

VERSION 0.1



HIMIS: Human Impact Management for Information Security

For creating "Responsible" Information Security Culture

Principal Author – Anup Narayanan, First Legion Consulting

9/3/2008

LICENSE

This work is licensed under the Creative Commons Attribution-Noncommercial-No Derivative Works 2.5 India License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/2.5/in/> or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.

VERSION

Version 0.1

Release date: 3rd of September, 2008

AUTHORS & REVIEWERS

Principal Author - Anup Narayanan, Founder & Sr. Consultant, First Legion Consulting

Contact – anup (at) firstlegion (dot) net

TABLE OF CONTENTS

1.	Introduction: The HIMIS methodology	4
2.	HIMIS – Key Features	7
3.	The HIMIS Model: plan-do-check-act	9
4.	The “PLAN” phase	11
4.1.	Identify the “Visibility” of the current information security awareness system	11
4.2.	Identify “At-Risk” Information Security awareness and behavior	12
4.3.	Calculate the current level of himis maturity of the organization	12
4.4.	Define disb (desirable information security behavior) expectations	13
5.	The “DO” Phase	14
5.1.	Qualities of an Information Security awareness management system	14
5.2.	Methods for information security awareness creation	15
5.3.	USING enforcement FOR GOOD INFORMATION SECURITY BEHAVIOR ADOPTION	15
6.	The “Check” Phase	17
7.	The “ACT” Phase	18
8.	Appendix 1: Information Security Awareness Visibility Rating Tool	19
8.1.	Instructions for using the Visibility rating calculator.....	19
9.	Appendix 2: at-risk information security “awareness” and “behavior” identification and rating	20
9.1.	The tool	20
10.	Appendix 3: methods for information security awareness creation	27

1. INTRODUCTION: THE HIMIS METHODOLOGY

HIMIS (Human Impact Management for Information Security) is a methodology for creating and managing responsible information security culture in an organization. Organizations that process sensitive business information are constantly threatened by poor information security practices by their workforce that compromises sensitive information and impacts the achievement of business goals. HIMIS helps organizations achieve a responsible information security culture by,

1. First, by creating information security awareness amongst the workforce
2. Second, by making the workforce apply the information security awareness (application of information security awareness in actual practice is considered “good information security behavior”)
3. Third, spread the good information security awareness and behavior amongst the majority of the workforce

The adoption and consistent display of good security behavior by a large part of the workforce is defined as “**Responsible Security Culture**”.

THE HIMIS APPROACH

HIMIS approach focuses on migrating the workforce from a stage of lack of information security awareness → to → being awareness about information security → to → applying the information security awareness at the workplace while handling sensitive business information, as described below.

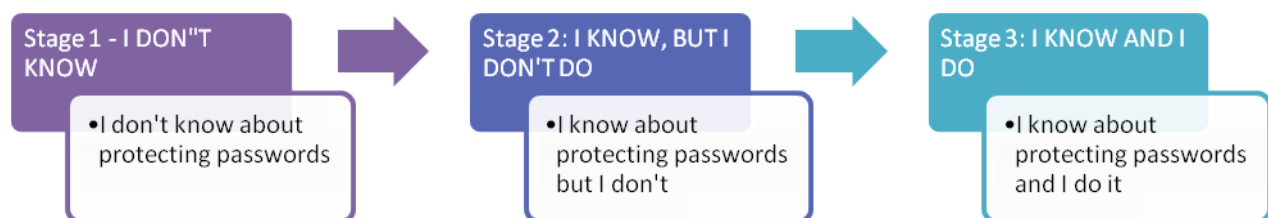


Fig 1 – The HIMIS Approach

SPECIAL FOCUS: “AWARENESS” IS NOT “BEHAVIOR”

A good analogy for describing the focus of HIMIS is to draw an example of traffic rules for road safety. Almost all drivers “KNOW” traffic rules. But, how many actually “PRACTICE” (Behave) the rules? In countries where self discipline and respect for the law is ingrained into the minds of the people, adherence to traffic rules is high. In countries where self discipline and respect for laws is poor, adherence is low. HIMIS views information security

practices in a similar manner. The first challenge is to create information security awareness amongst the workforce. The next challenge is not to stop at “Awareness” but migrate the “awareness” to good information security practices.

HIMIS TERMS AND DEFINITIONS: “AT-RISK” & DESIRABLE INFORMATION SECURITY AWARENESS AND BEHAVIOR

HIMIS enables organizations to identify “At-Risk” Information Security awareness and behavior. At-Risk Information Security awareness and behavior is defined as follows.

***At-Risk Information Security awareness:** Lack or absence of clear understanding of information security and it's importance for the organization*

***At-Risk Information Security behavior:** Lack or absence of proper application of information security practices while handling sensitive information*

***Desirable Information Security Behavior:** Good information security practices by the workforce that protects business sensitive information from compromise*

THE HIMIS MATURITY RATING SYSTEM

HIMIS maturity rating is derived by identifying “At-Risk” and “Desirable “ Information Security awareness and behavior and applying a scoring system for the same. The scoring system is further segregated to 5 different levels of maturity.

Level 5

- **Safe** - 80% or more of applicable Information Security "Awareness" and "Behavior" is "Safe"

Level 4

- **Tolerable** - Between 70% - 80% of applicable Information Security "Awareness" and "Behavior" is "Safe"

Level 3

- **Mild** - Between 60% -70% of applicable Information Security "Awareness" and "Behavior" is "Safe"

Level 2

- **Severe** - Between 50% -60% of applicable Information Security "Awareness" and "Behavior" is "Safe"

Level 1

- **Very Severe** Below 50% of applicable Information Security "Awareness" and "Behavior" is "Safe"

Fig 2 – The HIMIS Maturity Rating System

HIMIS: ISO 27001 COMPATIBILITY, USE AND APPLICABILITY

HIMIS follows the standard PDCA model for implementation. HIMIS is also compatible with any Information Security Management System that uses the PDCA model, especially ISO 27001. HIMIS is a good fit for “Section A.8 Human Resources Security” of the ISO 27001 standard.

HIMIS IS A METHODOLOGY

HIMIS is a methodology, which means that HIMIS tells you “**WHAT TO DO?**” and “**HOW TO DO IT?**” for effectively managing the human impact on information security and to achieve a responsible information security culture.

2. HIMIS – KEY FEATURES

The key features of HIMIS are,

1. Identify “At-Risk” Information Security “Awareness” and “Behavior”
2. Calculate the “Visibility” factor of current Information Security Awareness system
3. Define DISB (Desirable Information Security Behavior) targets for the workforce of the organization
4. Quality criterion for a good Information Security Awareness system
5. Information Security Awareness Creation Strategies
6. Intervention and Enforcement Strategies for motivating adoption of Good Security Behavior
7. Monitoring migration from “At-Risk Behavior” to “Desirable Security Behavior”

IDENTIFICATION OF “AT-RISK” INFORMATION SECURITY “AWARENESS” AND BEHAVIOR”

HIMIS provides a comprehensive checklist of “At-Risk” Information Security Awareness and Behavior. This checklist can be used to benchmark the current levels of Information Security “Awareness” and “Behavior” through an information security perception survey. Subsequently a business impact analysis can be done on the results of the “At-Risk” survey. This step is performed as part of the “PLAN” phase of HIMIS. [Read more....](#)

CALCULATING THE VISIBILITY FACTOR OF CURRENT INFORMATION SECURITY AWARENESS SYSTEM

HIMIS enables practitioners to calculate the current visibility of the information security awareness system by identifying the channels of communication used by the organization, the accessibility of these channels for the workforce and whether information security awareness messages are conveyed through these channels. This step is performed as part of the “PLAN” phase of HIMIS. [Read more....](#)

DEFINE DISB (DESIRABLE INFORMATION SECURITY BEHAVIOR) TARGETS FOR THE ORGANIZATION’S WORKFORCE

HIMIS enables organizations to define DISB targets for the workforce. This step is directly linked to identification of “At-Risk” behavior (refer 2.1) above and is performed as part of the PLAN phase of HIMIS. [Read more....](#)

QUALITY CRITERION FOR A GOOD INFORMATION SECURITY AWARENESS SYSTEM

HIMIS specifies quality criterion for designing and deploying high quality and effective information security awareness systems. This step is performed as part of the “DO” phase of HIMIS. [Read more](#)

INFORMATION SECURITY AWARENESS CREATION STRATEGIES

HIMIS provides strategies that can be used to design and deliver effective information security awareness messages that make people think and apply information security practices at the work place. This step is performed as part of the “DO” phase of HIMIS. [Read more](#)

INTERVENTION AND ENFORCEMENT STRATEGIES FOR MOTIVATING ADOPTION OF GOOD INFORMATION SECURITY BEHAVIOR

HIMIS provides suggestions on interventions and enforcement strategies that can be used to motivate adoption of good Information Security behavior. These steps are “corrective” or “rewarding” in nature. This step is performed as part of the “DO” as well as “CHECK” phase of HIMIS. [Read more](#)

MONITORING MIGRATION FROM “AT-RISK” BEHAVIOR TO “DESIRABLE INFORMATION SECURITY” BEHAVIOR

HIMIS provides a framework for monitoring the migration from “At-Risk” Information Security behavior to “Desirable Information Security Behavior”. Certain metrics are suggested as part of this model. This step is performed as part of the “CHECK” as well as “ACT” phase of HIMIS. [Read more](#)

3. THE HIMIS MODEL: PLAN-DO-CHECK-ACT

The HIMIS Model follows the PDCA (Plan – Do- Check – Act) model. The 4 segments are as shown below,

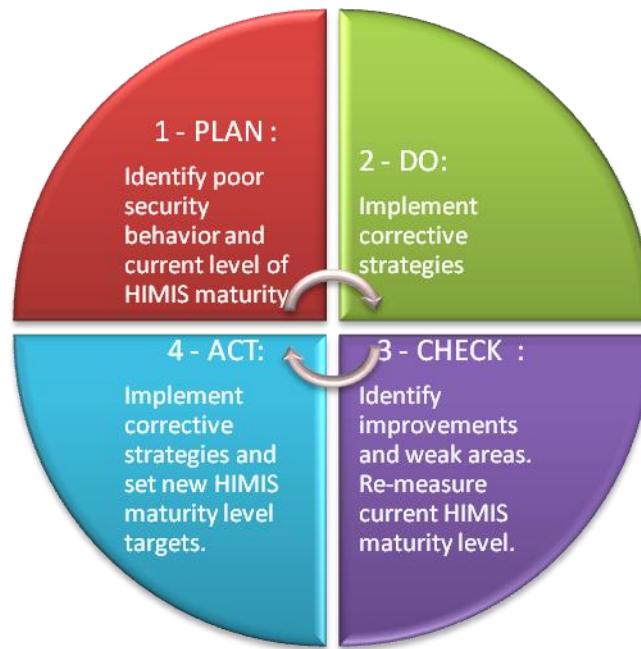


Fig 3 – The HIMIS Model

STEP 1 - THE PLAN PHASE

The Plan phase focuses on the following activities,

- Identifying the “Visibility” of the current information security awareness system
- Identifying “At-Risk” information security awareness and behavior of the organization’s workforce & the potential business impact on the organization’s business
- Calculate the current level of HIMIS maturity of the organization
- Define the list of “DISB (Desirable Information Security behavior)” expectations from the workforce

Go to the [PLAN phase...](#)

STEP 2 – THE DO PHASE

The Do phase focuses on the following activities

- Qualities of a good Information Security awareness system
- Designing and implementing Information Security “Awareness” and “Behavior” creation strategies
- Using “enforcement” as a tool for motivating adoption of good Information Security behavior

Go to the [DO phase....](#)

STEP 3 – THE CHECK PHASE

The Check phase focuses on the following activities

- Assess the migration from “At-Risk behavior” to “DISB”
- Identify the improvements (migration from “At-Risk Information Security behavior” to DISB)
- Identify the weak areas (persistent “At-Risk Information Security behavior”)
- Re-measure the current HIMIS maturity level
- Define strategies to correct weak areas

Go to the [CHECK phase....](#)

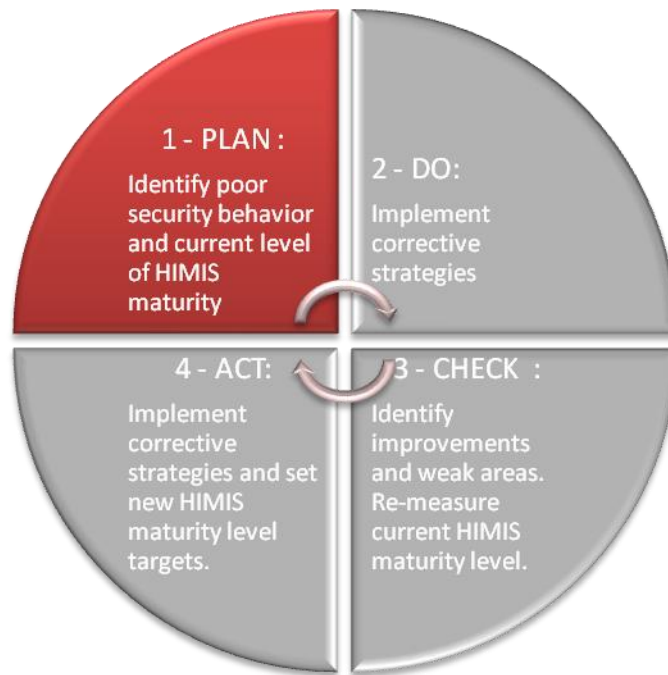
STEP 4 – THE ACT PHASE

The Act phase focuses on the following activities

- Implement the corrective actions to improve weak areas (persistent “At-Risk Information Security behavior”)
- Implement a continuous monitoring structure, preferably using metrics

Go to the [ACT phase....](#)

4. THE “PLAN” PHASE



The PLAN phase has 4 distinct activities and they are intended to lay a strong foundation for executing the HIMIS methodology. These activities are,

- Identify the “Visibility” of the current information security awareness system
- Identify “At-Risk” information security awareness and behavior of the organization’s workforce & the potential business impact on the organization’s business
- Calculate the current level of HIMIS maturity of the organization
- Define the list of “DISB (Desirable Information Security behavior)” expectations from the workforce

4.1. IDENTIFY THE “VISIBILITY” OF THE CURRENT INFORMATION SECURITY AWARENESS SYSTEM

Identifying the visibility of the current information security awareness system is important to understand whether the information security awareness messages are received by the entire workforce. For this purpose, this step focuses on the following activities,

1. Identify the constituents of the workforce (on-role employee, off-role employees, contractual personnel etc.)
2. Identify the sensitivity of the information handled by each constituent of the workforce
3. Identify the channels of communication that the workforce has access to (email, verbal, paper etc.)
4. Identify whether information security awareness messages are delivered through each of the channels

[The visibility rating tool is provided in “Appendix 1”](#)

4.2. IDENTIFY “AT-RISK” INFORMATION SECURITY AWARENESS AND BEHAVIOR

The purpose of identifying “At-Risk” Information Security awareness and behavior is to enable the organization to determine the impact of poor information security awareness and behavior on the business of the organization. Note that there is a clear segregation between “Awareness” and “Behavior” and they are considered linked, but independent. [Please refer Appendix 2, for the At-Risk Information Security Awareness and Behavior index.](#)

A variety of approaches can be used to identify “At-Risk” Information security awareness and behavior. This is mentioned in [Appendix 2.](#)

A scoring system is available for rating the intensity of the “At-Risk” Information security awareness and behavior. The cumulative score is the baseline or the current level of HIMIS maturity of the organization. Please refer next section (4.3)

4.3. CALCULATE THE CURRENT LEVEL OF HIMIS MATURITY OF THE ORGANIZATION

The cumulative score of the “At-Risk” Information Security Awareness and Behavior is the current level of HIMIS maturity of the organization. The scoring is classified as follows.

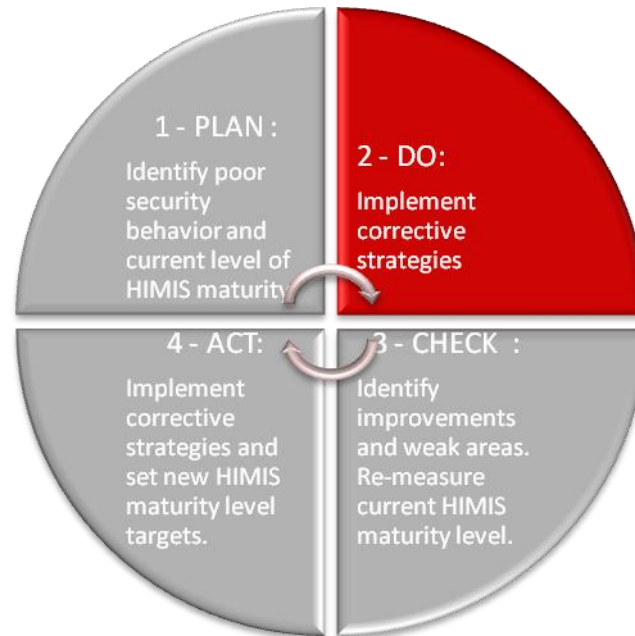
Level 5	• Safe “At-Risk” Awareness and “Behavior”. Very low impact to business. Very effective compensatory controls in place
Level 4	• Tolerable “At-Risk” Awareness and “Behavior”. Low impact to business. Effective compensatory controls in place
Level 3	• Mild “At-Risk” Awareness and “Behavior”. Medium impact to business. Compensatory controls must be more effective
Level 2	• Severe “At-Risk” Awareness and “Behavior”. High impact to business. Compensatory controls are not effective
Level 1	• Very Severe “At-Risk” Awareness and “Behavior”. Very High impact to business. No Compensatory controls in place

Fig 4 – The HIMIS Maturity Rating System

4.4. DEFINE DISB (DESIRABLE INFORMATION SECURITY BEHAVIOR) EXPECTATIONS

Once the “At-Risk” awareness and behavior inventory is established, the next target is to create the list of “Desirable Information Security behavior” expectations from the workforce. This is condensed as a list and strategies for achieve this shall be created. This is explained in the next section.

5. THE “DO” PHASE



The DO phase focuses on the following,

- Qualities of a good information security awareness management system
- Strategies to create good Information Security awareness (to implement the DISB)
- Using strategic enforcement to make the workforce apply “Awareness” (Behavior)

To generate good Information Security behavior, it is important to first create good information security “Awareness”. The key is to understand the qualities of a good Information Security awareness management system.

5.1. QUALITIES OF AN INFORMATION SECURITY AWARENESS MANAGEMENT SYSTEM

The qualities of a good Information Security Awareness system are,

- 1. Reach & Visibility:** The Information Security awareness management system must be accessible to all constituents of the workforce that handle sensitive business information. The “Visibility Calculator” tool can be used to analyze the current reach of the “Information Security Awareness”

2. **Clarity & ease of understanding:** The Information Security Awareness messages must be understandable and must not create ambiguity. Refer [Appendix 3](#) for some sample information security awareness materials.
3. **Impact Visualization:** The best Information Security awareness messages clearly visualize the impact of the violation or non-compliance to the audience. This has marked influence on the way people accept the Information Security awareness message and implement it in real practice at the work place
4. **Business Relevance:** The Information Security awareness message must have clear links to information security as a business requirement. For example, a company that creates machinery or software may achieve more impact through Information Security awareness messages that focus on protecting Intellectual Property Rights rather than wireless access security
5. **Consideration of cultural factors:** While designing information security awareness messages, it is important to consider cultural factors. These cultural factors can be used as themes, ideas or other types of content that clicks with the audience.

5.2. METHODS FOR INFORMATION SECURITY AWARENESS CREATION

Numerous strategies can be used to create good information security awareness that go beyond the poster near the water cooler. Some of the methods are,

1. Animated videos
2. Mind-maps
3. Analysis of own "At-Risk" behavior
4. Interactive training programs
5. Posters

Please check [Appendix 3](#) for examples of each of the above tactics

5.3. USING ENFORCEMENT FOR GOOD INFORMATION SECURITY BEHAVIOR ADOPTION

Qualities of a good information security awareness system

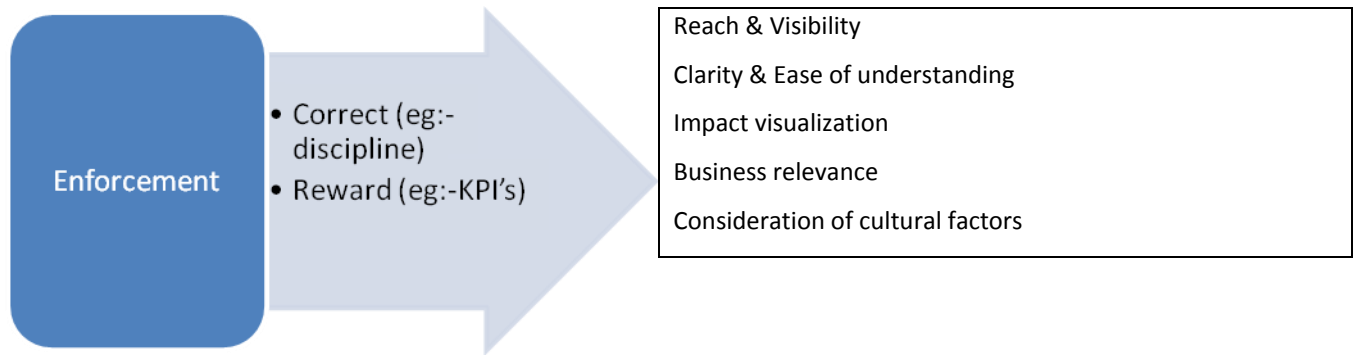


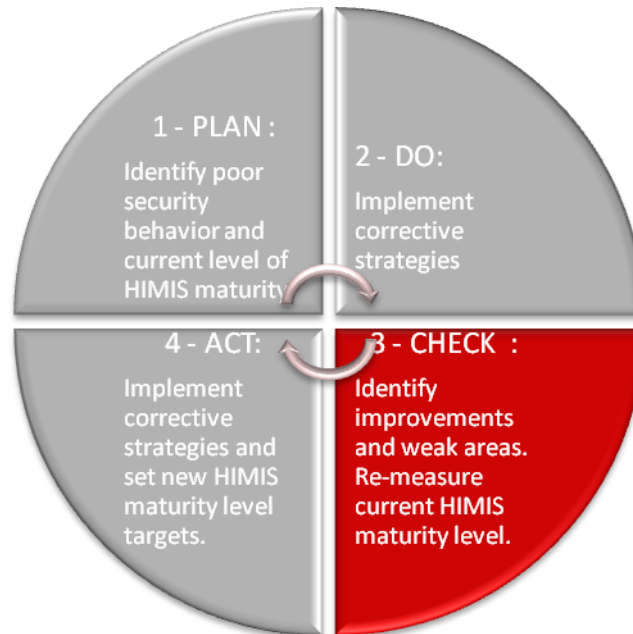
Fig 5 : Using enforcement strategies along with a good information security awareness system

Creating good Information Security awareness will alone not be sufficient to make workforce practice good information security. Hence it is important to focus on “enforcement” that can create behavior change.

Enforcements can be of two types,

1. Corrective enforcement: For example, disciplinary policies
2. Rewarding enforcements: For example, reward for good information security behavior by allotting additional points for employees in the performance review

6. THE “CHECK” PHASE



The Check phase focuses on the following activities

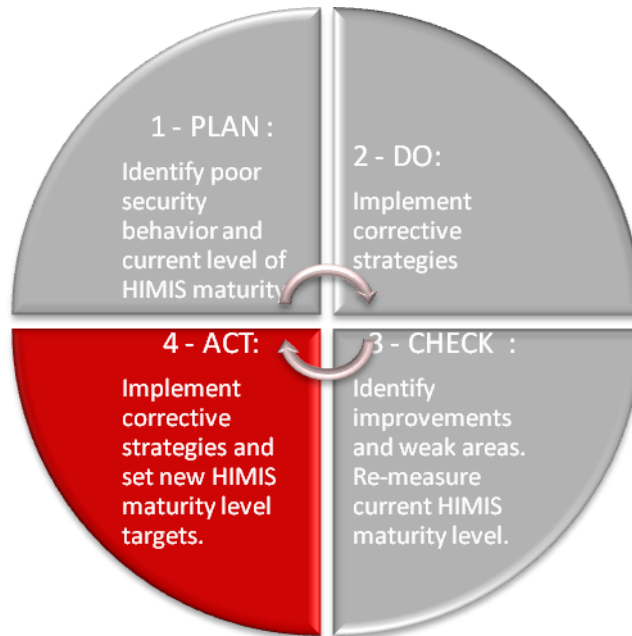
- Identify the improvements (migration from “At-Risk Information Security behavior” to DISB)
- Identify the weak areas (persistent “At-Risk Information Security behavior”)
- Re-measure the current HIMIS maturity level
- Define strategies to correct weak areas

The CHECK phase focuses on assessing the improvements i.e. the migration from “At-Risk” information security awareness and behavior to Desirable Information Security Behavior (DISB). This migration is checked as follows,

- Revisiting the At-Risk information security awareness and behavior list created during the PLAN phase
- Checking for improvements
- Noting the improvements and/or lack of the same

Once the improvements or the lack of same are noted, corrective strategies must be developed and implemented. The corrective strategies are covered in the last phase, the ACT phase.

7. THE “ACT” PHASE



The ACT phase focuses on the following activities

- Implement the corrective actions to improve weak areas (persistent “At-Risk Information Security behavior)
- Implement a continuous monitoring structure, preferably using metrics

The ACT phase deals with implementing corrective measures for continuously persisting “At-Risk” Information Security awareness and behavior. This is a continuous process and it depends on the following,

- Continuous identification of the At-Risk information security awareness and behavior identification
- An improvement measurement, review and monitoring structure
- Adoption of new strategies and discarding old strategies that did not work

8. APPENDIX 1: INFORMATION SECURITY AWARENESS VISIBILITY RATING TOOL

The Visibility Rating calculator can be [downloaded here](#). Use the instructions below to use the Visibility rating calculator.

8.1. INSTRUCTIONS FOR USING THE VISIBILITY RATING CALCULATOR

1. Create the list of workforce constituents (On-role employees, Contractual employees, Support Staff such as janitors, security guards etc.)
2. Create the list of interested parties (stake holders, customers, regulatory body etc.)
3. Rate the sensitivity of the information accessed and used by the workforce and interested parties on a scale of 1 to 3 where, 1=Low, 2= Medium and 3=High
4. Identify the channels through which information security awareness messages are conveyed to the workforce and check whether the workforce and interested parties have access to these channels
 - 4.1. If the workforce or interested parties have access to the channel, then the score is “1”
 - 4.2. If the workforce or interested parties do not have access to the channel, then the score is “0”
5. Rate the “visibility” using the information provided in step 3 and step 4 using the formula.....

9. APPENDIX 2: AT-RISK INFORMATION SECURITY “AWARENESS” AND “BEHAVIOR” IDENTIFICATION AND RATING

There are multiple techniques to identify At-Risk awareness and behavior. Some of them are mentioned below and the practitioner may choose the best method as per their discretion.

1. Direct audits (person-to-person)
2. Observations (indirect or stealth)
3. Social Engineering Strategies
4. Review of logs (incident management logs)

A good reference for conducting tests that include testing human resilience is OSSTMM (www.osstmm.org) by ISECOM.

9.1. THE TOOL

Domain	Desirable Information Security Behavior	Status of “Awareness”		Status of related “Behavior”		Confidence in compensatory controls	Business Impact Analysis
		Safe	At-Risk	Safe	At-Risk		
Information Security policies and procedures	Aware of and has read organizations’ information security policies						
	Aware and demonstrates from where the information security policies can be accessed and read						
	Aware of security clauses in the legal agreements with the organization, including disciplinary processes and does not violate them						

	The user is aware of the information security training schedules and has attended the trainings						
	Aware of background screening and verification of past records and has not falsified records						

Domain	Desirable Information Security Behavior	Status of "Awareness"		Status of related "Behavior"		Confidence in compensatory controls	Business Impact Analysis
		Safe	At-Risk	Safe	At-Risk		
Reporting of Information security incidents	Aware of contact procedures and policies in case of a security incident and demonstrates it						
	Aware that incidents should not be disclosed to others and demonstrates it						
	Aware that an investigation must not be attempted on their own and demonstrates it						

Domain	Desirable Information Security Behavior	Status of "Awareness"		Status of related "Behavior"		Confidence in compensatory controls	Business Impact Analysis
		Safe	At-Risk	Safe	At-Risk		
Responsible usage of information assets	Aware of distinction between personal information assets and company's assets and demonstrates the difference						
	Aware of asset classification guidelines of organizations' information assets and accords due importance to sensitive and high-value assets						
	Aware of Clear desk, clear screen, clear printer and clear board policy and applies it						

Domain	Desirable Information Security Behavior	Status of "Awareness"		Status of related "Behavior"		Confidence in compensatory controls	Business Impact Analysis
		Safe	At-Risk	Safe	At-Risk		
Responsible use of services and applications	Aware of internet access policy and applies it						

(Email, Internet, Intranet, etc.) OS	Aware of email access policy and applies it						
	Aware of instant messenger access policy and applies it						
	Aware of safe use of OS, applications and other services and demonstrates it						
	Aware of illegal software and Malware and does not install or use it						
	Aware of backup procedures and takes backups as per organization's requirements						

Domain	Desirable Information Security Behavior	Status of "Awareness"		Status of related "Behavior"		Confidence in compensatory controls	Business Impact Analysis
		Safe	At-Risk	Safe	At-Risk		
Resilience to Information security attacks and theft	Aware of Phishing and similar attacks and knows preventive, corrective and detective measures						
	Aware of Social Engineering and similar attacks and knows preventive, detective and corrective measures						

	Aware of tailgating, shoulder surfing and associated preventive, detective and corrective measures						
	Aware of malicious code (viruses, Trojans, spyware) and knows preventive, detective and corrective measures						

Domain	Desirable Information Security Behavior	Status of "Awareness"		Status of related "Behavior"		Confidence in compensatory controls	Business Impact Analysis
		Safe	At-Risk	Safe	At-Risk		
Access Control	Aware of physical segregation of facilities and does not access unauthorized areas						
	Aware of where "visitors" can go or "cannot" go and prevents visitors						

	from accessing unauthorized areas						
	Aware of workforce and visitor identification criterion and demonstrates it						
	Aware of escorting visitors to the facility and demonstrates it						
	Aware of password protection strategies and does not violate password policy						

Domain	Desirable Information Security Behavior	Status of "Awareness"		Status of related "Behavior"		Confidence in compensatory controls	Business Impact Analysis
		Safe	At-Risk	Safe	At-Risk		
Emergency response actions	Aware of emergency evacuation procedures and has attended drills						
	Aware of emergency help line, escalation procedures and demonstrates it						
	Aware of first aid procedures and demonstrates it						

Domain	Desirable Information Security Behavior	Status of "Awareness"		Status of related "Behavior"		Confidence in compensatory controls	Business Impact Analysis
		Safe	At-Risk	Safe	At-Risk		
Intellectual property Rights	Aware of difference between own intellectual property and company's intellectual property and demonstrates it						
	Aware of penalties in case of violation of IPR and does not violate IPR						

10. APPENDIX 3: METHODS FOR INFORMATION SECURITY AWARENESS CREATION

The below resources can be used as a model to create or design information security awareness content.

1. Animated videos
 - a. Example - depicting impact of a stolen access card, violations of clear desk, clear screen and clear board policy along with shoulder surfing. [Click here](#)
2. Mind-maps
 - a. The Wikipedia page for mind-maps is [here](#)
 - b. A sample mind-map that captures the impact of password sharing is [here](#)
3. Posters: Some examples can be seen [here](#)
4. Interactive training programs: *Examples shall be added soon*
5. Analysis of own at-risk behavior