

2010

HIMIS Conformance Levels and Assessment Model

Anup Narayanan
First Legion Consulting
6/18/2010

License

This work is licensed under the Creative Commons Attribution-Noncommercial-Share Alike 2.5 India License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-sa/2.5/in/> or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.

Version

1.0 – 14th of June, 2010

Author

Anup Narayanan

CISA, CISSP

Founder and Senior Consultant, First Legion Consulting

anup@firstlegion.net

www.firstlegion.net

HIMIS Website

<http://himis.isqworld.com>

Contents

1. Introduction	4
1.1. Conformance levels	4
1.2. Conformance assessment.....	4
1.3. Conformance levels vs. Maturity levels.....	4
2. Conformance assessment model	5

1. Introduction

HIMIS (Human Impact Management for Information Security) is a methodology for reducing information security risks that occur due to human mistakes. The purpose of this document is to specify various levels of conformance an organization can achieve with regards to HIMIS.

1.1. Conformance levels

HIMIS provides 3 levels of conformance. An organization can choose each conformance level based on their business objectives and availability of resources. The levels are explained in brief below.

- Conformance Level 0 – The organization must demonstrate evidence that the 4 steps defined by HIMIS (Define, Strategize, Deliver and Verify) are implemented with sufficient evidence. **This is the basic level and mandatory**
- Conformance Level 1 – Conformance Level 0 + the organization must provide evidence that information security awareness is measured as per a pre-defined frequency. Further, the organization must demonstrate evidence to prove that improvements in information security awareness management is implemented based on the awareness measurement results
- Conformance Level 2 – Conformance Level 1 + the organization must provide evidence that change in information security behaviour is measured as per a pre-defined frequency. Further, the organization must demonstrate evidence to prove that improvements in information security awareness and behaviour management is implemented based on the awareness and behaviour measurement results

Section 2 of this document explains conformance assessment models in detail.

1.2 Conformance assessment

Organizations can perform assessments independently or using 3rd parties as per the HIMIS methodology.

1.3 Conformance levels vs. Maturity levels

Research is still being done in this area to identify whether HIMIS conformance levels comply with maturity levels as identified by models such as ISM3, or CMMi. More information will be published based on research results.

2. Conformance assessment model

A graphical representation of the conformance assessment model is provided below. Please refer the HIMIS document before referring the table below in order to clearly comprehend the terms used.

HIMIS Steps	Evidence to be produced for	Level 0	Level 1	Level 2
Define	Independent review committee for the whole program Link between business goals and selection of ESP's	Yes	Level 0 + Information security awareness is measured as per a pre-defined frequency.	Level 1 + Change in information security behaviour is measured as per a pre-defined frequency.
Strategize	Definition and reasons for choosing a specific "coverage" for the program Criterion for choosing "format" of the content Method for ensuring maximum "visibility" of the content for target workforce Definition and reasons for choosing a specific "frequency" of delivery Implementation of "quality of content" criterion Method for "retention measurement" Motivational strategies for behaviour management Enforcement or disciplinary strategies for behaviour management.	Yes	Improvements in information security awareness management is implemented based on the awareness measurement results	Improvements in information security awareness and behaviour management is implemented based on the awareness measurement results
Deliver	Definition and considerations for "tolerable deviations" Considerations for "efficiency" in delivery Method for "collection of feedback" Method for "confirmation of receipt"	Yes		
Verify	Approach for verification Audit strategy – Selection of ESP's, sample size and audit methods Review of audit reports	Yes		