United Arab Emirates

هيئة تنظيم الاتصالات TRA
TELECOMMUNICATIONS REGULATORY AUTHORITY

National Guideline for Building an Organizational Information Security Awareness Program

Version 0.1

Issue Date: 3 November 2017

Telecommunications Regulatory Authority (TRA)
P O Box 26662, Abu Dhabi, United Arab Emirates (UAE)
www.tra.gov.ae

Document Control

Version	0.1
State	Draft
Owner	aeCERT
Creation Date	11/10/2017
Last Update	3/11/2017
Review Period	Yearly
Classification	RESTRICTED
Retention Period	5 years

Revision History

Version	State	Updated by	Date	Revision Notes
0.1	Draft	aeCERT	11/10/2017	Document Creation

Review & Approval History

Version	Reviewed by	Signature	Review Date	Approved by	Signature	Approval Date

Distribution list

Version	Entity	Name/Title	Date	Action/Purpose

1. Purpose

This guideline has been prepared to assist entities of every size and business type to plan, design, execute, maintain, and enhance an effective information security awareness program. This guideline was prepared in line with the requirements of international standards and best practices for implementing related information security controls.

The objective of this guideline is to direct entities towards a clear path of achieving higher maturity levels in accordance to a clear criterion. The cycle of any awareness program is continuous and the practice must not stop upon implementing all the steps addressed in this document.

All developed processes for any information security awareness program should be integrated with the organization's processes and must not hinder any daily work. The information security awareness program should be an integrated process within a comprehensive program for information security. All objectives selected for the program should also be in clear alignment with business objectives.

This guideline intends at minimum to achieve the following:

- Provide the guideline to members of the Organization of Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT) to assist in raising information security awareness levels among entities in their countries
- Provide tools to internal awareness teams for achieving maximum effectiveness of awareness efforts
- Ensure the effective and efficient development and implementation of organizational information security awareness programs
- Ensure that internal information security awareness programs are compliant with local and international information security standards

2. Overview

Information security is often addressed from a technical perspective. Thus, it is of outermost importance to address and understand weaknesses surrounding the human element within information security. Many information security breaches have occurred due to human error, where the human error have proven to be both of intentional and unintentional nature. Consequently, it is critical to ensure that entities implement effective information security awareness programs. By doing so, users will understand their information security responsibilities and follow best practices.

3. Compliance with local and international standards

This guideline consists of a set of best practices for managing information security awareness programs. While making use of this guideline, it is the responsibility of each entity to use this guideline in conjunction with any applicable local laws, standards and/ or regulations.

a. ISO/IEC 27001:2013 Reference

ISO/IEC 27001:2013 Controls	Description
A.7.2.2 Information security awareness, education and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

Table 1 - ISO/IEC 27001:2013 Reference Table

4. Guideline Scope

This guideline consists of a set of best practices that can be followed by entities of every size and business type to, design, execute, maintain, and enhance an effective information security awareness program. Each section of the guideline includes practical recommendations to ensure a successful information security awareness program.

The guideline also includes templates and toolkits to support the implementation of specified practical information security awareness recommendations. Provided toolkits and templates can be found in Annex A of this guideline.

5. Leadership and management commitment

Obtaining support and effective participation from all stakeholders is essential for ensuring the success of the program. Before the start of any information security awareness related activities, the individual responsible for the program such as the CISO, ISMS manager or information security officer must obtain top management approval and support. All internal individuals and stakeholders at all organizational hierarchical levels starting from management must be committed to follow information security awareness best practices. Commitment is usually demonstrated through effective participation, involvement, and support. Top management should be committed to provide the required resources and support for implementing a successful information security awareness program. Resources should include all required financial, technical, informational, and human resources needed for all activities planned for the program.

a. Implementation guidance:

In order to obtain top management support, the key responsible personnel must develop a business case to be presented to management. Any investment done by management must be justifiable and must show a clear return of investment to the board.

Below table addresses various ways of obtaining management buy in:

Approach	Description	Examples
Present program benefits	Focus on benefits to the organization and how those benefits are linked to the vision, mission, and goals of the organization. Link every benefit to the overall gain in business.	The following are some examples of program benefits: - Protecting sensitive information and organization intellectual property - Enforcing internal information security policies and procedures - Establishing a cyber secure culture - Helping to improve the current information security controls - Helping to reduce the number of cybersecurity incidents, thus reducing costs resulting out of response and recovery - Protecting organization's reputation - Gaining and keeping customer and employee trust in the organization and

		maintaining their satisfaction
Address risks	Address risks that can arise from lack of awareness and human error. Moreover, address the impact these risks might have on the overall business.	Examples of risks: - A successful phishing attack can result in leaking entire customer database - Unauthorized physical access can result in leakage of top secret information
Highlight regulatory compliance and non-compliance implications	Refer to specific regulatory compliance requirements and highlight implications of non-compliance and that can be one of the most effective techniques for obtaining top management support.	Examples can include: - Lack of compliance with international standards such as ISO/IEC 27001:2013 awareness requirements can affect business with other entities - Non-compliance with local regulations and laws can result in fines
Real attacks	Use recent attacks and real scenarios to address possible damage. If possible use examples of attacks in the same sector.	Examples of attacks: - A ransomware in Bank X has cost the bank 32 billion dollars - A phishing attack has resulted in leakage of all online account credentials in company A

Table 2 - Methods for Obtaining Management Buy in

b. More information:

Management support must be in form of provision of required resources as well as moral support. Any information security awareness program will fail without management commitment and support. During meetings with management when the business case is presented, ensure showcasing recent information security statistics. The presentation should be concise and to the point and specific to the organization and related to the organization's overall strategy. Technical terms or details should not be included in the presentation. Presentation should be presented with confidence together with a clear justification for every demand. Management support and involvement should be at every phase of the information security awareness program. However, the most critical phase is at this initial phase to ensure their commitment till the end.

6. Management roles, responsibilities, and authorities

Top management should be responsible for enforcing information security policies, processes, and procedures. They should mandate participation of all their employees in information security awareness activities. They should define the information security responsibilities of the staff as part of their job description.

a. Implementation guidance:

Below are some of management roles, responsibilities, and authorities:

- Effective involvement in the program
- Participation in workshops and sessions
- Approvals of budgets
- Provision of necessary technical and financial resources
- Signing memos or policies mandating involvement of all staff in the information security awareness program
- Mandating involvement in awareness programs by including it as a yearly objective for all staff
- Providing feedback on all program material
- Being involved in corrective and preventive actions as needed

b. More information:

It is recommended to select a management representative or representatives from various departments to be directly involved in the program to provide inputs and approvals when needed. It is not recommended to create separate committees or groups to address awareness tasks. It is more effective to integrate these discussions in existing committee or team meeting discussions dealing with information security matters keeping in mind that awareness is a continuous matter that need to be addressed.

7. Program overview

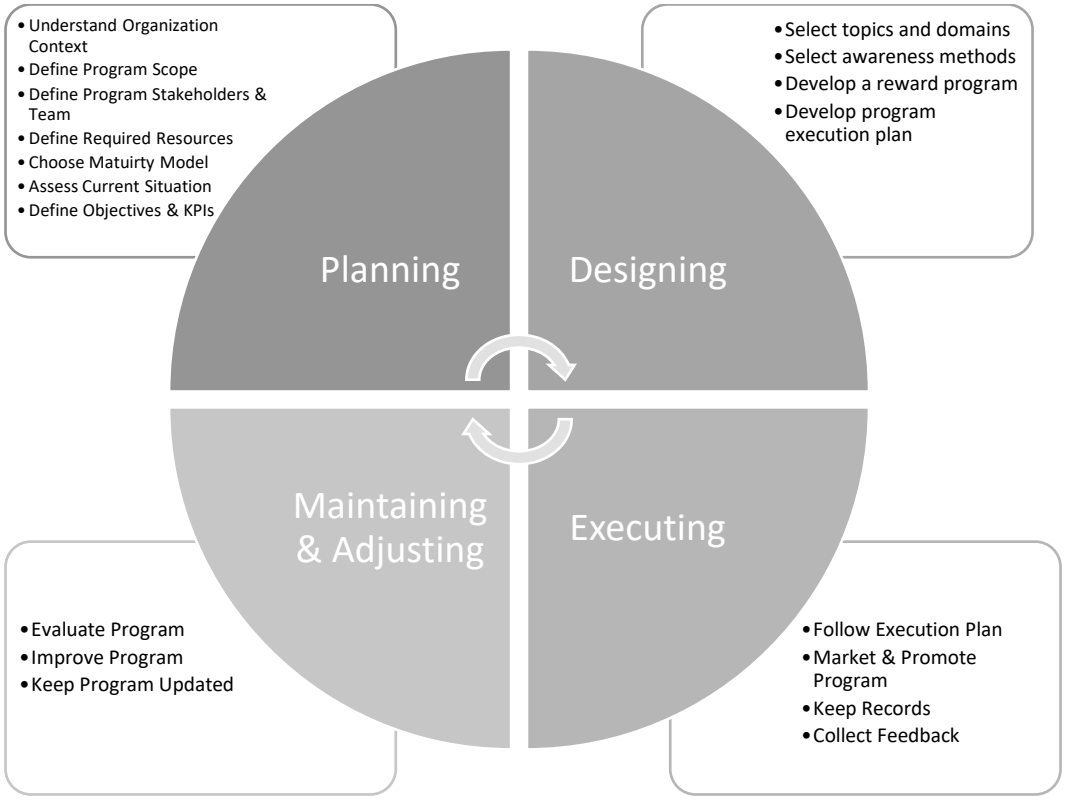

Table 3 - Program Overview

8. Program Planning

8.1 Understanding the organization and its context

When planning for an awareness program, it is recommended to start with understanding the organizational context to ensure the success of the program. The awareness team running the program should identify what makes the entity unique they should also address aspects that may impact the success of the program. The outcome of this part should be a clear map of the organization and all current available informational, technical, financial, human resources as well as any limitations.

a. Implementation guidance:

The following activities can be carried out to better understand the organization context:

- Understand the business objectives
- Conduct a PEST or SWOT analysis focusing on aspects affecting awareness
- Study the current situation
- Start a survey in the organization to have a better understanding of the company culture and preferable channels for education and awareness
- Conduct interviews with key department representatives
- Send questionnaires to management to identity key issues
- Study past awareness surveys or results and conduct a meeting with the training team to address lessons learned
- Meet the marketing or corporate communication team if any to identify any limitations observed in the past while running other programs or campaigns in the organization

Outcome of all activities:

- PEST or SWOT analysis report
- Current available budget for awareness and any limitations
- Current available human resources and any limitations
- Existing awareness activities
- Existing information organization information security policies, procedures, and guidelines and their current state (draft, approved, distributed, etc.)
- Available facilities, training venues, logistics, and any limitations
- Awareness program timeline and deadlines and any specific times to be avoided such as holiday seasons
- Available technologies that can be used during the awareness as well as limitations
- Information about company culture what is accepted and what is generally not accepted
- Collected information about perceived attitude towards cybersecurity
- Other relevant information

b. More information:

Before starting any information security awareness program, the program leader together with a top management representative should conduct a SWOT analysis of the current situation in relation to information security awareness in the organization. In this step, all internal and external issues that may negatively impact the IS awareness program should be identified. These issues may include environmental, cultural, legal, regulatory, financial, or any other limitations in the organization.

8.2 Determine the scope of the program

After understanding the organization, the team should have a clear understanding of the current situation and limitations. It is recommended to start all awareness activities gradually in the organization rather than starting a company-wide campaign.

a. Implementation guidance:

Start by setting priorities by defining the following:

- Most critical areas of the business
- Departments holding most confidential information in the organization
- Departments with highest risks related to lack of awareness
- Quick wins (least time consuming and cost effective)

b. More information:

A clear scope should be defined for better planning of the program. Program scope can be chosen based on location, targeted audience, department, personnel, etc. All exclusions and constraints should be defined and justified. Any awareness program must eventually be rolled out to all individuals having access to information in the organization. The scoping exercise is carried out due to limitations that may exist in any organization which is discovered while understanding the organization context.
Examples of defined program scope:

- The program scope covers all departments and personnel located within the organization's head quarter and all other locations and personnel are currently excluded from the scope. (Note: A good selection for scope if all critical functions are provided from the head quarter.
- The program scope covers all individuals in the C level and above and all others are currently excluded from the scope
- The program scope covers IT department only and others are excluded from the scope

8.3 Define program stakeholders

Based on the chosen scope, the team should identify all the program stakeholders. This step is critical for ensuring effective planning and ensuring that all needs, expectations and dependencies are addressed. In many organizations, all awareness programs are fully dependent on the human resources departments or the event management team, etc.

a. Implementation guidance:

Below is a sample list of program stakeholders that should be included:

1. Top management
2. Events team
3. Regulator
4. Targeted audience
5. HR team
6. Corporate communications and marketing team
7. Third party supplier
8. IT team
9. Information security team
10. Etc.

b. More information:

Ensure that all dependencies are addressed to avoid any failures and ensure having succession plans.

8.4 Form the program Team

Every entity should have a standing awareness team responsible for identifying training needs, building and acquiring training, enrolling and tracking employees, maintaining records, and ensuring the continuity of such programs. The size and requirements of the organization plays a major role in defining the number and structure of the team. Smaller organizations may find themselves in situations where only one individual will remain in charge of the awareness efforts and have to take on multiple roles, but it is still recommended that each team should at minimum have one manager and one subject matter expert. Similarly, larger organizations, depending on their needs and requirements may decide to create formal full-time positions of information security awareness managers or practitioners where each team should have at least one team manager, one subject matter expert (SME) representative and one Human Resources (HR) representative.

A. Implementation guidance:

A RACI or any similar roles matrix table should be defined based on the various roles of stakeholders. If needed, competencies should also be assessed to ensure that the team is capable of delivering the program successfully.

B. More information:

It is recommended for entities having multiple locations and departments to select department representatives to be trained as information security champions to assist during awareness and training programs. These champions should have basic required knowledge to carry out program activities within their own departments and areas of responsibility.

Below are the common roles and responsibilities of champions:

- Assist during program planning and assessing phases
- Collect feedback about running programs
- Assist in program execution
- Conduct trainings and deliver messages
- Act as a point of contact for any matters related to information security awareness
- Assist end users in following information security policies and procedures

8.5 Define program resource requirements

Based on all the previous phases and organization context as well as available resources, the team should list down all required resources for the program.

a. Implementation guidance:

Top management or a representative should be involved in this process. While defining required financial resources, ensure that justification is given for requesting budget for awareness activities including the budget for rewards. Various quotes from suppliers can be attached to serve as evidence. In this step, various people should be involved to ensure addressing all required information.

The program team lead can use various ways for collecting requirements as below:

- Questionnaires
- Interviews

When evaluating needed resources, the following resources should be considered:

- Human resources
- Information
- Technology
- Venues

- Financial
- Etc.

Financial requirements should be finalized in the design phase.

b. More Information:

Other teams should be involved in this step for ensuring that all requirements are covered as per the defined scope.

8.6 Define and choose your maturity model

Various maturity models are available for selection by entities. All activities for the assessment will depend on the maturity model. Selection of maturity model will be based on the entity type, size, and business model.

a. Implementation guidance:

The selected maturity model should be clear, realistic and scalable. The entity may choose to change and modify the maturity model overtime based on assessment results. Maturity model should be approved by top management.

b. More information

It is recommended to look at any information security awareness models available and provided by trusted entities or used by other entities within the same sector. The regulator may be consulted to assist during the selection of a maturity model.

8.7 Assess current situation

The current awareness level should be assessed to ensure that the program is designed in a way that is suitable to the maturity level of the targeted scope.

a. Implementation guidance:

When assessing the current level of awareness of the targeted scope, a randomly selected sample should be chosen if the total number of the targeted audience exceeds 50 employees. The selected sample should be at least more than 50% for the behavior analysis.

Five or six critical domains should be chosen within information security based on the organization's context.

Domains can include the following:

- Information security policy
- Social engineering
- Password security

- Incident management
- Information classification
- Etc.

Since human behavior remains unpredictable, it is difficult and challenging to get accurate results. It is recommended to have two types of assessments covering the same domains.

- Assessments focusing on human behavior
- Assessments focusing on human knowledge

Examples of assessments related to human behavior can include:

- Phishing emails
- Scam calls
- Scam SMS

To evaluate the failure of success every behavior assessment clear criteria should be chosen in advance for success or failure of the assessment.

Examples for assessment criteria:

- Clicking on a phishing link is considered a success of an attack and a failure in awareness
- Provision of information about projects over the phone is considered success in attack and failure in awareness
- Replying to a scam SMS message with personal information is considered success of an attack and failure in awareness

Examples of assessment related to human knowledge can include assessments such as:

- Define social engineering?
- Spot the phishing email among these two examples

Each answer should be given a certain weight depending on the risk value to the organization.

The overall maturity should be calculated by taking an average of the results of knowledge analysis as well as behavioral analysis for each domain. Then an average should be taken for all maturity levels of all domains to be recorded as the overall awareness maturity level.

b. More information:

Assessments should mature over time and become more advanced and targeted. All scenarios should be based on real attacks. For instance, mature organizations can use spear phishing as a behavioral assessment tool. Champions can be used to assist

during any assessment and distribute questionnaires or social engineer the selected sample for the assessment. To ease collecting statistics for the knowledge assessment, tools can be used and the assessment can be conducted online.

8.8 Define objectives and KPIs

Based on the outcome of the current information security awareness assessment, the team should identify the program objectives and KPIs. Since objectives and KPIs should be derived from the outcome of the assessment, KPI areas should be made up of the information security awareness areas chosen in the assessment phase. Legal, regulatory, and contractual requirements should also be considered when defining objectives and KPIs.

a. Implementation guidance:

Objectives should be smart and in alignment with the business objectives. Defining SMART objectives and KPIs is crucial in order to establish an effective information security awareness program. Objectives should be justified by linking every objective where possible to assessment results. KPIs should be selected based on the selected maturity model. Ensure choosing realistic KPIs and not assuming a huge difference between pre-and post-assessment results.

b. More information:

Ensure that objectives and KPIs are aligned with the overall business objective of the entity. Moreover, it is recommended to involve senior management executives when defining the program objectives and KPIs.

9. Program Designing

The key to successfully developing an information security awareness program is to make it the most beneficial for the organization. This goal can be achieved by aligning the program efforts with the business objectives of the organization. All information collected in the planning phase should be used as an input in the designing phase of your program.

When designing the program keep the following in mind:

- Organizational context: The current state of the organization. This includes the current information security awareness levels and available resources.
- Desired awareness levels: The state of the organization after the Program is successfully developed and executed based on the organizational context.
- Program Scope: The targeted audience of this program

9.1 Select Domains and Topics

Based on the results of the assessments carried out during the assessing phase, the information security awareness program team should prioritize topics based on identified weaknesses. Selection of topics can also be based on risks identified in the risk assessment, weaknesses identified during an audit, etc. Specific information security awareness topics should be driven by the organization's business needs. For example, if the organization is planning on implementing a Bring Your Own Device (BYOD) policy, expanded mobile security modules should be included in the information security awareness materials. Since any awareness program is a continuous exercise, priorities may change during the course of the program based on the changes in the infrastructure or business needs.

a. Implementation guidance:

Every information security awareness program should at minimum cover the below topics: -

- Information security fundamentals
- Information security threats
- Information security controls
- Legal information security responsibilities of the organization and the employees
- Acceptable use policy of information assets
- Disciplinary process for violating security policies
- Procedures for identifying and reporting information security incidents and issues

Topics can be divided in different categories as below:

- Core Topics: Topics that are applicable to all target groups
- Role Specific Topics: Topics that are specific content to certain target groups only

Examples of core topics:

1. Password security
2. Clear desk and clear screen policy
3. Physical security
4. Social engineering
5. Email security
6. Mobile security
7. Etc.

Examples of role specific topics:

1. HR security policy
2. System security best practices
3. Network security best practices
4. Incident management
5. Change management
6. Supplier relationship policies and procedures
7. Information security in project management
8. Information security continuity planning
9. Etc.

b. More information:

The learning objective for every topic must be clearly defined while selecting topics. In order to attract the target audience to be engaged in the program, ensure including personal topics within the program such as children online protection or social media risks.

9.2 Select awareness methods

The program team should select suitable awareness methods based on all collected information in previous phases. Awareness methods are not limited to selecting onsite or online methods, it should consider the language to be used as well as well venue.

a. Implementation guidance:

Every program should have a selected design theme that can reflect the objective of the program, hence be attractive for the audience. Mascots, logos, and characters can be used as symbols to represent a certain program or phase of the program. Humans tend to relate more to visuals than text, therefore, it is recommended to minimize text and use more animation and visuals. Humans are also better in connecting stories and cases rather than pure DO's and DON'TS. Ensure that you are not underestimating the knowledge of your targeted audience and not designing very basic unappealing content. Most effective materials and methods are the ones that challenge the audience and make them think. The organization can use existing learning and

educational platforms on the cloud or implement an internal platform for uploading the awareness content. There are many learning management systems (LMS) available that can be used in tracking assessment results and number of users using the platform.

Primary methods include:

- On-site instructor-led training
- Web-based computer training

Supplemental methods include:

- Videos
- Posters
- Screensavers
- Email tips
- Newsletters
- Desktop wallpapers
- Flyers
- Games
- Storybooks
- Panel discussions
- Group discussions
- Mobile applications

b. More information:

When designing any information security awareness program, it can be useful to involve selected members of the targeted audience to be directly involved in providing feedback in the designing phase of the program. Moreover, involve the audience in group or panel discussions while executing the program. It is highly recommended to use interactive and innovative methods of delivering awareness programs if the entity can afford to do so. Ensure that your program use methods of learning by watching, listening, discussing, and interacting. Since it is recommended to use minimum content with direct messages, the audience must be provided with references to read more about all discussed subjects. Organization's information security policies and procedures can be the best reference for self-reading as well as any other available trusted sources.

9.3 Develop a reward program

A comprehensive and attractive reward program can serve as a powerful motivating factor for the program adoption and should be developed during the Program Design phase. A reward program can be developed based on selected scope and available resources. Certain budget should be allocated for rewards within the program.

There are various techniques for rewarding such as giving points for attending sessions or completing web based courses. Rewards can also be given purely based on passing certain exams or quizzes. Rewards should not only be used for achievements in terms of course completion of attendance. Rewards can also be used

for motivation, for example, motivating staff to report information security incidents or security weaknesses.

a. Implementation guidance:

The types of rewards and incentives may vary depending on the organizational context; however, the following key factors need to be considered when creating a reward program:

- Rewards should be attractive. What constitutes an attractive reward will depend on the culture of the organization, but any reward should be useful for the recipient to use.
- Rewards should be appropriate, consistent, and proportional to the existing reward practices. The team leader should ensure that similar rewards are given for similar achievements, and that greater achievements receive greater rewards. It is also important to maintain balance with the existing reward programs, in order to avoid making those programs less or more meaningful/attractive.
- Rewards should only have a positive impact on the organization. The team should work closely with HR, department managers, and supervisors to avoid any potential negative effects of the reward program. For example, if an out-of-office activity is being offered as a reward, the terms and conditions for using this reward should be clearly defined to avoid disrupting the department's normal operations.
- The reward system should be scalable to ensure that the target audience continues to participate in the program. For example, even if an employee receives the highest points and receives the best gift, he should have an opportunity to get other rewards.
- Rewards can also be in other means rather than any gift with a value. For example, an appreciation certificate, one day leave, etc.
- Reward programs should include rewarding the program team and champions to encourage them and motivate them.

b. More information:

The team should coordinate with the HR Manager to see if it is possible to include the information security awareness KPIs as part of the overall employees' performance appraisals system in the organization. This can be an attractive reward for the targeted audience, especially if the KPIs are linked with a bonus system.

9.4 Develop program execution plan

By this phase all needed information should be documented and ready to feed into the overall program execution plan.

a. Implementation guidance:

The program execution plan should at minimum include the following information:

- Every phase with delivery dates
- Responsibilities during execution
- Objective of every phase or activity
- Execution method of each activity

Once the Program Execution Plan is approved by top management, it needs to be communicated to the appropriate stakeholders. The fact that a team exists will help ensure that the Program remains strong and flexible. However, additional opportunities for executive sponsor, top management, information cybersecurity, human resources and other team interaction should be built into the Program's governance because those vital lines of communication will help the Program Team complete its mission and avoid being disbanded.

b. More information:

It is recommended to involve a representative from top management to provide feedback during the development of the program execution plan and propose how it should be communicated to management for approval either in a meeting or via email communication. Moreover, a successful program is usually a program that delivers the messages partially and doesn't give away all information at once. Therefore, the program execution plan must be developed in a way that divides the delivery of all messages starting from basic information to more advanced.

10. Program Executing

10.1 Marketing & Promoting the program

Before implementing or launching the program, it is highly recommended to start marketing activities for the program to build interest among targeted audience. Some of the material developed in the designing phase can be used during this phase to create a buzz around the program.

a. Implementation guidance:

Various marketing techniques can be used to start the buzz. The marketing or corporate communications department of the organization should be involved in this process. Lessons learned from previous campaigns and events should be used to develop attractive teasers for the program. If a creative and innovative theme has been chosen during the design phase, this can be used to the advantage of the program to

develop creative teasers. If a mascot is developed for the program, the mascot can be introduced as a teaser.

Below are few tips to be considered when developing teasers:

- Show the impact of an information security incident on the company or on individuals
- Avoiding having long text and use more visuals
- Use areas that are commonly visited or seen by the targeted audience to display the teasers such as the company intranet, desktop wallpaper, elevators, floors, etc.
- Use more than one medium to showcase the teasers
- Ensure that teasers are directly connecting with human emotions and generating general curiosity
- Avoid mentioning any information security topics and do not make the teasers too obvious, the most effective teasers are the ones that make the audience think

The program also has an attractive slogan such as below:

- Security starts with you
- If you care be aware
- You are the center of security
- Security is everyone's responsibility

b. More information:

Like all other phases, it is crucial to involve top management in promoting the campaign. After the buzz period, an official letter or email can be sent from the CEO to all targeted audience addressing the criticality of the subject and the importance of participating and engaging in the program. Rewards can also be used as essential means to attract the targeted audience to be more involved. Separate advertisements can be created showcasing all rewards and activities of the program.

10.2 Running the program

Once the program is launched, the team must ensure keeping the excitement and continuity of the program. The program execution plan should be followed by all stakeholders. The program should be kept human centric and focus on involving all targeted audience. If the organization have selected champions, they should be fully involved in this phase to deliver required messages.

a. Implementation guidance:

As the program is running, various activities need to be carried out by the program leader as follows:

- Keep records of attendance and activities
- Collect feedback at every step and make modifications to the execution plan or designs if needed

b. More information:

All recorded issues or major negative comments together with recommended corrective and preventive actions should be communicated to management if actions are required from top management to resolve these issues.

11.Program Maintaining and Adjusting

10.3 After the program

Once the program is completed, the program leader must assess the overall effectiveness of the program and ensure that all KPIs have been met as per the planning phase. There should be a clear comparison between the pre-and post-assessment results with clear maturity levels calculated. All remaining weaknesses should be documented to be considered in future programs.

a. Implementation guidance:

Assessments can be carried out either at the end or after every major milestone and corrective as well as preventive actions must be taken. Changes can be done to any phase of the program based on the identified weaknesses. The measurement should include the exact same sample selected during the pre-assessment activity otherwise the results are not accurate or realistic. If pre-and post-assessment results are not reflecting reality, the team leader can together with management modify the assessment and maturity model and select an alternative model for future programs. The program can be evaluated after every quarter and ensure that suggested improvements are imbedded in the planned activities of the program. Keep the content updated with the latest threats and risks and never communicated outdated information. Feedback forms should also be used to evaluate the program and make adjustments as needed.

b. More information:

To ensure continuity of the program and involvement of the targeted audience, provide additional references and sources for the audience to keep up to date with the latest risks and best practices. Ensure referring to the organization's policies and procedures as the main reference for any inquiries. Keep the communication open between the program team and targeted audience until a new program is launched.

12. References

- UAE National guidelines for building an organizational cybersecurity awareness program

Annex A

Attached Toolkit