



ACHILLES PRACTICES CERTIFICATION

VENDOR APPRAISAL

Version 2.0 December 2010

Disclaimer

This Vendor's guide is provided to facilitate the Achilles Practices Certification processes and is subject to change. This document is produced and owned by Wurdtech Security Technologies and may not be copied, photocopied, reproduced, translated, or converted to any electronic or machine-readable form in whole or in part without prior written permission from Wurdtech.

Wurdtech Security Technologies, Inc. retains the right to change information in this guide without notice.

Wurdtech Security Technologies, Inc. believes the information in this report to be reliable and accurate but it is not guaranteed. Using and relying on this guide is at your sole risk. Wurdtech Security Technologies, Inc. is neither liable nor responsible for any loss, damage or expense arising from any omission or error in this guide.

WORLDTECH SECURITY TECHNOLOGIES, INC. GIVES NO WARRANTIES, EXPRESSED OR IMPLIED. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT ARE DISCLAIMED AND EXCLUDED BY WURLDTECH SECURITY TECHNOLOGIES, INC. IN NO EVENT SHALL WURLDTECH TECHNOLOGIES, INC. BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

This guide does not constitute a recommendation, endorsement or guarantee of any of the hardware or software products certified or the hardware and software used in certifying the Vendor's system.

The certification does not guarantee that there are no functional or security defects or errors in the Vendor's system. It does not guarantee that the Vendor's system will meet the user's requirements, expectations or specifications, or that the Vendor's system will operate securely without interruption.

This guide does not imply any sponsorship, endorsement, affiliation or verification by or with any company mentioned in the document.

All trademarks, service marks, and trade names used in this guide are trademarks, service marks, and trade names of their respective owners. No endorsement, sponsorship affiliation or involvement in the certification, the guide or Wurdtech Security Technologies, Inc. is implied nor should it be inferred.

Trademarks

Achilles™ is a registered trademark of Wurdtech Security Technologies, Inc. in Canada and/or other countries.

© 2010 Wurdtech Security Technologies, Inc. All rights reserved.

Table of Contents

1: Introduction

1.1: Scope of this Document	1
1.2: Purpose and Intended Audience.....	1

2: Appraisal Questionnaires

2.1: Questionnaires to Collect Evidence	2
2.1.1: Vendor Declaration of Scope.....	2
2.1.2: Instructions for Completing Questionnaires	2
2.1.3: Sampling Procedure	2
2.1.4: Vendor Representation/Warranty	2
2.1.5: Questionnaire Objectives	2

3: APC Program Criteria

3.1: Pass/Fail/P3I Criteria	3
3.2: Grade Pending	3
3.3: Pass Criteria	3
3.4: Fail Criteria.....	4
3.4.1: Remedial Action Levels	4
3.5: Pre-Planned Product Improvement (P3I).....	5

4: Wurldtech Certification

4.1: Certification Levels	6
4.1.1: Bronze Certification	6
4.1.2: Silver Certification	6
4.1.3: Gold Certification	7

List of Tables

Table 2-1: Vendor Questionnaire Template	2
Table 3-1: Appraiser's Grading Template	3
Table 3-2: Remedial Action Recommendation	4
Table 3-3: Remedial Action Levels	4

1 Introduction

1.1 Scope of this Document

This guide describes the comprehensive set of Achilles Practices Certification (APC) Program requirements for the Vendor Appraisal Process. It states the questionnaire objectives for each certification level, and includes instructions on how to complete and submit the APC Program questionnaires. The full set of questionnaires is contained in the *APC Vendor Submittal Workbook*.

For more information about certification levels and evidence requirements, see *APC Program Description*, which explains each element in the APC Program and includes a glossary of terms used throughout the APC Program documents.

1.2 Purpose and Intended Audience

This guide is written for certification applicants. Specifically, it is intended for the applicant point-of-contact (PoC) and technical lead responsible for resource management and certification performance. It provides a comprehensive description of the appraisal process so the PoC can allocate the necessary resources to achieve certification.

2 Appraisal Questionnaires

2.1 Questionnaires to Collect Evidence

During the APC Program, the applicant selects an appropriate certification level and answers relevant compliance appraisal questions. The applicant must meet specified evidence requirements to support claims of compliance. The APC Program uses questionnaires to clearly list these evidence requirements.

2.1.1 Vendor Declaration of Scope

Before the appraisal questionnaires are administered, the vendor completes the *APC Order Form* to declare the appraisal scope and objective of Bronze, Silver or Gold certification. Vendor scope declaration requirements are specified in *APC Program Vendor Submittal*.

2.1.2 Instructions for Completing Questionnaires

Questionnaires are administered to collect evidence for appraisal. *Table 2-1* illustrates the information included in all questionnaires. Vendor instructions for completing the questionnaire are specified in *APC Program Vendor Submittal*.

Table 2-1: Vendor Questionnaire Template

Applicant's Response				Remarks	MRE ID	MRE#	Requirement Traceability		
QR#	Question Response		Evidence ¹				Evidence Requirement	M	O
	YES	NO	Don't Know						

2.1.3 Sampling Procedure

10 percent of the evidence submitted (to a maximum of 20 percent) is selected for examination. The evidence samples are treated as Vendor intellectual property which is subject to the terms and condition of the nondisclosure agreement between the Vendor and Wurldtech.

2.1.4 Vendor Representation/Warranty

Each completed appraisal questionnaire must include a representation and warranty statement signed by a Vendor authorized signatory. Vendor instructions for completing the warrant are specified in *APC Vendor Submittal*.

2.1.5 Questionnaire Objectives

Questionnaire objectives are described in *APC Vendor Submittal*.

¹ Evidence document is considered normative. Remarks are considered informative to qualify the normative evidence data and guide the appraiser to the appropriate section of a cited document.

3 APC Program Criteria

3.1 Pass/Fail/P3I Criteria

The Wurldtech appraisal process allocates a Pass, Fail or P3I grade to each Vendor response. Only applicable requirements as declared in the Vendor's approved declaration of scope are subject to appraisal. *Table 3-1* describes the appraiser's grading template; all entries in this table are retained for historical reference. The date on which the submitted evidence is received is recorded in the **Audit Status** column and the status is noted as *Received*.

Table 3-1: Appraiser's Grading Template

Pass/Fail/P3I	Audit Status		Comments
	Date	Status	
			<ol style="list-style-type: none"> 1 Document marked "Draft" - Effective Date TBD. Assume policy/practice not enabled or practiced. 2 Version not deployed and/or no data collected. 3 Build-to or as-built specifications require update for alignment with version considered for certification. 4 Test Plan/Procedures require update for alignment with version considered for certification. 5 Document cited is not for the system version under consideration and no evidence was submitted that applies to this version. 6 Document is not approved nor is evidence submitted that approval is granted for the system version under consideration. 7 MRE requirement is for a build-to and an as-built specification. Document cited is neither. 8 Not applicable.

3.2 Grade Pending

If the evidence is selected for audit, the date of audit request is recorded in the **Audit Status** column in *Table 3-1* and the status is noted as *Audit Requested*. When the cited supporting evidence is received, the date is recorded in the **Audit Status** column and the status is noted as *Supporting Evidence Received*. The appraiser can select a comment from the drop-down menu in the *Vendor Submittal Workbook* to explain why a grade is pending. See *Table 3-1* for a list of these comments.

3.3 Pass Criteria

A pass grade is allocated to a Vendor's response that is fully responsive to the MRE.

3.4 Fail Criteria

A fail grade is allocated to a Vendor's response that is not fully responsive to the MRE, except when the Vendor has declared that P3I is applicable. Whenever a response receives a fail grade, the appraiser selects a comment (see *Table 3-1*) to explain the reason. In addition to the appraiser's comment, Wurldtech describes a remedial action to correct the deficiency, using the following table.

Table 3-2: Remedial Action Recommendation

Remedial Action Levels	Interim Credit for Incremental Build (Subject to Formal Warrant Submittal)

In addition to the Remedial Action Level (RAL) as described in *Table 3-3* below, two entries may be recorded in the **Remedial Action Level** column.

- No Action: Not Applicable, which results in no entry in the PASS/FAIL/P3I column.
- No Action: Option Not Exercised, which results in an entry in the PASS/FAIL/P3I column.

3.4.1 Remedial Action Levels

There are five Remedial Action Levels (RALs).

Table 3-3: Remedial Action Levels

RAL	Action Required	Associated Grade
0	No action	Pass grade for the evidence submitted in response to an applicable MRE. An appraiser can justify an RAL=0 grade by giving credit (Interim Credit) for an incremental build. Vendor submittal remarks must include supporting rationale to justify this credit. If interim credit is given, the appraiser enters one of the following remarks in the Interim Credit column. <ul style="list-style-type: none"> • RAL=0: Incremental Build Demo • RAL=0: FAT Complete & Accepted • RAL=0: Equivalent Policy & Procedure Practiced • RAL=0: Equivalent Test P&P Practiced • RAL=0: Equivalent Maintenance & Support P&P Practiced
1	Vendor editorial	Pass grade for the evidence submitted in response to an applicable MRE because a Vendor editorial change is required to clarify, improve, or correct the language of the evidence submitted. The technical content is correct. The Vendor is encouraged to correct the editorial defect by issuing an amendment to the evidence submittal prior to voting approval for certification described in <i>"Wurldtech Certification"</i> on page 6. If a pass grade is not awarded, the appraiser must state the reason in the Comments column.

Table 3-3: Remedial Action Levels

RAL	Action Required	Associated Grade
2	No policy or policy not practiced	Fail or P3I grade for evidence submitted in response to an applicable MRE because the Vendor fails to show that a required policy exists or is practiced and must develop the policy or establish procedures to practice a required policy within 12 months from the date of certification. The Vendor could choose to tag the deficiency as P3I.
3	Required security capability not in Vendor's system	Fail or P3I grade for evidence submitted in response to an applicable MRE because the Vendor system lacks the required APC Program built-in security capabilities and must define a plan to provide the required capability within 12 months from the date of certification (Vendor could choose to tag deficiency as P3I).
4	Required capability fails test	Fail or P3I grade for evidence submitted in response to an applicable MRE because the Vendor's system fails to demonstrate the required APC Program security capability and must correct the security function built into the system within 12 months from the date of certification. The Vendor could choose to tag the deficiency as P3I.

3.5 Pre-Planned Product Improvement (P3I)

The Vendor applicant must declare in the Certification Planning Phase described in the *APC Program Description* if an applicable BP is a P3I. If so, the Vendor must qualify the declaration as follows.

- The applicable BP is a recognized deficiency and a P3I plan is currently being developed to correct the deficiency within 12 months from the date of current certification. If an approved P3I plan is not available at the time of certification, the Vendor must submit a resourced and approved P3I plan within 30 days after certification.
- The applicable BP is a recognized deficiency and an approved P3I plan is submitted as evidence. The approved P3I plan shows evidence of milestones that can be tracked, organizational responsibilities, and funding profiles. The P3I always provides a clear description of scope of work and references a test plan and procedure for the changes.

4 Wurldtech Certification

4.1 Certification Levels

Appraisal results are presented to the voting applicant members for final edits and approval. When a consensus vote regarding certification has been reached, Wurldtech awards a Bronze, Silver or Gold certificate for the selected Process Areas (PAs) within the objective certification level. Certification emphasizes quality security process practiced by the Vendor, rather than the quality of the security solution.

4.1.1 Bronze Certification

All applicable PA requirements must be satisfied. If an applicable Base Practice (BP) or Requirement Enhancement (RE) identified as a Bronze requirement is not satisfied, the applicant's evidence must show the following.

- It is a work-in-progress with planned completion within one year of the date of certification.
- It is explicitly certified in the applicant's resourced P3I program.
- The applicant's warranty must attest to the above.

Bronze certification is designed to measure the existence of a core set of security policies, procedures, design-to and as-built documentation, test plans and procedures, and maintenance and support manuals required to build security into the Vendor's system and support services. Bronze certification does not focus on the quality of security solutions offered by the Vendor.

4.1.2 Silver Certification

All applicable PA requirements for Bronze and Silver certification must be satisfied. Silver certification verifies that an extended set of applicable policies and practices are in place, enabled, and practiced to enhance the security mechanisms built into the Vendor's product and services. If an applicable BP or RE identified as a Bronze or Silver requirement is not satisfied, the applicant's evidence must show the following.

- It is a work-in-progress with planned completion within one year of the date of certification.
- It is explicitly certified in the applicant's resourced P3I program.
- The applicant's warranty must attest to the above.

Silver certification is designed to measure the existence of an extended set of security practices. Silver certification does not focus on the quality of security solutions offered by the Vendor.

4.1.3 Gold Certification

All applicable PA requirements for Bronze, Silver and Gold certification must be satisfied. Gold certification verifies that a complete set of applicable policies and practices are in place, enabled, and practiced to monitor and track performance of the Vendor's security mechanisms and improve those mechanisms through planned and resourced improvement programs. If an applicable BP or RE identified as a Bronze, Silver or Gold requirement is not satisfied, the applicant's evidence must show the following.

- It is a work-in-progress with planned completion within one year of the date of certification.
- It is explicitly certified in the applicant's resourced P3I program.
- The applicant's warranty must attest to the above.

Gold certification is designed to measure the existence of a complete set of security practices with significant focus on the Vendor's approach to monitoring and tracking the performance of built-in capabilities, and the Vendor's approach to improving those capabilities by describing a well-formed resourced P3I program.

Wurldtech Security Technologies

For more information about Wurldtech Security Technologies contact:

Wurldtech Security Technologies, Inc.

401 W Georgia Street, Suite 1680

Vancouver BC Canada

V6B 5A1

Tel +1 (604) 669 6674

Fax +1 (604) 669 2902

Email info@wurldtech.com

We also invite you to visit our website at:

www.wurldtech.com

