 4.5 Testing Goals
- 4.6 Testing Limits
- 4.7 Communications
- 4.8 Testing Checklist
- 4.9 Authorization
- 4.10 Testing Scope Changes
- 4.11 RFP
- 4.12 Summary

5. Testing Deliverables

- 5.1 Introduction
- 5.2 Report
- 5.3 Supplementary Deliverables
- 5.4 Workshop
- 5.5 Summary

Open Methodology License (OML)

Copyright (C) 2000-2003 Institute for Security and Open Methodologies (ISECOM).

PREAMBLE

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

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

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

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

TERMS AND CONDITIONS

1. The license applies to any methodology or other intellectual tool (i.e. matrix, checklist, etc.) which contains a notice placed by the copyright holder saying it is protected under the terms of this Open Methodology License.
2. The Methodology refers to any such methodology or intellectual tool or any such work based on the Methodology. A "work based on the Methodology" means either the Methodology or any derivative work by copyright law which applies to a work containing the Methodology or a portion of it, either verbatim or with modifications and/or translated into another language.
3. All persons may copy and distribute verbatim copies of the Methodology as are received, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and creator or creators of the Methodology; keep intact all the notices that refer to this License and to the absence of any warranty; give any other recipients of the Methodology a copy of this License along with the Methodology, and the location as to where they can receive an original copy of the Methodology from the copyright holder.
4. No persons may sell this Methodology, charge for the distribution of this Methodology, or any medium of which this Methodology is apart of without explicit consent from the copyright holder.
5. All persons may include this Methodology in part or in whole in commercial service offerings, private or internal (non-commercial) use, or for educational purposes without explicit consent from the copyright holder providing the service offerings or personal or internal use comply to points 3 and 4 of this License.
6. No persons may modify or change this Methodology for republication without explicit consent from the copyright holder.
7. All persons may utilize the Methodology or any portion of it to create or enhance commercial or free software, and copy and distribute such software under any terms, provided that they also meet all of these conditions:

- a) Points 3, 4, 5, and 6 of this License are strictly adhered to.
 - b) Any reduction to or incomplete usage of the Methodology in the software must strictly and explicitly state what parts of the Methodology were utilized in the software and which parts were not.
 - c) When the software is run, all software using the Methodology must either cause the software, when started running, to print or display an announcement of use of the Methodology including an appropriate copyright notice and a notice of warranty how to view a copy of this License or make clear provisions in another form such as in documentation or delivered open source code.
8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on any person (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If said person cannot satisfy simultaneously his obligations under this License and any other pertinent obligations, then as a consequence said person may not use, copy, modify, or distribute the Methodology at all. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.
9. If the distribution and/or use of the Methodology is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
10. The Institute for Security and Open Methodologies may publish revised and/or new versions of the Open Methodology License. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

NO WARRANTY

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

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