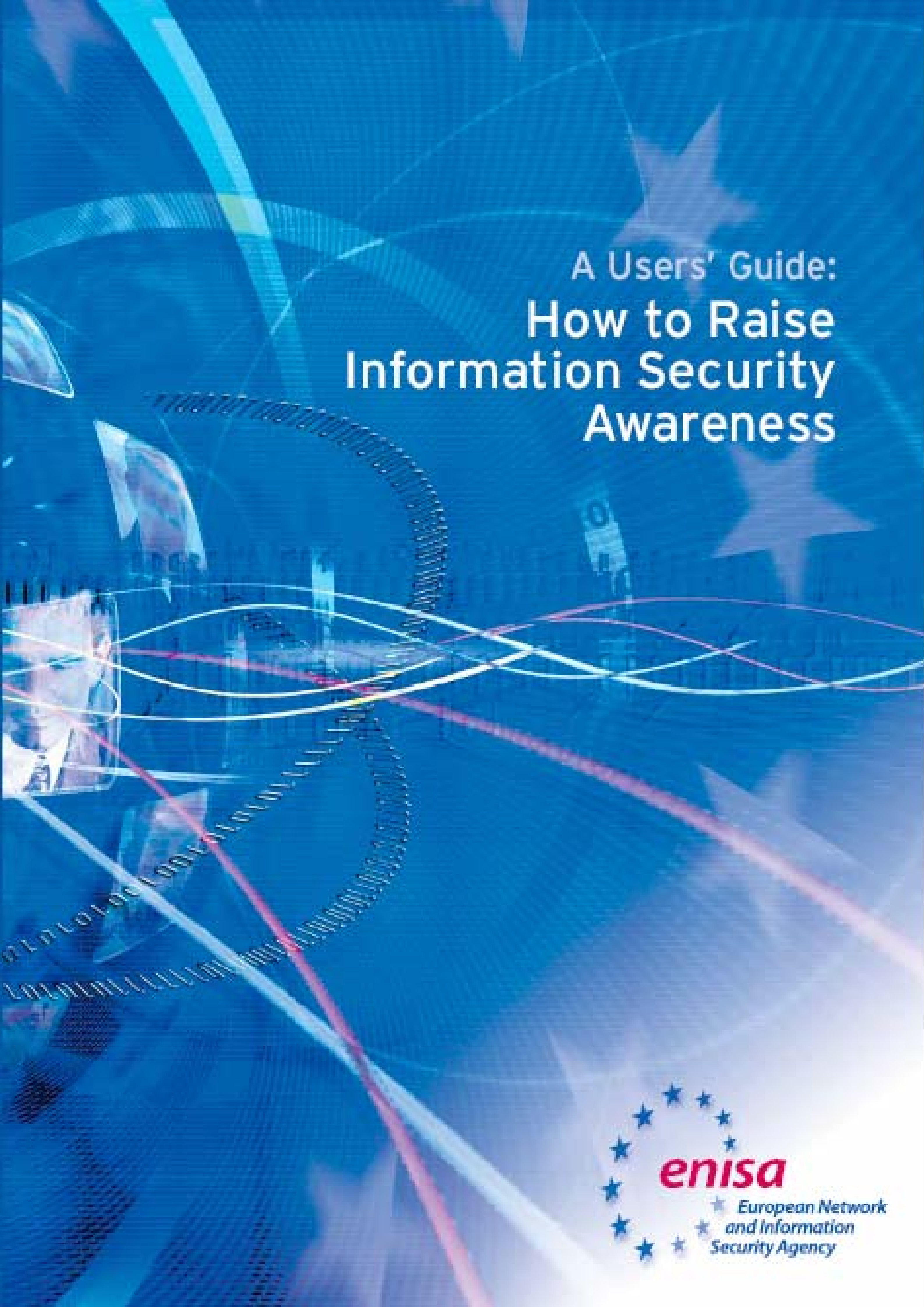


A Users' Guide: How to Raise Information Security Awareness

enisa

European Network
and Information
Security Agency

A Users' Guide: How to Raise Information Security Awareness

June 2006

Legal Notice

By the European Network and information Security Agency (ENISA).

Notice must be taken that information contained in this document has been compiled by ENISA staff also on the basis of information that is publicly available or has been supplied to ENISA by appropriate organisations within the EU Member States. This document does not necessarily represent state-of the-art and it might be updated from time to time.

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contains in this publication. ENISA is not responsible for the content or the external web sites referred to in this publication.

No part of this document may be reproduced in any media except as authorised by written permission and provided that the source is acknowledged.

Table of Contents

Summary

Awareness of the risks and available safeguards is the first line of defence for security of information systems and networks. This Guide provides practical advice for Member States on how raise information security awareness of different target groups, particularly Home Users and SMEs. This document is aimed at European Union (EU) Member States for use when conducting awareness raising initiatives and programmes.

The *Users' Guide: How Raise Information Security Awareness* illustrates the main processes necessary to plan, organise and run information security awareness raising initiatives: plan & assess, execute & manage, evaluate & adjust. Each process is analysed and time-related actions and dependencies are identified. The process modelling presented provides a basis for "kick-starting" the scoping and planning activities as well as the execution and assessment of any programme. The Guide aims to deliver a consistent and robust understanding of major processes and activities among users.

The planning and assessing phase is recognised as critical to any programme's success. Key activities are identified and described to the users. In particular, the Guide emphasises the importance of defining the goals and objectives of initiatives; defining target groups; developing the communications plan; and measuring the success of awareness programmes. Moreover, the Guide recognises that taking a change management approach to awareness initiatives is crucial as it helps close the gap between a particular issue and human responses to the need to change.

Templates and samples of suggested tools are included to help users during the different phases of awareness campaigns. These include, among others, a lessons learned template, a work plan sample and a target group data capture form.

The Guide also points out obstacles to success and provides practical advice on how to overcome them during the planning and implementation phases of programmes. In addition, it describes main factors for success of any information security initiative. For example, a baseline of current status needs to be determined before implementing (or modifying) an awareness programme and getting publicity is a vital part of any awareness campaign as it will multiply the impact by increasing the number of people who receive the message.

ENISA hopes this guide will provide Member States with a valuable tool to prepare and implement awareness raising initiatives and programmes. Providing information security is a huge challenge in itself; awareness raising among select target audiences is an important first step towards meeting that challenge.

Introduction

In today's digital age where we live and work, citizens and businesses find Information Communication Technologies (ICTs) invaluable in daily tasks. At the same time, more and more citizens and businesses are at risk of information security breaches. This is due to vulnerabilities in these new and existing technologies, together with convergence, the growing use of "always on" connections and the continuous and exponential user uptake within Member States. Such security breaches may be IT related, for example through computer viruses, or they may be socially motivated, for example through theft of equipment. In an age ever more reliant on digital information, there are an increasing number of dangers. A considerable number of citizens are unaware of their exposure to security risks.

With the advancement and proliferation of these dangers, the information security solutions of today will be obsolete tomorrow. The security landscape is continually changing. Most analysts report that the human component of any information security framework is the weakest link. In this case, only a significant change in user perception or organisational culture can effectively reduce the number of information security breaches.

There is clearly a significant shortcoming in information security awareness across Europe. For example, Home Users in many Member States are unaware that their personal computers can be controlled without their knowledge by hackers' intent on electronic identity fraud or as part of a network to launch a denial of service attack.

The European Network and Information Security Agency (ENISA) advises and assists Member States in developing a better understanding of awareness raising to help propagate safety and responsible use of ICTs.

Scope

ENISA recognises that awareness of the risks and available safeguards is the first line of defence for security of information systems and networks. Therefore, the purpose of this Guide is to provide practical advice for Member States to prepare and implement awareness-raising initiatives related to information security. The information covered features step-by-step advice to help form the basis of an effective and targeted awareness campaign.

This Guide relies on the basis of studies and analysis contacted by ENISA staff and on information that is publicly available or has been supplied to ENISA by appropriate organisations within the EU Member States. It is aimed at EU Member States for use when conducting awareness raising campaigns.

Objectives

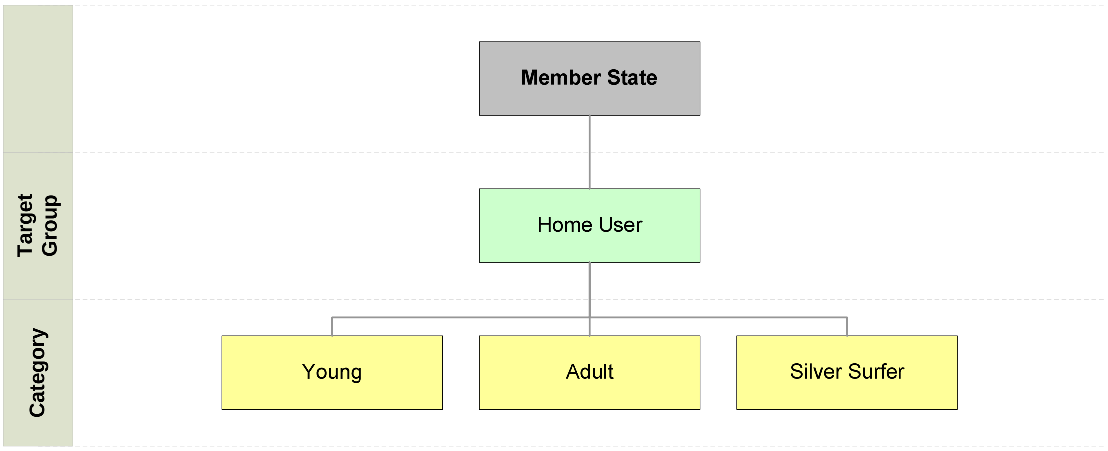
The aims of this document are for ENISA to:

- Illustrate a sample strategy on how to plan, organise and run an information security awareness raising initiative.
- Highlight potential risks associated with awareness initiatives in an effort to avoid such issues in future programmes.
- Provide a framework to evaluate the effectiveness of an awareness programme.
- Offer a communication framework.
- Present templates and tools to be used as starting points by the awareness raising team.
- Contribute to the development of an information security culture in Member States by encouraging users to act responsibly and thus operate more securely.

Target Audiences

This Guide refers to specific target groups for which awareness initiatives can be organised: Home Users and Small and Medium sized Enterprises (SMEs).

Home Users: citizens with varying age and technical knowledge who use ICTs for personal use anywhere outside their work environments. This user group can be further divided into three categories:

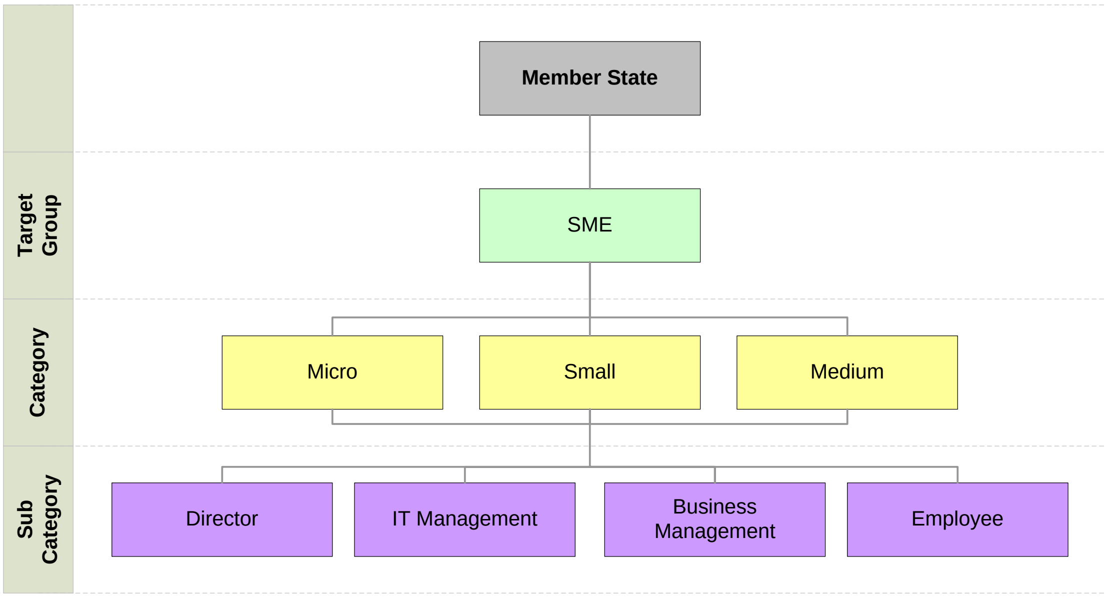


Youths – typically between seven and 15 years old**,** these citizens have grown up in an ICT environment with their levels of knowledge largely dictated by the state of infrastructure in each Member State. These citizens are trustworthy due to their youth, have a high capacity for learning and often experiment with technologies.

Adults – citizens born after the 1950s and older than 16 years of age**,** this group has partly grown up in an ICT environment. These users probably have the most diverse range of skills and knowledge of ICTs as compared to the other groups, ranging from non-existent to a high level of sophistication. These citizens can be parents or childless, with various types of careers.

Silver Surfers – citizens born in the 1950s or earlier, having grown up in a non-ICT environment. Their level of knowledge is low to non-existent and although they are typically not technically oriented, they can be service oriented (for example using mobile based e-services). As they have not grown up with ICTs, they may be more doubtful of or mistrust technology.

SMEs: both employers and employees of micro, small or medium sized enterprises (businesses). The European Commission classifies medium enterprises as having less than 250 employees, small enterprises as having less than 50 employees and micro as those with less than 10 employees[1]. The size classification of the type of business varies across the individual Member States. This target group is extremely important constituting 99% of the total number of enterprises in the EU and encompassing some 65 million jobs. This group of users can be further divided into three categories, each with four sub-categories.



Micro – a micro enterprise is defined as an enterprise that employs fewer than 10 people with an annual turnover and/or annual balance sheet of less than €2 million. Typically, this group of citizens does not have in-house IT or security experts. The numbers vary by Member State; for example in the UK a micro enterprise is typically comprised of fewer than five people.

Small – a small enterprise is defined as an enterprise that employs fewer than 50 people with an annual turnover and/or annual balance sheet total less than €10 million. The definition of a small business or enterprise also varies among Member

[1] *Recommendation 2003/361/EC*, OJ L 124 of 20.05.2003, p. 36. For more details on SME definition see http://europa.eu.int/comm/enterprise/enterprise_policy/sme_definition/index_en.htm

States. A small business may or may not have an IT expert and is unlikely to have a security expert.

Medium – a medium-sized enterprise is defined as an enterprise that employs fewer than 250 people and which have an annual turnover not exceeding €50 million, and/or annual balance sheet total not exceeding €43 million. The definition of a medium business or enterprise varies among Member States. Typically, a medium sized business has an IT expert and may have someone with security knowledge.

Within each of the three target group categories, four sub-categories of users can be defined:

Director/Owner – the key decision maker for investment in security.

IT Management – technically inclined, this group of users may not be security experts, but need to understand and implement information security protocols.

Business Management – often not technically orientated, this group of users needs to be educated and understand the importance of information security. This will allow them to implement the relevant security policies and controls in their business areas.

Employees – the largest number of users within the target group and arguably the most important if, as research suggests, most of the information security breaches are caused by human error.

For the purposes of this Guide, micro, small and medium enterprises will be considered as one entity (SMEs), as the three categories are often targeted as one in Member States.

In any awareness raising initiative, there are numerous ways to establish the profile of citizens to target. For example, the campaign can target users based on age group, social demographics, geographic location or job profiles. The campaign could also be targeted to collective groups such as institutions, non-governmental organisations (NGOs), universities or in the case of this Guide, to home users and SMEs.

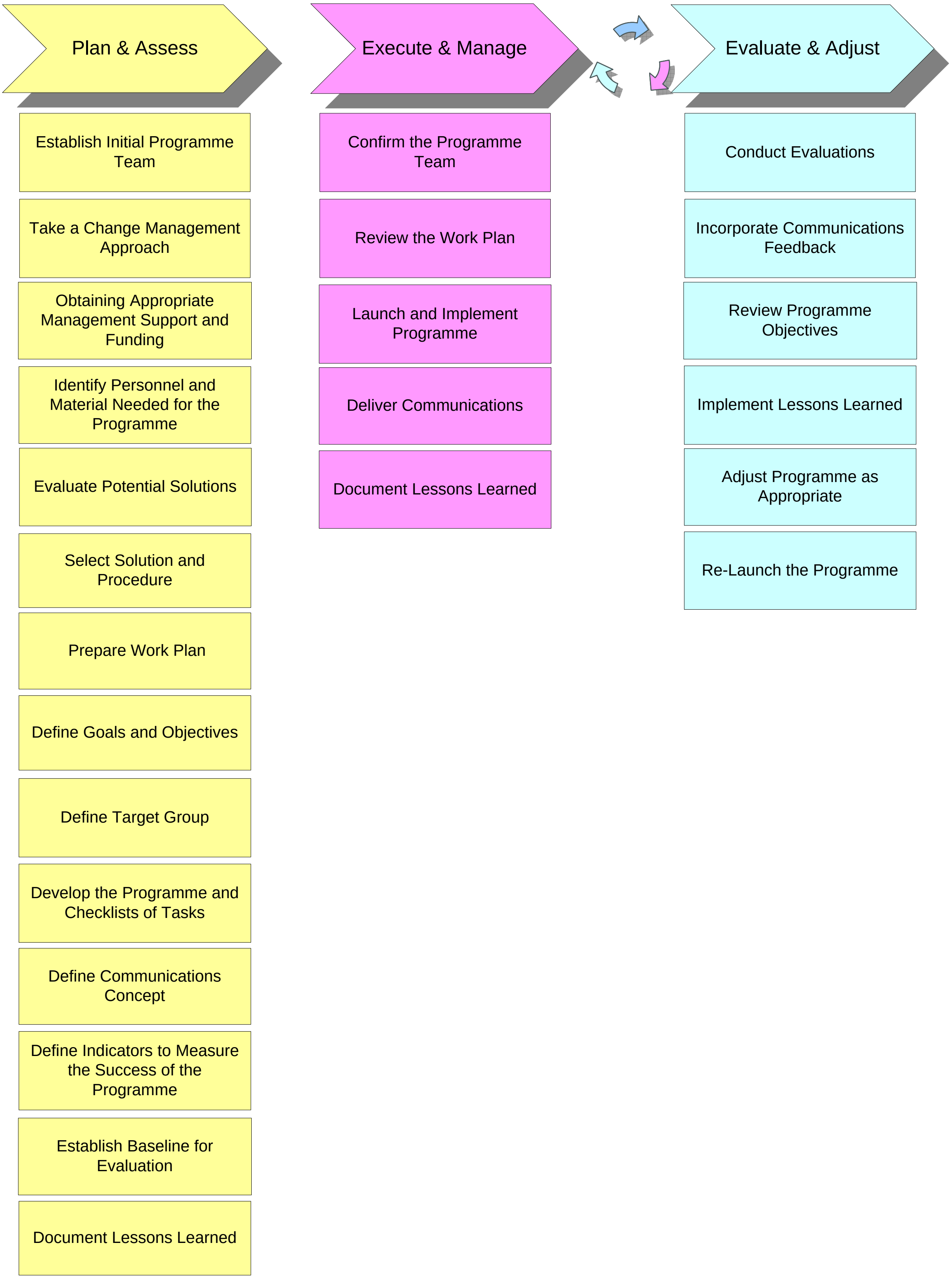
About ENISA

ENISA is a European Union Agency created to advance the functioning of the Internal Market by advising and assisting Member States, EU bodies and the business community on how to ensure a high and effective level of network and information security. ENISA also serves as a centre of expertise for Member States and EU institutions that facilitates information exchange and cooperation.

Contact Details

Isabella Santa
e-mail: awareness@enisa.europa.eu Internet http://www.enisa.europa.eu

Overall Strategy for Executing Awareness Initiatives and Programmes



Plan & Assess

- Establish Initial Programme Team
- Take a Change Management Approach
- Obtaining Appropriate Management Support and Funding
- Identify Personnel and Material Needed for the Programme
- Evaluate Potential Solutions
- Select Solution and Procedure
- Prepare Work Plan
- Define Goals and Objectives
- Define Target Group
- Develop the Programme and Checklists of Tasks
- Define Communications Concept
- Define Indicators to Measure the Success of the Programme
- Establish Baseline for Evaluation
- Document Lessons Learned

Execute & Manage

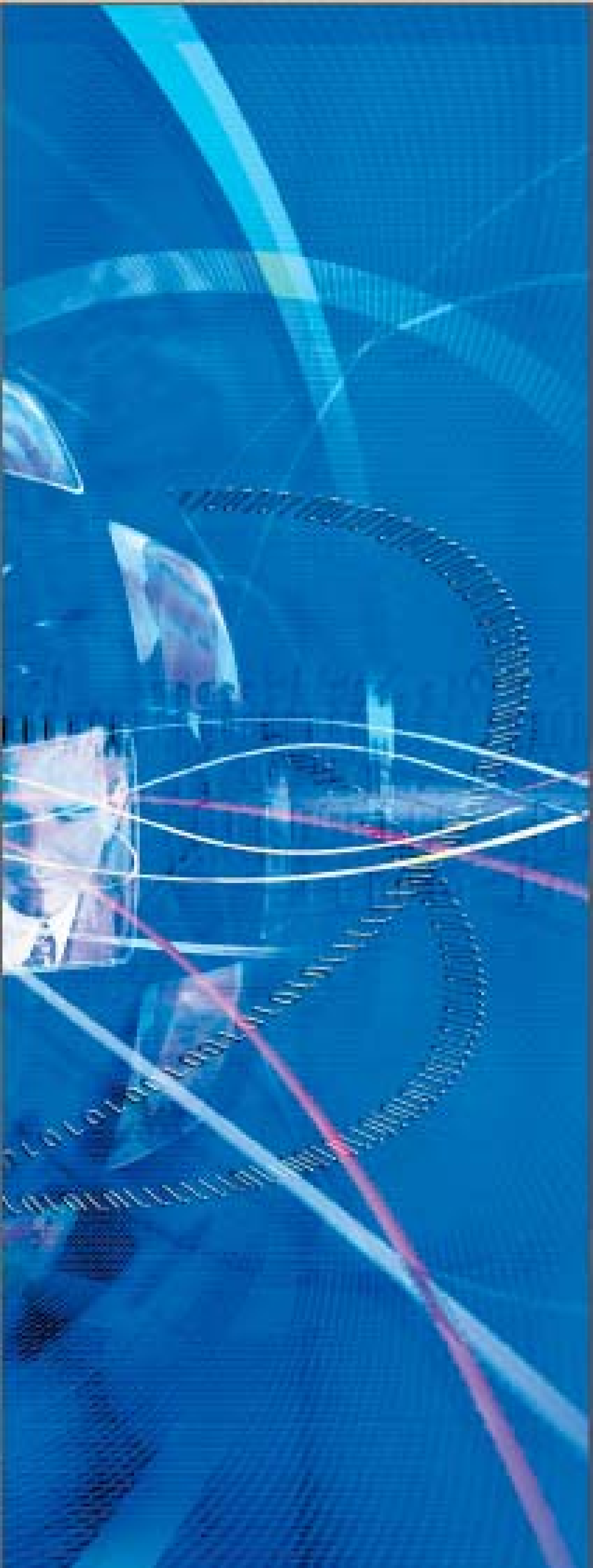
- Confirm the Programme Team
- Review the Work Plan
- Launch and Implement Programme
- Deliver Communications
- Document Lessons Learned

Evaluate & Adjust

- Conduct Evaluations
- Incorporate Communications Feedback
- Review Programme Objectives
- Implement Lessons Learned
- Adjust Programme as Appropriate
- Re-Launch the Programme

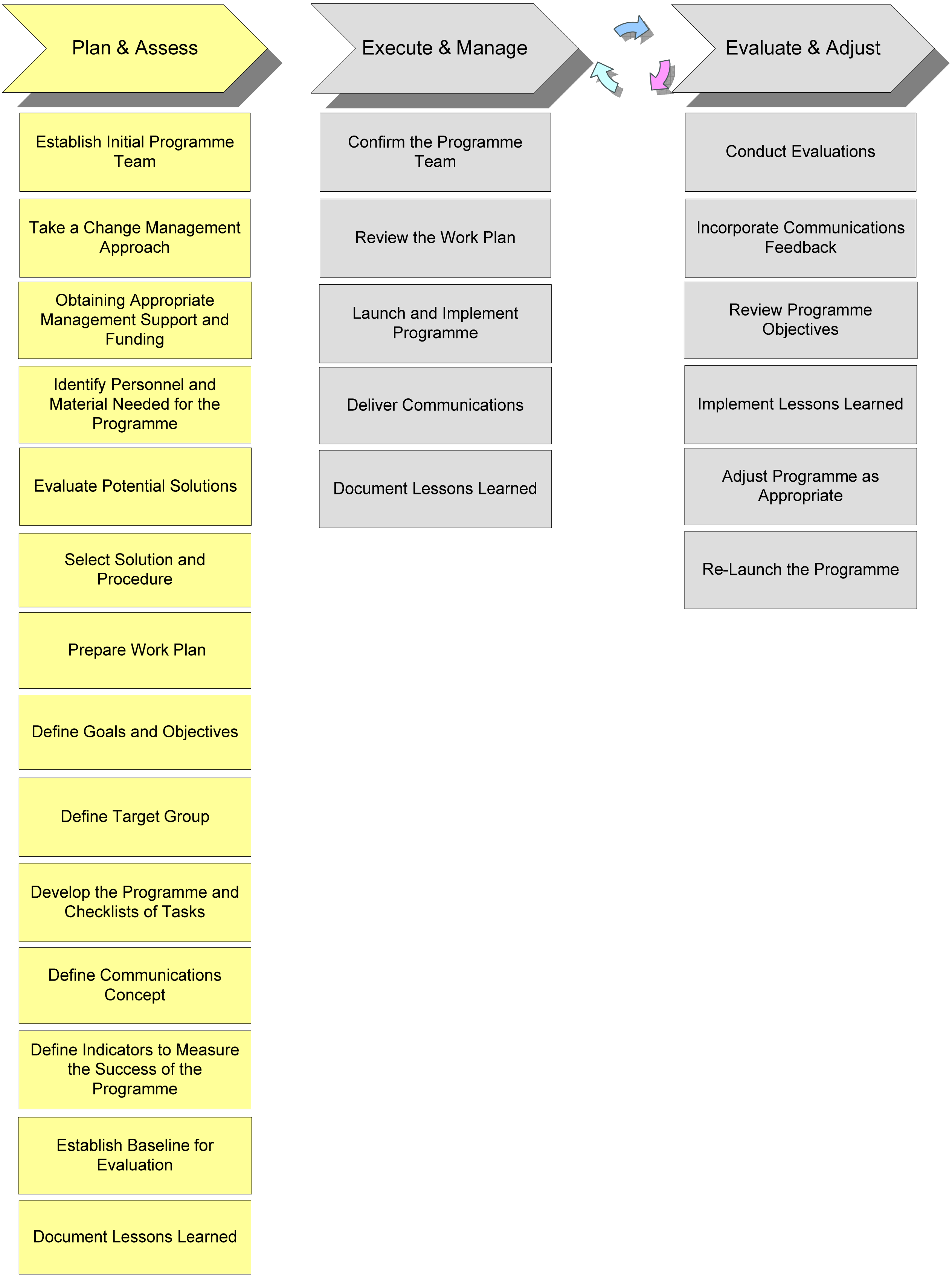
This section illustrates the main processes necessary to plan, organise and run an information security awareness raising initiative: plan & assess, execute & manage, evaluate & adjust. Each process has been analysed in order to identify time-related actions and dependencies. This process modeling provides a basis to "kick-start" the scoping and planning activities, executing and assessing a programme and a consistent and robust understanding of major processes and activities.

Templates and tools are also presented for helping users better understand how to implement the strategy for executing awareness initiatives and programmes.



Phase I
Plan & Assess

Phase I – Plan and Assess



Plan & Assess

- Establish Initial Programme Team
- Take a Change Management Approach
- Obtaining Appropriate Management Support and Funding
- Identify Personnel and Material Needed for the Programme
- Evaluate Potential Solutions
- Select Solution and Procedure
- Prepare Work Plan
- Define Goals and Objectives
- Define Target Group
- Develop the Programme and Checklists of Tasks
- Define Communications Concept
- Define Indicators to Measure the Success of the Programme
- Establish Baseline for Evaluation
- Document Lessons Learned

Execute & Manage

- Confirm the Programme Team
- Review the Work Plan
- Launch and Implement Programme
- Deliver Communications
- Document Lessons Learned

Evaluate & Adjust

- Conduct Evaluations
- Incorporate Communications Feedback
- Review Programme Objectives
- Implement Lessons Learned
- Adjust Programme as Appropriate
- Re-Launch the Programme

Establish Initial Programme Team

A team must be assembled to launch the process of planning an awareness programme. The team's main goal is to plan and organise the initiative by completing the tasks foreseen in this first phase.

Take a Change Management Approach

Taking a change management approach to an awareness initiative is crucial as it helps close the gap between a particular issue and human responses to the need to change, even in the case of a cultural change.

Using the main principles of change management (e.g. targeted communications, involvement, training and evaluation), will help ensure that awareness initiative objectives are met, as well as provide a sound platform for future or follow-up programmes.

Change must be managed holistically to ensure that efforts are integrated and the change achieves real and enduring benefits. To support an awareness programme, it is important to agree on the following principles for change:

- Identify and involve key stakeholders in decision-making, planning, implementation and evaluation.
- Establish a clear goal for the change endpoint, in consultation with key stakeholders.
- Clearly define roles, responsibilities and accountabilities.
- Link and integrate key elements of change.
- Manage risks and address barriers to change.
- Provide leadership at all levels for the change process.
- Communicate in an open, honest, clear and timely manner.
- Allow for flexibility in approaches to suit different stakeholder needs.
- Resource, support and manage the change.
- Support with training and development to ensure a change in behaviour and culture.
- Learn from previous and ongoing experiences, build capability for change and celebrate achievements.

Obtain Appropriate Management Support and Funding

Gaining management support and sponsorship for the awareness programme is perhaps the most crucial aspect of the entire initiative. It is vital to build consensus amongst decision makers that the awareness programme is important and worthy of funding. This is where the concept of stakeholder management comes into play. If the key stakeholders do not understand the imperative of an information security awareness programme and do not support the objectives and goals, the initiative will not go forward.

It is important to develop an understanding of stakeholder values and issues to address and keep everyone involved for the programme's duration. If a programme does not have the necessary support from those providing resources and those who will be using the outputs, it is unlikely to succeed. Therefore, the creation of a coalition of interest and support for the programme is very important. Do not underestimate the importance of stakeholder management for any project, programme or initiative.

Depending on the organisation or institution, there may or may not be a need to make a solid financial case for the investment. However, more senior managers buy into the benefits of an awareness programme once they are presented with figures in black and white.

Greater and more clearly defined coordination or partnerships, for example through public-private or cross-Member State initiatives, can lead to maximising the potential reach of any campaign. Public-private partnerships can be a highly effective way to deliver campaigns, especially if each organisation can leverage strengths and resources. If a joint programme is developed, it is important to have Codes of Conduct (Terms of Reference) and elements such as Design Guides. The organisational set-up of the public-private partnership should include a Steering Group, a Project Management Team, a Working (and Media) Group and Sub-Project Teams.

Cost Benefit Analysis

To run a successful awareness programme, a formal request of funds will have to be made to support the initiative. The principal expenses will be incurred by the Information Security Awareness Programme Team. If appropriately experienced staff already exists within the organisation, those individuals would need to be seconded to the initiative. Otherwise, expenses need to include a manager's salary and associated costs, as well as the costs associated with the development, production and delivery of awareness materials. Included in this are any additional staffing costs for those assigned to the awareness programme team, as well as fees associated with procuring security awareness materials, external training courses, etc. Typical cost elements can be summarised as follows:

1. Full- or part-time Information Security Programme Manager and assistants (salaries and benefits plus potential recruitment costs).
2. Awareness materials (subscriptions to best practice experts such as Gartner, IsecT, etc.) if these have not already been acquired.

3. Promotional materials (themed items such as screensavers, pens, posters, mouse pads, quizzes with prizes, etc.).
4. Printing (for all materials not sent electronically).

The total for items 1 – 4 will represent the requested budget for the programme.

Identify Programme Benefits

In order to obtain appropriate management support and funding, it is very important to identify the programme benefits.

IsecT Ltd., the IT consultancy specialised in information security, writes, "Information security is a bit like having brakes on a vehicle: yes, they slow you down, but they also make it safer for you to go faster." In other words, information security provides the basis to operate in todays increasingly interconnected and technologically complex world. An information security awareness programme will:

1. Provide a focal point and a driving force for a range of awareness, training and educational activities related to information security, some of which might already be in place, but perhaps need to be better coordinated and more effective.
2. Communicate important recommended guidelines or practices required to secure information resources.
3. Provide general and specific information about information security risks and controls to people who need to know.
4. Make individuals aware of their responsibilities in relation to information security.
5. Motivate individuals to adopt recommended guidelines or practices.
6. Create a stronger culture of security, one with a broad understanding and commitment to information security.
7. Help enhance the consistency and effectiveness of existing information security controls and potentially stimulate the adoption of cost-effective controls.
8. Help minimise the number and extent of information security breaches, thus reducing costs directly (e.g. data damaged by viruses) and indirectly (e.g. reduced need to investigate and resolve breaches). These are the main financial benefits of the programme.

Identify Personnel and Material Needed for the Programme

At this stage in the process, it's time determine what is needed in terms of personnel and materials. A logical first step is to begin looking within the organisation for appropriate resources. Staff within IT, HR, Communications, Training and Development would likely have experience and backgrounds most suitable for an awareness programme.

Advice and lessons learned from colleagues and/or Member States managing other awareness, training or educational programmes could prove most valuable concerning materials and experience. In addition, consulting with them serves a stakeholder management purpose as it may help obtain their support for delivering the programme in the future. Not involving colleagues may inadvertently set them against it.

The Internet offers a vast array of information available both free of charge and on a fee basis. A quick search on terms such as "security awareness" and "information security awareness" will prove to be very helpful. There are a number of free forums specifically focused on security awareness. It could be useful to become a member, especially as members are granted access to archives.

While it is easy to amass a large volume of information on related products and services, it's important to be systematic about the way the information is gathered, as it will make the remaining steps easier.

With all the information collected, a thorough review of the list of internal and external resources is in order. Specific focus should be identifying those pieces that might be useful for and suit the needs of the programme. A typical reaction is to discard information that appears unsuitable, but exercise caution. It is easy to overlook useful resources that are incompletely described, or in the case of commercial services, poorly marketed.

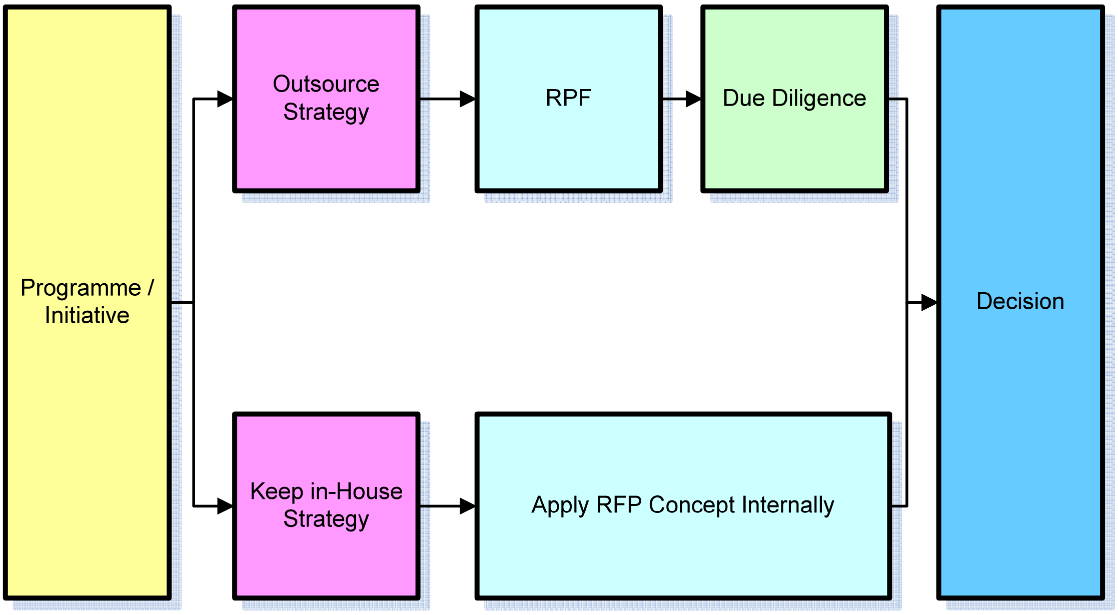
The last part of this phase is to compile the short list of potential solutions that will be evaluated as part of the next step.

Evaluate Potential Solutions

While evaluating potential solutions, a main consideration is whether the awareness programme will be kept in-house or be outsourced. Over time, the use of outsourcing as a strategic decision has increased. Organisations and institutions are now better at recognising those areas of operation where they excel and those that can be effectively done by external partners. This change brings with it the challenge of deciding whether to outsource, identifying what can be outsourced, the nature of the outsourcing relationship and the selection of partners that will not threaten the success of future programmes and initiatives.

The process illustrated below outlines best practice for decision making regarding retaining work in-house or outsourcing. It is recommended that the same Request for Proposal (RFP) approach be applied, even when the work remains in-house because it is rigorous and will help the team organise the requirements in a structured manner.

Decision Making Process to Keep in-House or to Outsource



The complete evaluation and assessment process is derived from the traditional tendering sub-process:

1. Prepare a formal Request for Proposal (RFP) containing precise requirements derived from the first two steps of this process.
   Composition of Programme Team needs to be determined along with desired experience and attributes, roles and responsibilities and reporting structures.
   Programme procedures and policies need to be determined and formalised. Included in this are approaches for weekly status reporting, financial reporting and issues management.
2. Send RFP to potential bidders indicating the deadline for responses.
3. Compile questions received by bidders and respond in a timely manner to all bidders without disclosing the originator of the questions.
4. When the deadline expires, reject any further proposals but begin systematically evaluating and scoring the offers used on the checklist written earlier.
5. Focus on essential requirements first; this may lead immediately to exclusion of some bidders if they do not meet essential needs.
6. Be sure to review additional offers submitted by bidders as they might provide useful and valuable ideas that have been previously overlooked. They can also help determine a final decision if scores are very close for a couple of offers

7. Look at the quality of the proposals as well as the sample awareness systems or materials included with the proposal, as they are valid indicators of professionalism and quality of bidders
8. Calculate the scores of the bidders (the total of (score for each criterion X the weighting assigned to that criterion) divided by the maximum possible score and then X 100%.
9. If it has been decided to outsource the programme (or portions thereof), be certain to involve procurement professionals in the tendering process, as they will be able to ensure that the process is fair.
10. If the work will remain in-house, making decisions regarding the programme in a committee forum could contribute to an inclusive and transparent atmosphere.

When formalising requirements as outlined in Point 1 above, consideration should be given to how the programme's effectiveness will be evaluated.

The RFP should contain precise requirements. An RFP sample is available in Annex I. Moreover, at this stage it is very important to determine and formalise procedures and policies, including weekly reporting etc. A Weekly status report template is available in Annex II.

Select Solution and Procure

The end result of the evaluation step may not have produced a single winning bid, but rather a decision to keep some portions of the programme in-house, contract out other portions to one or more external providers. Part of the selection step involves negotiations; perhaps further clarification of budget, price and terms as well as what is to be produced and in which time frame.

Finally, a decision is made, the Purchase Order is created and the contract signed.

Prepare Work Plan

Once the solution has been selected and the team appointed, it is recommended to prepare a work plan. At this stage the work plan will include only the main activities for which the required resources, timescales and milestones will be identified. The work plan will be reviewed as soon as the programme is developed.

It is important to prepare a work plan identifying activities, resources, timescales, and eventually, relevant milestones. The use of a tool is recommended to effectively manage the work. A work plan sample is available in Annex III.

Define Goals and Objectives

It is important to start preparing for any security awareness programme by determining what you aspire to achieve. Note that until objectives are clear, it will be problematic to attempt to plan and organise a programme and evaluation of the programme is clearly impossible. A series of questions to help facilitate setting a programme's goals and objectives is below.

*A quick note on **Goals** versus **Objectives**:*

To avoid confusion over terms, remember that goals are broad whereas objectives are narrow. Goals are general intentions; objectives are precise. Goals are intangible; objectives are tangible. Goals are abstract; objectives are concrete. Goals cannot be validated as-is; objectives can be validated.

It's been said: "The goal is where we want to be. The objectives are the steps needed to get there."

To determine what you are trying to achieve during an awareness initiative, think carefully about the following basic questions:

- Is there currently any information security programme in place, or is this effort a new initiative in your organisation? Perhaps no other information security programme exists, but are there other awareness programmes in place that could be used as a tried and tested example or starting point?

- Will the programme focus solely on awareness or will it include training and education, or a combination of these?
- What are the specific topics to be covered by the programme? What related subjects could also be included?
- At what frequency will the programme address individuals? Is the frequency adequate to maintain the topic of information security in the minds of individuals?
- What is the appropriate level of information (and detail) to provide worthwhile advice to target audiences? Should it be in-depth or is a superficial overview sufficient?

Once you have answers to the questions above, additional points should be considered:

- Is the intention to make people "aware" of security? Or does the programme endeavour to have individuals alter their behaviour as a result of being aware? Experts agree that awareness is certainly worthwhile in itself, but it should not be the final goal. A programme plan should continue beyond simply raising awareness.
- Is your goal overall security awareness or specific information (and possibly training) for particular problems, or a combination of the two? Is the list of particular problems or topics fixed or will it evolve over the coming months and years? Responses to these questions will help determine the feasibility of planning a one-time programme or whether a longer-term initiative is required to avoid overloading and/or intimidating target group members.
- Related to the above question: will the awareness programme run on an ongoing basis or is it intended to be a one-off campaign or a similar short-term action to address a specific issue? Both approaches have their merits given the right circumstances; however, there are times when a combined approach is needed.
- How will the initiative be run? As an integrated part of the organisation? Or will it be outsourced? Will a project team be put together? Who will be in charge? What qualifications/experience do team members have in information security and security awareness/training/education? What roles and responsibilities will each person have?

It is worthwhile to emphasise the need to be realistic in the time and effort required to plan and implement your programme!

Define Target Groups

It is critical to define the specific audience that is targeted by the awareness initiative. Questions to help define target groups include:

- Who is the awareness programme intended to reach?
- Are the needs of your target groups the same or do they have different information needs? Are there groups that require radically different information?
- Is the knowledge of your target groups the same or do they have different knowledge?
- What form of communication should be used to deliver the message as part of the awareness programme?
- How is the culture of information security perceived by your target groups? Is it generally taken seriously or not considered to be very important? Have members of the target groups ever seen recommended information security guidelines or practices? If yes, are they maintained and up-to-date, or will the awareness programme need to develop and promote them?

It is important to define the specific audience that is targeted by the awareness programme. The use of a tool to capture this information is recommended. A target group data capture template is available in Annex IV

Develop the Programme and Checklists of Tasks

Clearly, awareness programmes take a good deal of effort to be well organised and run. Therefore, efforts must focus on designing the programme, further developing the plan to establish the programme, and finally managing it effectively to ensure that the projected benefits are realised.

If the list of information security topics is long, it is recommended to plan the programme in separate sections spread out over a period of time. This will allow the effort to focus on specific topics in a way that makes sense to each target audience, without overloading or adding confusion. For example, the problem of viruses would require that anyone who uses a computer connected to a network in some way to have a very basic understanding of viruses. While explaining viruses, topics such as configuration management, network or systems access, etc. might be introduced at the same time.

However, it is best not to go into depth on the related subjects. Messages alerting the target audience that related topics will be dealt with at a later time are acceptable. This way, an expectation of a follow-up effort at a later date as part of the awareness initiative on further security topics is created. Carrying through with the follow-up is important to maintain the programme's credibility.

After a full list of topics to be covered during the programme is developed, it is important to evaluate each one and rank them in order of importance. A simple method of evaluating topics is to assign a weight to each one for example with 3 = crucial, 2 = important and finally 1 = nice to have. This will help to focus on the most important topics and allow defining and refining of requirements for the awareness programme. This in turn facilitates the development of the associated plan.

Define Communications Concept

Communications is key to an awareness programme. Effective communications planning is critical to a programme's success. Efficient managers will use the necessary resources to ensure that information needed by those involved in or affected by the programme (i.e. the message) is delivered at the right time, in the right manner. As a member or stakeholder of any programme or initiative, it is critical to ensure the timely and appropriate generation and disposition of programme information. The communications information listed below was featured in the ENISA's CD Information Package: Raising Awareness in Information Security – Insight and Guidance for Member States[2].

Effective Communication

Analysing many campaigns that have been executed in several Member States, some key points are apparent for any country that embarks on an information security related awareness-raising initiative.

Following are some key recommendations for an effective campaign.

The Basics

- Reach out to as broad an audience as possible. It is advantageous to look at the multiplier criteria to maximise the reach of the message.
- Do not be alarmist or overly negative about a situation. If issues or risks need to be detailed, then it is often easier for the audience to understand in the context of real world experiences.
- The goal of any awareness raising initiative should be to change the target group's secure behaviour in a positive way.
- The message delivered, the channels used and the sender of the message must be influential and credible, otherwise the target group may be less inclined to listen.
- The target groups obtain information from a variety of sources. To engage them successfully, more than one communication channel must be used.

[2] *Information Package: Raising Awareness in Information Security – Insight and Guidance for Member States*, ENISA, December 2005, page. 47 – 58.

- Ensure the initiative is flexible and adaptable as external factors can often change the landscape.

The Message

- Deliver the right message content to the right audience using the most effective communication channels. This will maximise the appeal of the message and persuade them to take action, especially if the message fits with the target group's interests and needs. The message could and should be tailored to the knowledge or technical aptitude of the target group. To help design an effective campaign, certain data should be gathered.
- The message should be proactive, topical for the target group and consistent. Often a "Top 10 Tips" format works well due to conciseness of information and easier readability/accessibility.
- In its simplest form, any message as part of an awareness raising initiative should state the risks and threats facing the users, why it is relevant to them, what to do and not to do, and finally how to be protected.
- The message should be compelling. With so much information in the market being received by the target group, finding creative ways to deliver the message help it to be noticed. Having central and consistent themes and/or slogans will help.

The Value Added

- If possible, allow the target group to give feedback on the campaign to help improve it or subsequent initiatives.
- Planning and executing a campaign is half the effort. Evaluation of the communications campaign (against metrics, performance objectives, etc.) should also be conducted to report on the campaign's effectiveness, and to establish lessons learned to improve future initiatives. A measurement such as the number of visitors to a website, the number of downloads or requests for publications or the number of newspaper articles can be used to track success.
- Evaluation of the effects of various campaigns on raising awareness for the target group can also be measured through qualitative (e.g. focus groups, interviews) and/or quantitative (e.g. questionnaires, omnibus surveys) research. See section on programme evaluation.
- Look to organisations such as ENISA and to other countries with a similar user landscape for examples of good practice and specific awareness raising initiatives.

A Communication Strategy can be constructed highlighting the main process steps in any effective awareness raising initiative.

Main process	***Description***
Establish Aims & Objectives of the Initiative & Define Target Group	• Ask questions such as why undertaking the campaign, key issues to address, why the need to address the issues and are you the right organisation to address. • Do not make assumptions. Where possible, get data and use methods such as focus groups. • Establish metrics to measure performance of campaign and to aid in developing lessons learned.
Partner Up if Needed	• Look to partner up with another organisation if you do not have access to your intended audience, do not have the necessary resources or if your audience trusts another organisation to be informed about information security. • Need to ensure there is a common message and shared views and opinions.
Establish Message for a Specific Target Group	• Necessary to target a specific group that has similar interests and priorities as the public in general has diverse interests, expertise and experiences. Because different audiences place different emphasis on different risks (often stemming from personal experiences), message needs to be targeted to a specific group. • Ask questions such as what will they notice or grab their attention, why should they care (tailored to audience's needs and concerns) and what will they do.
Detail Message	• Need to understand the audience such as their level of awareness for the issue, their needs, and the issues they are concerned about, where they get the information and what information they like to receive. • Actual message content needs to do three things: catch audience's attention, alert them to risk and provide them with information or a reference from where to get it. • Need to make sure the message is as inclusive as possible, for example, it should not discriminate against minorities.
Test Message	• Launch the campaign and evaluate results or responses. Evaluation (quantitative and qualitative) can be done through methods such as focus groups, Interviews, questionnaires or omnibus surveys.

The most effective way to deliver the message as part of any awareness raising initiative is to use multipliers that can help communicate the campaign message to as broad a range of audiences as possible within the target group.

Several partners or multiplier bodies can be used to help deliver the messages as part of an initiative. Examples include:

- Adult Education Programmes
- Banks
- Businesses
- Community Centres
- Community Colleges
- Computer Stores
- Independent Agencies
- Industry Bodies (unions, associations)

- Institutions
- ISP's
- Leading Academics
- Libraries
- Local Trade Organisations
- Media
- NGOs
- Parent Teacher Associations
- Universities

Channels of Communication

The following matrix details some of the main channels available to help raise citizen awareness as part of an information security related initiative. The table only lists a selection of advantages and disadvantages and as such, should not be viewed as a comprehensive guideline.

Channel	*Advantages*	*Disadvantages*
Brochure or Magazine	✓ Easier to define message content and format. ✓ Allows for careful study of content by Target Group. ✓ Established audiences can be reached.	× Not a static source of information as material could be lost. × May only appeal to a select Target Group.
Comic	✓ Instant appeal to certain Target Groups like the young. ✓ Message content can be more abstract in nature.	× Difficult to incorporate messages with more detail. × May only appeal to a select Target Group.
Distant Learning - Computer Based Training (CBT) - Online Training	✓ Enables training over geographically dispersed areas. ✓ Message content can be more detailed.	× Can be expensive to create training programmes. × Implies trainee has some technical knowledge already.
Education - Education Pack - Teaching Material	✓ Good way to reach large numbers of children. ✓ Often established channels exist to distribute materials.	× Time in school is already at a premium and curricula are often crowded. × Teachers may not have expertise to deliver message. × Computing facilities may not allow some activities e.g. practice in installing antivirus software.
Email	✓ Relatively cheap channel to target mass audience. ✓ Allows Target Group to digest information in own time	× Message may be undermined due to volume of emails and spam. × Email addresses must be known.
Event - Fair - Meeting - Seminar - Conference	✓ Can reach a very wide range of audiences by careful selection of venues and topics. ✓ Has more chance of interesting the audience due to the interactive element of the channel.	× Your intended audience may not attend. × Not a proactive channel with the Target Group expected to participate.
Leaflet or Fact sheet	✓ Can provide a lot of information. ✓ Cost effective to produce.	× Need to organise distribution channels so your leaflets get the right audience. × Not a static source of information as material could be lost.

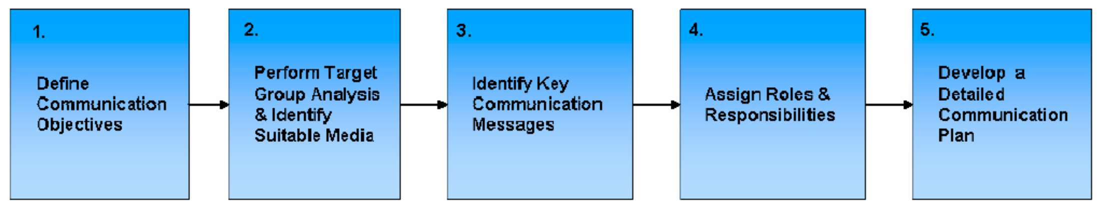
Channel	*Advantages*	*Disadvantages*
eNewsletter	✓ Have similar advantages as with the email channel.	× Not a proactive channel as typically requires users to register. × Implies trainee has some technical knowledge already.
Newspaper	✓ Mass circulation with deep market penetration. On a cost-per-thousand basis, newspapers are generally an inexpensive, cost-efficient means of delivering a message to a wide audience. ✓ A newspaper ad can give as much detailed information as is needed and even display images or logos.	× The clutter factor. There is a lot of competition for the reader's attention in a newspaper. Newspapers are usually filled with many ads, in various sizes and styles, promoting many products and services. × If wishing to reach only a specific population segment may find that newspapers waste too much circulation. × Newspapers have a short life. They are frequently read in a rush, with little opportunity for careful study..
Phone	✓ Allows direct Target Group contact. ✓ Has more chance of interesting the audience due to the interactive element of the channel.	× Can be relatively expensive. × Target Group contact details need to be available.
Poster	✓ Can be attention grabbing due to size and format ✓ Information can be universally available when put up on walls.	× With abundance of information material, message may be overlooked.
Radio	✓ Radio's biggest advantage is high frequency (reaching the same audience numerous times) at a reasonable cost. ✓ Station music formatting helps define interest groups and some demographic categories. So you can choose the specific type of audience you'd like to reach.	× Radio has heavy commercialisation. × You can't show your subject and cannot demonstrate it. × A radio spot lacks the permanence of a printed message. × Because of formatting and audience specialisation, a single station can seldom offer broad market reach.
Screensavers	✓ Places information on the computer so users are likely to see it.	× Requires development × Inexperienced users may be unable to install it. × Does not reach those without Computers.
SMS	✓ Message content can be delivered straight to the Target Group ensuring visibility.	× Need to work with Telecoms provider. × Effective channel to alert the Target Group of dangers but not raise awareness due to limited content.
Training	✓ Has more chance of interesting the audience due to the interactive element of the channel. ✓ Content of message can be more detailed and customised.	× Not a proactive channel with the Target Group expected to participate. × Can't really reach mass audience due to resources and logistics involved.
TV	✓ High impact, combining sight, sound and motion - can be attention-getting and memorable. ✓ TV comes as close as any medium can to face-to-face communication. ✓ The personal message delivered by an authority can be very convincing. ✓ You can demonstrate message. ✓ TV offers audience selectivity by programming. It offers scheduling flexibility in different programs and day parts, and the opportunity to stress reach or frequency.	× Cost - Budget requirements are relatively high. × Although you can pick your programmes, you run the risk of the most popular shows being sold out.
Video - DVD - CD	✓ Allows for creative freedom with awareness message. ✓ Professionalism of channel if implemented correctly could help enforce message.	× May not reach a technologically naïve audience.
Website	✓ Can be updated to reflect changes . ✓ Can present content for multiple audiences. ✓ Can easily link to other information.	× May not reach a technologically naïve audience. × Implies trainee has some technical knowledge already. × Not a proactive channel and with wealth of websites and information on the Internet available, message may get overlooked.

Guide to Communication Planning

This section presents a process and approach that can be used to develop a comprehensive Communications Plan by Member States. The templates and tools presented are intended to be used as starting points by the awareness raising team.

The Process

Development of a concrete communication plan is a key step to ensuring the successful change of behaviour by the target group. We recommend a five-step process as outlined in diagram below.


1. Define Communication Objectives
2. Perform Target Group Analysis & Identify Suitable Media
3. Identify Key Communication Messages
4. Assign Roles & Responsibilities
5. Develop a Detailed Communication Plan

Key Process Characteristics

- The communication objectives drive the selection of communication activities.
- Target group analysis assists in prioritising the target stakeholder groups and identifies the communication goals and requirements.
- Key messages must be tailored for issues and concerns specific to the different target groups.
- The communication plan describes the message, media and frequency of communication to target groups. The timing of specific messages is designed to support the achievement of awareness raising programme milestones.
- Gaining target group feedback is critical to maintain the quality, consistency and effectiveness of communication delivery.

Define Communication Objectives

Information security communications should effectively involve, enrol and communicate with all key target groups to support successful awareness raising. Communication objectives could be to:

- Promote the vision for network and information security and its benefits across society.
- Actively involve and engage all identified target groups.
- Provide affected target groups with an understanding of the information security issues and what those issues will mean to them.
- Provide an opportunity for target group members to ask questions and address concerns.
- Build energy and momentum to support the creation of the new learning environment.

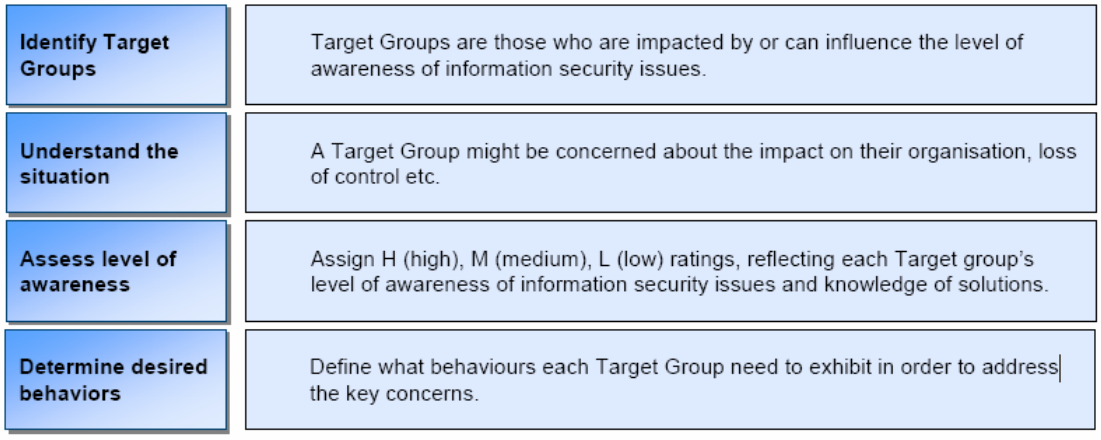
Target Group Analysis and Channel Identification

Identifying the various target groups and engaging them appropriately is critical to success. Society consists of a diverse collection of individuals with differing interests, levels of expertise and priorities. For this reason, it is difficult to find issues and messages that will be relevant to everyone. Hence, it is generally necessary to identify specific target groups with similar interests and priorities. ENISA has identified a number of target groups for Member States as part of the awareness raising initiative. Once the awareness raising team has identified the various target groups, research should be conducted in order to understand each group's:

- Level of awareness of information security issues.
- Level of awareness of corresponding solutions.
- The purposes for which they use ICT.
- Key concerns.
- Where they currently receive information.

An example of sample steps to take when conducting a target group analysis is outlined below.

Sample Steps in Conducting a Target Group Analysis

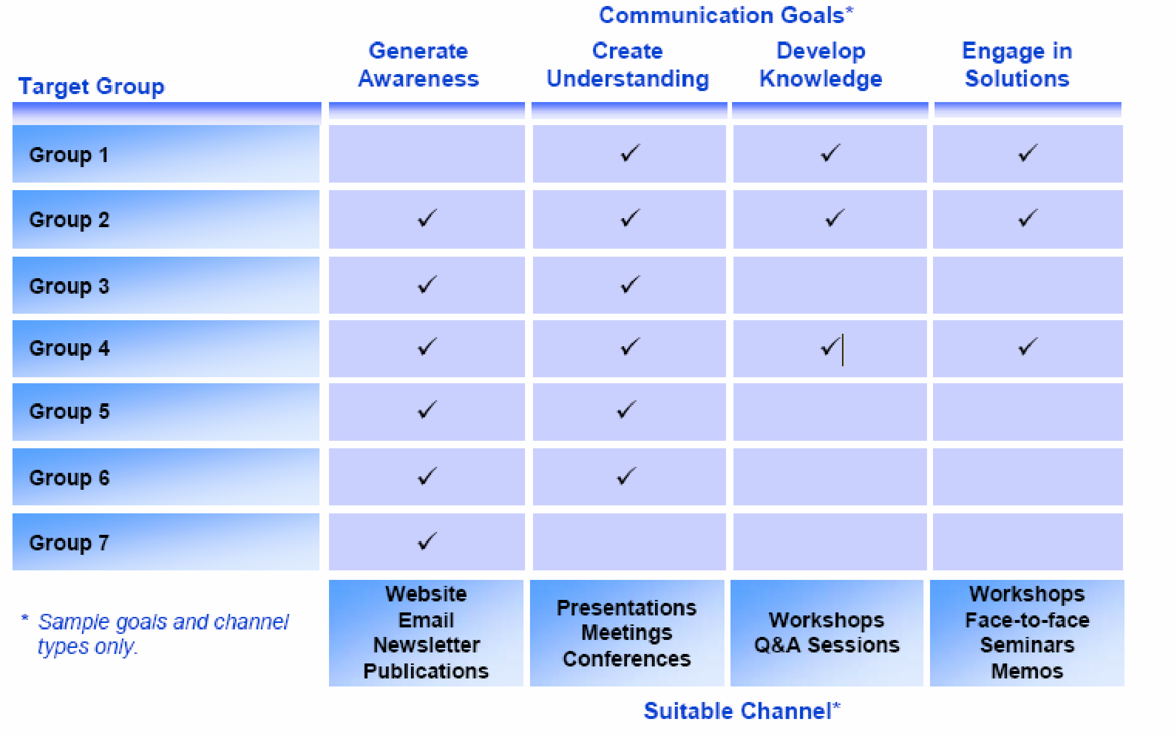


Identify Target Groups	Target Groups are those who are impacted by or can influence the level of awareness of information security issues.
Understand the situation	A Target Group might be concerned about the impact on their organisation, loss of control etc.
Assess level of awareness	Assign H (high), M (medium), L (low) ratings, reflecting each Target group's level of awareness of information security issues and knowledge of solutions.
Determine desired behaviors	Define what behaviours each Target Group need to exhibit in order to address the key concerns.

Benefits of Performing a Rigorous Target Group Analysis

- The need for information and action will be more fully understood.
- There will be a clear understanding of the impact of information security issues and the actions needed to overcome these issues.
- The communication plan can be developed to ensure that target group members receive the right information at the right time in the right way.
- The awareness raising team will be cognisant of and able to manage each target group's level of awareness.

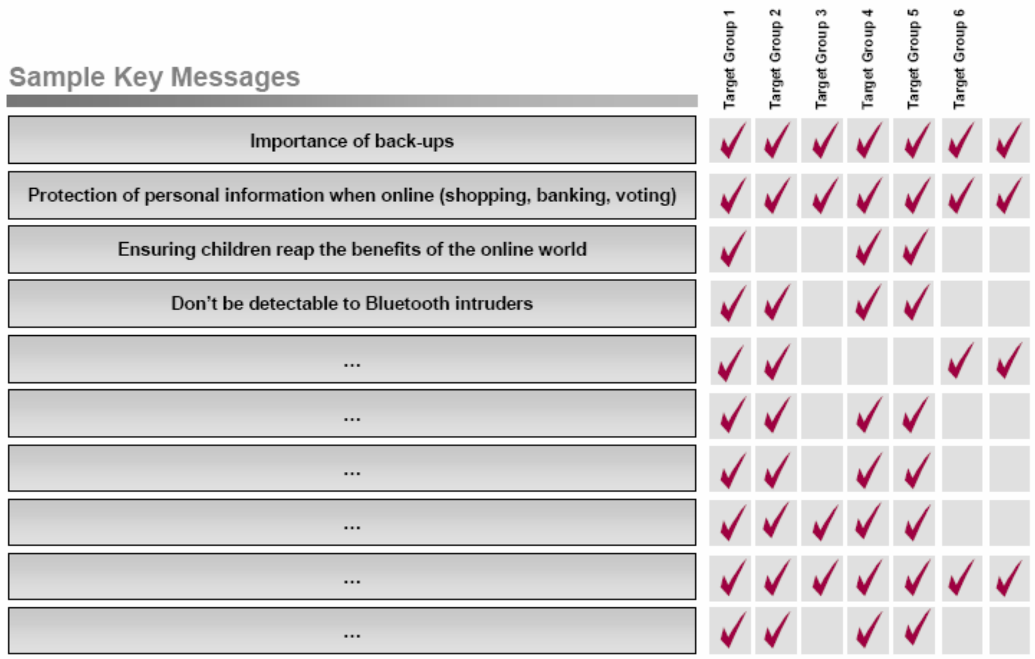
Once the target group analysis is complete, appropriate communication goals can be determined and suitable channels identified. The matrix below illustrates a method for performing these tasks.



	Communication Goals*			
Target Group	Generate Awareness	Create Understanding	Develop Knowledge	Engage in Solutions
Group 1		✓	✓	✓
Group 2	✓	✓	✓	✓
Group 3	✓	✓		
Group 4	✓	✓	✓	✓
Group 5	✓	✓		
Group 6	✓	✓		
Group 7	✓			
* Sample goals and channel types only.	Website Email Newsletter Publications	Presentations Meetings Conferences	Workshops Q&A Sessions	Workshops Face-to-face Seminars Memos
	Suitable Channel*			

Identify Key Communication Messages

The message and the target group are tightly linked; each affects the other. You could focus the message on dealing with a class of risk, for example, threats to privacy, or by focusing on a specific technology, for example, mobile phones. An audience with little prior experience of information security is more likely to identify and understand a message that relates to how they are using or interacting with ICT. For example: "When using your mobile phone you need to consider the following . . ." is more effective than a general message about protecting privacy. Messages could also apply to multiple target groups, as illustrated below.

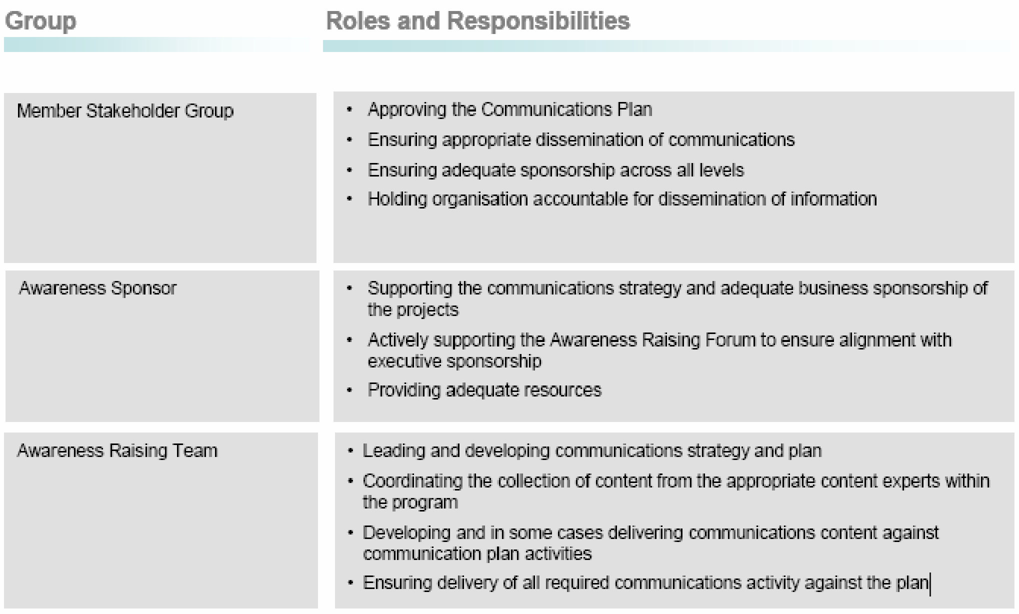


Sample Key Messages	Target Group 1	Target Group 2	Target Group 3	Target Group 4	Target Group 5	Target Group 6	
Importance of back-ups	✓	✓	✓	✓	✓	✓	✓
Protection of personal information when online (shopping, banking, voting)	✓	✓	✓	✓	✓	✓	✓
Ensuring children reap the benefits of the online world	✓			✓	✓		
Don't be detectable to Bluetooth intruders	✓	✓		✓	✓		
…	✓	✓				✓	✓
…	✓	✓		✓	✓		
…	✓	✓		✓	✓		
…	✓	✓	✓	✓	✓		
…	✓	✓	✓	✓	✓	✓	✓
…	✓	✓		✓	✓		

Illustrative Only

Assign Roles & Responsibilities

Each member of the awareness raising team (including partners) will play a role in communications, acting as communications agents. As such, specific roles and responsibilities will need to be identified for team members to ensure the smooth coordination of events that are likely to take place across a wide variety of departments and organisations. An illustration is provided below.



Group	Roles and Responsibilities
Member Stakeholder Group	• Approving the Communications Plan • Ensuring appropriate dissemination of communications • Ensuring adequate sponsorship across all levels • Holding organisation accountable for dissemination of information
Awareness Sponsor	• Supporting the communications strategy and adequate business sponsorship of the projects • Actively supporting the Awareness Raising Forum to ensure alignment with executive sponsorship • Providing adequate resources
Awareness Raising Team	• Leading and developing communications strategy and plan • Coordinating the collection of content from the appropriate content experts within the program • Developing and in some cases delivering communications content against communication plan activities • Ensuring delivery of all required communications activity against the plan

Illustrative Only

Develop Detailed Communication Plan

Once communication objectives, channels, key messages, roles and responsibilities are clearly defined, the awareness raising team will be well positioned to build a detailed communication plan. Developing and executing a targeted communication strategy and customised plans will identify, address and increase awareness in the defined target groups.

The communication plan helps engage the target groups in a structured way and reduces the possibility of missing key stakeholders. Communication plans are typically produced annually (with updates as required) and coordinate all the events to be undertaken for all target groups. This also reduces the possibility of duplicated effort though uncoordinated planning. An illustrative example of an extract from a communication plan is shown below.

Target Audience	*Audience Needs*	*Message*	*Channel*	*Owner*	*Objectives*	*Timing/ Frequency*	*Feedback Tool*
Who will be receiving the message	The communication needs of the audience	The content of the communication	The form in which the message will be sent	Who is responsible for making this communication happen	What we hope to accomplish through this communication	When the communication on event should take place	What will be used to collect feedback
Silver Surfers	Level of knowledge is low to non-existent As the citizens have not grown up with ICT's they may be more doubtful or mistrust technology	Protection of personal information when online	Information distribution through health care solutions Information in co-operation with social security institution	Awareness team	Increase understanding of issue and solutions available	Coincide with National Seniors week	E-mail Telephone

Define Indicators to Measure the Success of the Programme

The effectiveness of an awareness programme and its ability to improve information security can be measured. The need for security awareness is widely recognised, but not many public or private organisations have tried to quantify the value of awareness programmes.

Evaluation of a campaign or programme is essential to understand its effectiveness, as well as to use the data as a guide to adjust the initiative to make it even more successful. It is worth noting that evaluation metrics cannot be universally applied to all target groups as needs and situation differ greatly. This section will highlight metrics for evaluating campaigns aimed at Home Users and to a lesser extent at SMEs as these are the most likely target groups for public awareness campaigns focused on information security. However, with minimal effort, the metric presented can be adapted to suit the needs of other target groups.

The main difference between Home Users and SMEs is that awareness programmes aimed at the latter should focus on the need to develop and implement an information security policy, as well as suggesting means of compliance to the policy within the organisation. This also applies to public institutions and private companies of all sizes[3].

By contrast, public authorities will never be in the position to develop any type of information security policy for Home Users. Therefore, authorities should focus on developing "recommended guidelines" or "best practices" for information security and promote them to the public.

Categories of Measurement

In general, there are four main categories against which to measure security awareness:

- Process Improvement.
- Attack Resistance.
- Efficiency and Effectiveness.
- Internal Protections.

Security awareness can be measured by using and adapting the metrics as proposed by Gartner to suit the needs of Home Users and SMEs. The primary metrics are described below.

1. Process Improvement

This category deals with the development, dissemination and deployment of recommended security guidelines as well as awareness training. Evaluation metrics include:

1. Has the public authority or public-private initiative developed recommended security guidelines for the general public? Are they clear and concise? (Expected answer: yes.)

   For SMEs: Has the SME developed an overall security policy for its organisation? Is it readable and concise? (Expected answer: yes.)

2. Are the recommended security guidelines endorsed by an appropriate authority? Is the initiative adequately sponsored? (Expected answers: yes.)

   For SMEs: Is the overall security policy endorsed at the highest levels of the organisation? (Expected answer: yes.)

3. What percentage of individuals surveyed know that recommended security guidelines exist? How many have seen or read them? (Expected change: increase.)

   For SMEs: What percentage of the SME's employees knows that a security policy exists? How many have read it? (Expected change: increase.)

[3] For more information *and guidance on information security policies see the SANS Security Policy Resource at http://www.sans.org/resources/policies/*

4. What percentage of individuals is confident that they understand the recommended security guidelines? (Expected change: increase.)

   For SMEs: What percentage of employees has demonstrated through automated testing or other processes that they understand the security policy? (Expected change: increase.)

5. What percentage of individuals knows the correct procedure to follow in case of an incident or whom they can call? (Expected change: increase.)

   For SMEs: What percentage of employees knows whom to call if an incident occurs or know the correct procedure to follow? (Expected change: increase.)

6. What is the average time for the authority/initiative to deliver a mass warning email after recognition of a new threat or to post warnings on high-trafficked websites? (Expected change: decrease.)

   For SMEs: What is the average time to deliver a company-wide warning email after recognition of a new threat? (Expected change: decrease.)

7. Has an awareness training programme been developed and deployed? (Expected answer: yes.)

   For SMEs: Has any awareness training been developed? (Expected answer: yes.)

8. What percentage of individuals has attended the training? (Expected change: increase.)

   For SMEs: What percentage of employees has attended the training? (Expected change: increase.)

9. How often is the content of the awareness training updated? (Expected change: increase.)

   For SMEs: What is the average elapsed time since an employee has had awareness training? (Expected change: decrease.)

   For SMEs: Have there been any terminations for security policy non-compliance? How many? (Expected change: decrease.)

   For SMEs: Is there a programme of internal and external security audits? (Expected answer: yes.)

   For SMEs: Do internal and external security audits show improved security policy conformance? (Expected answer: yes.)

2. Attack Resistance

This category is concerned with recognition of a security event and resistance to an attack. Evaluation metrics include:

1. What percentage of surveyed individuals recognises a security event scenario when tested? (Expected change: increase.)
2. What percentage of surveyed individuals fells prey to the chosen scenario? (Expected change: decrease.)
3. What percentage of users failed testing to reveal their password? (Expected change: decrease.)

   For SMEs: What percentage of IT administrators or helpdesk personnel failed to prevent an improper password change attempt? (Expected change: decrease.)
4. What percentage of users activated a "test virus"? (Expected change: decrease.)

3. Efficiency & Effectiveness

This category is focused on efficiency and effectiveness with regard to security incidents. Evaluation metrics include:

1. What percentage of security incidents experienced by individuals had human behaviour as a majority factor in the root cause? (Expected change: decrease.)
2. What percentage of downtime was due to such security incidents? (Expected change: decrease.)

   For SMEs: What is the SME's security awareness spending as a percentage of security spending and/or as a percentage of revenue? (Expected change: decrease.)

4. Internal Protections

This category is concerned with how well an individual is protected against potential threats. Evaluation metrics include:

1. What percentage of an individual's software and hardware purchases has been made with security in mind? (Expected change: increase.)

   For SMEs: What percentage of a SME's software, partners and suppliers have been reviewed for security (including awareness)? (Expected change: increase.)
2. What percentage of an individual's critical data is "strongly" protected? (Expected change: increase.)

   For SMEs: What percentage of a SME's critical data is "strongly" protected, including awareness for data managers, administrators, etc.? (Expected change: increase.)
3. What percentage of an individual's critical data is not protected according to the recommended guidelines? (Expected change: decrease.)

   For SMEs: What percentage of a SME's critical data is not protected according to the company's security standards? (Expected change: decrease.)

4. What percentage of an individual's system surveyed had malicious software or semi-malicious spyware installed? (Expected change: decrease.)
5. What percentage of an individual's system any pirated software installed? (Expected change: decrease.)

Establish Baseline for Evaluation

In the paragraph before, we present metrics to evaluate the effectiveness of an awareness programme. However, to be able to use the metrics, a baseline of the current status needs to be established. By determining the situation beforehand, it is possible to track the benefits brought about by the awareness programme. Evaluations provide an ideal opportunity to assess which components had the highest rate of success, as well as those that were less successful.

Questionnaires and omnibus surveys provide the opportunity to evaluate the effectiveness of programmes. As future evaluation will be compared to this baseline, it is important to note that similar questionnaires and surveys should be re-used at future stages of the initiative.

> *Questionnaires and omnibus surveys provide the opportunity to evaluate the effectiveness of programmes. An Awareness questionnaire sample is available in Annex V.*

Document Lessons Learned

Having completed all the steps within this first phase, time should be allotted for determining and documenting the lessons learned thus far in the programme. The following process may be used as an aide to identify, document and submit lessons learned. However, it is not intended to imply that lessons learned can only be documented as a result of a group process.

Depending upon the programme environment and circumstances, there should be a means by which individual programme team members can write notes or stories and submit them to a designated person for "polishing" and submitting to a repository or database. Such a process should be defined and documented as a result of Step 1 in the procedure.

Key Considerations

When establishing the ground rules at the beginning of the meeting, address the issue of what constitutes lessons learned session and how to provide constructive criticism. Following are some guidelines for providing constructive feedback:

- Lessons learned are programme management-oriented and not work product-oriented.
- Case examples are the most effective means for making a point.
- Criticism should be constructive and directed toward a process, not a person. Participants are encouraged to be thoughtful when providing feedback.
- If there is no way of fixing, improving, mitigating, or influencing an issue, do not discuss it.
- Individual preparation for the meeting expedites the process.
- Keep in mind that this forum is for both criticism and praise; don't take either one too personally because it is a team effort.

A lesson learned debriefing session can actually provide an opportunity to achieve several organisational objectives:

- Discuss alternative approaches to current processes and improve the current programme.
- Demonstrate to staff that their input is valued and listened to.
- Help boost team morale.
- Allow future programmes with similar objectives to learn from this programme's lessons learned.

An Excellent Opportunity for Feedback and Growth

Some staff members have very strong feelings about the way certain portions of a programme are managed. This forum is an excellent opportunity to allow them to relay their opinions, bounce ideas off of others, and discuss different approaches to current processes. If handled correctly by the facilitator, this meeting can provide a forum for team members to vent their frustrations in a positive and constructive manner, as well as provide feedback on how processes can be improved going forward.

The programme manager or team leader must effectively manage the expectations going into the meeting and balance the positive aspects of the debriefing with the realities of the programme schedule. Otherwise, there is the risk of having a counterproductive debriefing session and deflating team morale. Consider that there may be an unspoken assumption on the programme's team's behalf that any identified improvements will be implemented on the current programme. If there is insufficient time to implement any of the recommended changes (lessons learned) on the current programme, communicate this up front.

The team may have identified an issue that could improve the process but it simply takes too much time and effort at this point in the programme to implement the new process (a case of the cure being worse than the disease).

Programme management lessons learned include both positive and negative learning experiences. It is equally important to document what has worked and should be repeated on future programme, as well as it is to record what has or can go wrong and how it may be prevented or addressed in the future.

Tips for Constructive Feedback Sessions

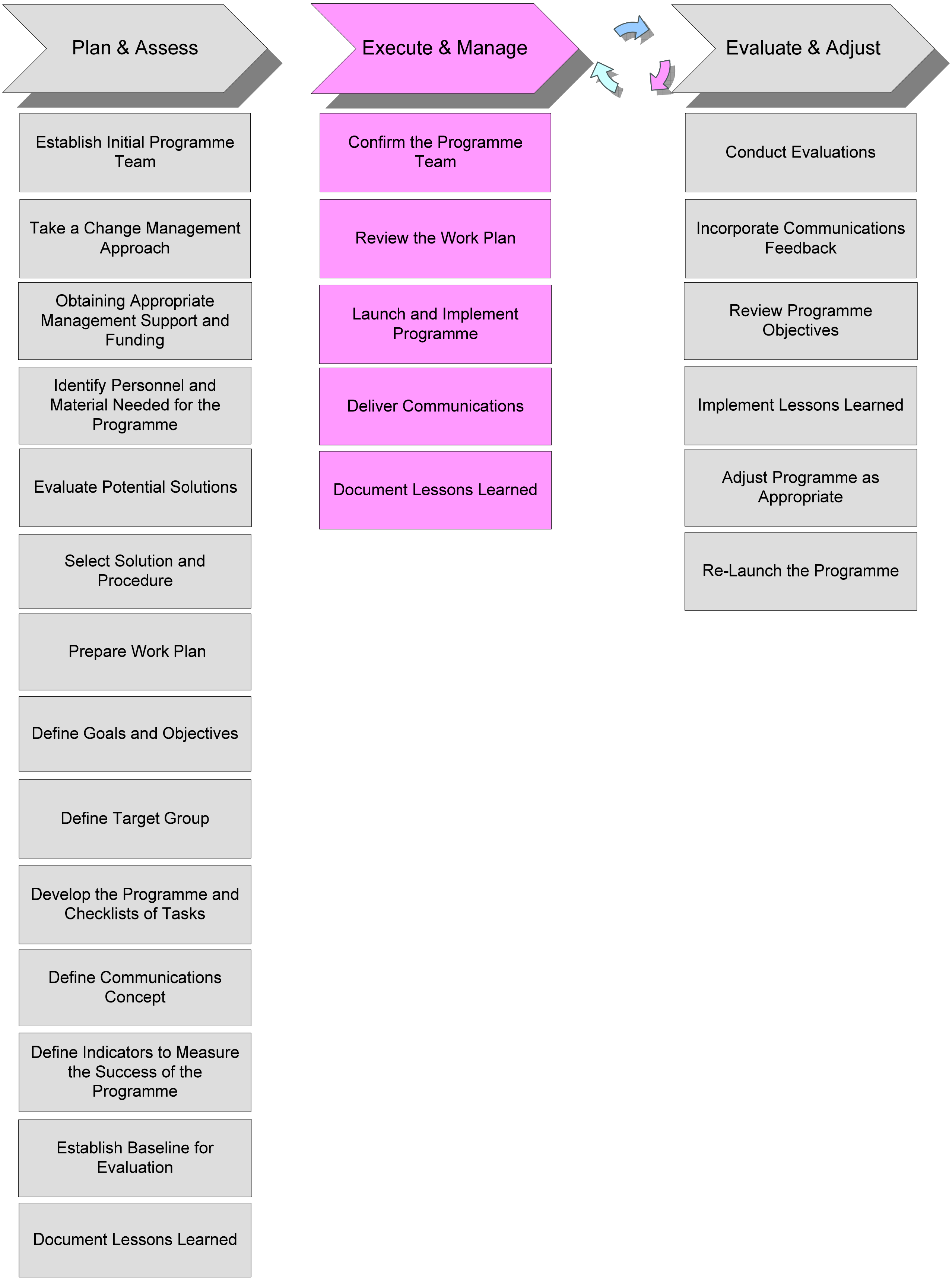
- Consider limiting time during the session. Many times, debriefing sessions can be productive but time consuming. Placing time limits on responses can help keep some semblance of order even in a fairly unstructured or free form environment.
- Consider having team members bring documented ideas to the meeting that they have already thought about. If the dialogue becomes stagnant, be prepared to bring up previous programme difficulties and how they were handled. A great place to start looking for potential improvements is through any status meeting notes or issues log.
- If individuals do not record lessons learned as they think of them, the lessons will probably be lost.
- Team members should be encouraged to keep logs or diaries during the programme. These can be referred to in order to prepare for the debriefing sessions. Team members are encouraged to be thoughtful when making comments and entries into logs and diaries, as the log or diary may become part of the programme documentation at some point.
- Consider adding a lessons learned section to the status reports so that you can go back and easily identify the lessons at the end of a phase or programme.
- Strategically schedule the times to capture the lessons learned. Typically the best times to identify lessons for improving programme management are at the end of a programme, a programme phase, the delivery of a major deliverable, the acquisition or decommissioning of staff, and after performance evaluation reviews. These are periods when any processes that could have been improved are most vividly recalled. The frequency with which these debriefing sessions are held depends upon the size and complexity of the programme.

- Long-term or complex programmes may need to conduct lessons learned debriefings on a periodic basis, while smaller programmes may only need to perform this activity once. Prior to the rolling on of team staff, determine a control process for entering lessons learned and explain the process during team orientation. For example, is it necessary to have a meeting and formalise the lessons learned before the lessons learned are submitted to programme management or can individuals submit lessons learned for the programme on an ad hoc basis? Much of this depends upon the experience of the staff and the judgment of the programme manager.
- Consider conducting interviews with other teams or inviting other teams to your debriefing session to identify any interfacing, communication, or integration lessons learned.

It is important to identify, document and submit lessons learned. The use of a tool is recommended to manage effectively the work. A lesson learned capture form template is available in Annex VI.

Phase II
Execute & Manage

Phase II - Execute and Manage



Plan & Assess
Establish Initial Programme Team
Take a Change Management Approach
Obtaining Appropriate Management Support and Funding
Identify Personnel and Material Needed for the Programme
Evaluate Potential Solutions
Select Solution and Procedure
Prepare Work Plan
Define Goals and Objectives
Define Target Group
Develop the Programme and Checklists of Tasks
Define Communications Concept
Define Indicators to Measure the Success of the Programme
Establish Baseline for Evaluation
Document Lessons Learned
Execute & Manage
Confirm the Programme Team
Review the Work Plan
Launch and Implement Programme
Deliver Communications
Document Lessons Learned
Evaluate & Adjust
Conduct Evaluations
Incorporate Communications Feedback
Review Programme Objectives
Implement Lessons Learned
Adjust Programme as Appropriate
Re-Launch the Programme

Confirm the Programme Team

In the second phase, the programme moves into execution mode. Each member of the awareness raising team will need to play a specific role to implement and manage the initiative. Before launching the programme, confirm the team that will be responsible for both execution and results.

Review Work Plan

Before kicking-off the programme, update the work plan and determine programme milestones so that they comply with goals and objectives, as well as budget requirements.

Launch and Implement Programme

The work done in the above steps combined with those in the previous phase may have seemed lengthy and bureaucratic, but at this point all the time spent on deciding the requirements, designing the solution and refining the outcome will pay off as the implementation will go smoother and be more effective.

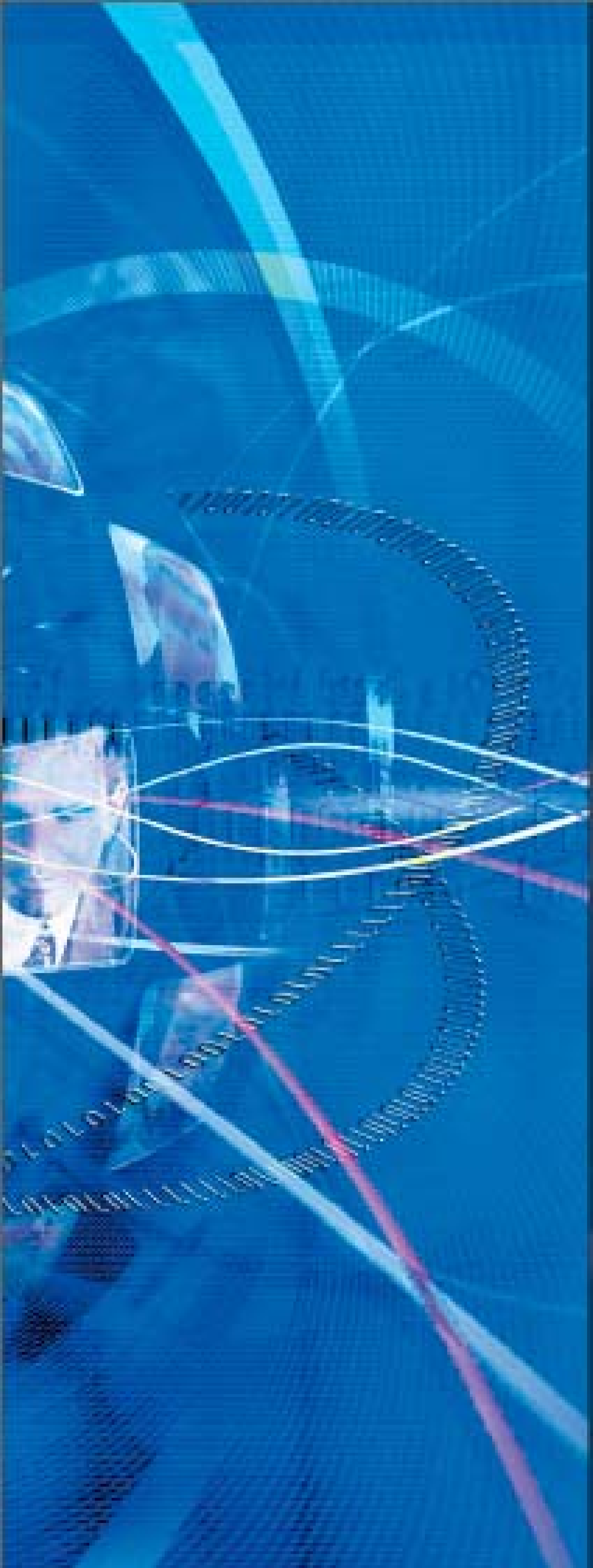
With a well-written plan in place as well as the appropriate resources to deliver it, the time has come to call on the support of your internal colleagues and chosen external suppliers to build and deliver the programme with the goal of realising the benefits of information security awareness.

Deliver Communications

Raising awareness is about communicating to the selected target groups. It is now time to implement the communications plan. It is equally important to collect feedback on the communications the programme has delivered. This feedback will provide valuable information that should be taken into consideration for future cycles of communications delivery.

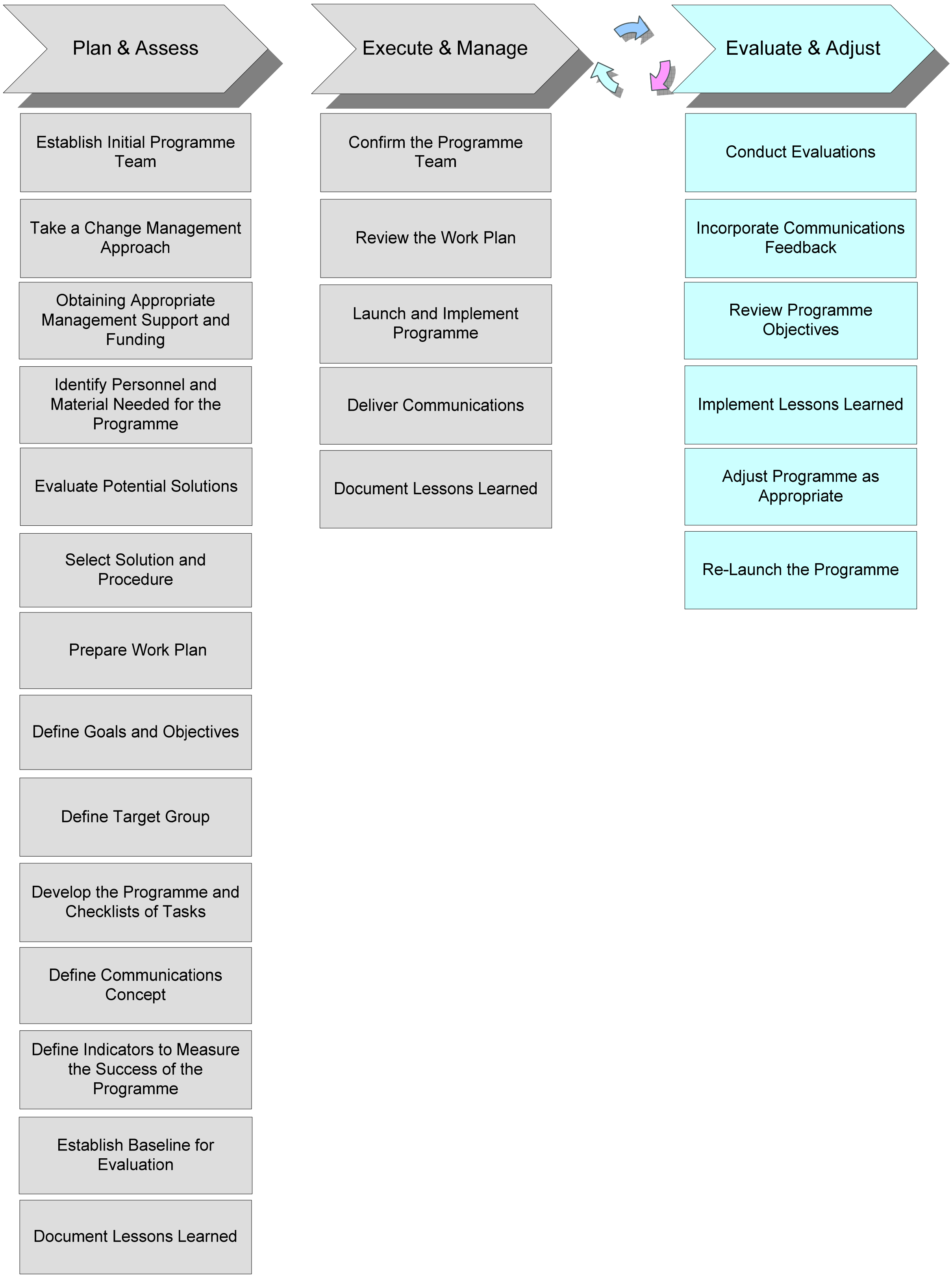
Document Lessons Learned

As the programme has been launched and implemented, it is important to capture lessons learned during this second phase. The procedure completed at the end of Phase I should be repeated. It will be interesting to compare the historical evolution of the programme from this learning perspective.



Phase III
Evaluate & Adjust

Phase III - Evaluate and Adjust



Plan & Assess

Establish Initial Programme Team

Take a Change Management Approach

Obtaining Appropriate Management Support and Funding

Identify Personnel and Material Needed for the Programme

Evaluate Potential Solutions

Select Solution and Procedure

Prepare Work Plan

Define Goals and Objectives

Define Target Group

Develop the Programme and Checklists of Tasks

Define Communications Concept

Define Indicators to Measure the Success of the Programme

Establish Baseline for Evaluation

Document Lessons Learned

Execute & Manage

Confirm the Programme Team

Review the Work Plan

Launch and Implement Programme

Deliver Communications

Document Lessons Learned

Evaluate & Adjust

Conduct Evaluations

Incorporate Communications Feedback

Review Programme Objectives

Implement Lessons Learned

Adjust Programme as Appropriate

Re-Launch the Programme

Conduct Evaluations

As stated in Phase I, the effectiveness of an awareness programme and its ability to improve information security can be measured, despite some claims to the contrary.

The baseline determined prior to the launch of the programme provides a picture of the beginning situation within the target groups. Follow-up questionnaires and omnibus surveys allow the tracking of progress of awareness.

Incorporate Communications Feedback

The feedback captured when delivering the programme's communications should be reviewed with a view of how future communications might be improved and made more effective. This information should be combined the results derived from the evaluation metrics.

Review Programme Objectives

The programme's objectives need to be revisited in light of the effectiveness results. What has the team achieved? Have the benefits been realised? If so, there is surely cause for celebration. If not, what is required to achieve the desired results? Or do objectives need to be modified? Reviewing the objectives allow for a serious assessment to take place.

Implement Lessons Learned

Evaluate the lessons learned from the awareness programme. Which lessons can be applied to increase the effectiveness and success of the programme in the future? The main focus should be to learn from past experiences both positive and less so; then put that learning into practice.

Adjust Programme as Appropriate

The experiences gained since the launch of the programme provide the knowledge and understanding to adjust the programme to make it more successful. The kind of adjustments required could involve each and every activity and task performed in the context of the programme. The key is to make adjustments while maintaining the focus on the programme objectives and goals.

Re-launch the Programme

Now that the programme has made adjustments based on what was learned to date, the next step is re-launch the programme, completing the tasks in Phase II. It is an ideal opportunity to follow-up on additional topics or to reinforce subjects that have been covered at an earlier stage.

Obstacles to Success

Implementing a successful security awareness programme can be a difficult task. Even some of the best-planned programmes can come up against some large barriers and obstacles. However, understanding some of these common obstacles will help to overcome them during the planning and implementation phases of the programme.

General

1. **Implementation of New Technology**

   When new technology is implemented, it often requires a behaviour change or new level of user understanding. This alone is not an issue, however, sometimes technology moves faster than or independently from the awareness programme. It could happen that the awareness team is not up-to-date nor adequately informed of these types of educational opportunities until it is too late. This is why it is important for a security awareness programme to emphasise internal communications, as well as ensure that an emergency or crisis communication strategy is in place.

2. **One-Size-Fits-All**

   Some security awareness programmes fail to segment their audience adequately and appropriate messages are not delivered. This results in messages being ignored. Information technology users receive hundreds of messages every day from a multitude of sources. It is critical to segment audiences and ensure that people only receive the messages they need. A one-size-fits-all strategy might be easier to develop and implement, but it will not be effective.

3. **Too Much Information**

   Over-education is quite a common mistake. The public tends to have a threshold of how much information they are willing to accept from any one source. If individuals are inundated with a constant barrage of messages, it is likely to turn their attention away. Even after having taken the necessary steps to segment the audiences and only sending appropriate messages, too much information is simply too much. An awareness programme does not have to be built over a very short period of time. Take the time to be open to the audiences' needs and find the right balance.

4. **Lack of Organisation**

   Many awareness programmes fail to develop consistent processes and strategies for delivering messages to users. Without a consistent style, theme and delivery, it is difficult for the user to engage in the programme or even know what to expect. It is key to develop consistency in communications. This will also help establish an identity for the programme and build a relationship with the audiences.

5. Failure to Follow-Up

It is quite common for security awareness programmes to be launched with great enthusiasm only to fizzle out with little success. Many programmes fail to establish and maintain a regular cycle of communications. It is important to establish regular communications so that users receive regular reminders of the key messages. In addition, many programmes fail to follow-up with their audiences and solicit feedback. It is critical to listen to the audiences and adjust the programme based on their needs.

6. Getting the Message Where it will Have an Effect

Often it is a real challenge to deliver the right message to the right audience. This is especially true in large communities. For example, even if a local council has already developed a thorough communication strategy with a well-maintained process for targeted communications, delivering the right messages to right audience can still be very difficult. Email groups based on individual criteria can be helpful, but do not fully solve the problem.

In some cases, although a particular audience has been identified, it might be a challenge to figure out specifically who belongs in the audience. For example, there may be a message that needs to be delivered to one particular segment. For example, parents may have been identified based on school registration, but it is likely that the list is not complete due to reasons such as children living full-time with another parent. The challenge is how best to identify and maintain a list that ensures all pertinent messages get to all of the parents every time. This is a difficult task.

7. Lack of Resources

This usually stems from the lack of management support. Without management support, it is difficult to secure adequate resources; without adequate resources, a security awareness programme is limited in what it is able to achieve.

8. No Explanation of Why

Many security awareness programmes fail to educate users on why security is important. All other aspects are covered, but unfortunately the information that is most likely to motivate users to change behaviour is omitted. Users who understand why certain behaviours are risky are most likely to take ownership of the issue and change their behaviour. For example, if guidelines on a new password process with more stringent complexity rules are communicated, users will most likely view the new process as nothing more than an inconvenience. However, if it is also communicated how passwords are cracked and misused and the potential impact this could have, and then users are much more likely to take ownership and follow the new guidelines.

9. Social Engineering

Social engineering may not necessarily have an impact on the implementation of an awareness programme, but can affect its success. The issue is important to address because it specifically targets the “people link” that an awareness programme is trying to strengthen. Social engineering is the art of preying on natural human tendencies to trust and help others in order to obtain information that would otherwise be hard to obtain. Most people believe that no one would purposefully try to trick or manipulate the public, but, in reality, social engineering is one of the most widely used forms of attack.

Attackers often choose this method because it is surprisingly easy and does not take a great deal of time. Why would attackers want to spend hours trying to crack your password when they can contact a member of the public directly, impersonate a bank's or other institution's help desk, and then trick a gullible person into giving over sensitive information? Some of the most common social engineering methods include impersonation, flattery, and sense of urgency as well as third-party authorisation. It is critical to develop and implement an educational strategy that specifically addresses this issue. Unfortunately, as illustrated by Granger, Steven and Berg, recognised information security and social engineering experts, social engineering is a form of attack that can trick even the most security savvy users.

Specific to SMEs

Below are some obstacles to success faced specifically by SMEs. However, the leanings discussed could be applied universally to information security awareness programmes aimed at other target groups.

1. Changing Long-Established Behaviours

In many organisations, security is often implemented as an afterthought. Because security is not always integrated from the very beginning, users have months, weeks and even years to develop bad habits. This makes the challenge of implementing a security awareness programme even more difficult. Not only is there a need to educate users on security, but also users need help to “unlearn” any bad habits that they may have acquired. In addition, such users tend to have more difficulty buying into the value of security. As far as they are concerned, the organisation has operated just fine for many years without security. New security requirements are viewed as unnecessary changes that make their lives more difficult.

2. “Security is an information technology department problem, not mine . . .”

Many users share the perception that security is the sole responsibility of the IT department. They tend to limit their role to the bare minimum of compliance to maintain their jobs rather than the big picture of how to be a part of the solution. While adhering to policy is a good start, there is much more that can be done. It is important that users understand that IT staff cannot tackle information security alone.

3. Lack of Management Support

Obtaining management support is one of the most essential aspects of a security awareness programme. It is also one of the most challenging. For security messages to be effective, they must be supported from the top down. Even though many managers express their desire to support security initiatives, putting it into action is another story. This is because managers have their own roles and responsibilities. Their primary goal is to meet their business objectives and it is often difficult to find room for security issues, no matter how much they believe security is important.

Critical Success Factors

The main factors for success of any information security programme include:

- A baseline of current status needs to be determined before implementing or re-launching an awareness programme.
- Security awareness programmes will fail if they do not reach the target audience.
- Use NGOs, institutions, banks, ISPs, libraries, local trade organisations, community centres, computer stores, community colleges and adult education programmes, schools and parent-teacher organisations to get the message across.
- Getting publicity is a vital part of any awareness campaign as it will multiply the impact by increasing the number of people who hear the message.
- Establishing public-private partnerships when required.

For programmes aimed at SMEs, keep in mind that:

- Security awareness programmes for SMEs will fail if they are counter to organisational culture or unsupported by senior management.
- Building continued support for programmes within SMEs requires a demonstration of how well security awareness efforts are working.

The metrics discussed in this Guide can demonstrate security awareness success or failure.

Conclusion

European citizens are both increasingly mobile and connected to the Internet. As a result, they are demanding dependable, secure connectivity, anywhere, anytime. This new trend opens the door to thousands of possibilities for Europe's communities. However, this surge in push-and-pull communication also brings with it security issues that today's governments are obligated to resolve.

Any system is only as strong as its weakest component. Human error can undermine even the most stringent information security framework. Awareness of the risks and available safeguards is the first line of defense for the security of information systems and networks.

ENISA hopes this guide will provide Member States with a valuable tool to prepare and implement awareness raising initiatives and programmes. Providing information security is a huge challenge in itself; awareness raising among select target audiences is an important first step towards meeting that challenge.

Bibliography

Information Package: Raising Awareness in Information Security – Insight and Guidance for Members States

http://www.enisa.europa.eu//deliverables/index_en.htm

Building a Security Awareness Program - CyberGuard
http://www.gideonrasmussen.com/article-01.html

NIST 800-50 Security Awareness and Training Program
This NIST publication provides detailed guidance on designing, developing, implementing, and maintaining an awareness and training programme within an agency's IT security programme.

http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Security Awareness Tips - Gideon T. Rasmussen
http://www.gideonrasmussen.com/sectips/

Security Awareness Toolbox - The Information Warfare Site
The Security Awareness Toolbox contains many useful documents and links.
http://www.iwar.org.uk/comsec/resources/sa-tools/

SANS Reading Room - Security Awareness Section
http://www.sans.org/rr/whitepapers/awareness/

SANS Security Policy Resource
http://www.sans.org/resources/policies/
University of Arizona Security Awareness Page
http://security.arizona.edu/awareness.html

NoticeBored information security policy management system with creative security awareness materials
http://www.noticebored.com/html/white_papers.html and http://www.isect.com/
Human Firewall Council
http://www.humanfirewall.com/

Cybersecurity Awareness Resource Library
http://www.educause.edu/CybersecurityAwarenessResourceLibrary/8762
The UK Government's ITSafe Service
http://www.itsafe.gov.uk/
CERT's Virtual Training Environment
https://www.vte.cert.org/vtelibrary.html
Success strategies for security awareness
http://techrepublic.com.com/5100-10878_11-5193710.html#

Building a Security Awareness Program - Addressing the Threat From Within

By Gideon T. Rasmussen

http://www.gideonrasmussen.com/article-01.html

CIS Center for Internet Security

http://www.cisecurity.org/resources.html

Information Systems Security Association

http://www.issa.org/

US CERT Cyber Security Tips

Advice about common security issues for non-technical computer users.

http://www.us-cert.gov/cas/tips/index.html

Common Sense Guide to Cyber Security for Small Businesses

http://www.us-cert.gov/reading_room/CSG-small-business.pdf

Home Network Security

Gives home users an overview of the security risks and countermeasures associated with Internet connectivity, especially in the context of "always-on" or broadband access services (such as cable modems and DSL).

http://www.us-cert.gov/reading_room/home-network-security/

The National Cyber Security Alliance (NCSA) for cyber security awareness resources and education for home user, small business, and education audiences.

http://www.staysafeonline.org/

The Yahoo security awareness group provides a forum to discuss awareness programme methodologies and share security awareness tips

http://groups.yahoo.com/group/security-awareness/

The Society for the Policing of Cyberspace (POLCYB)

http://www.polcyb.org/index.htm

Raising Citizen Awareness of Information Security: A Practical Guide, eAware, 2003

Templates & Samples

Annexes - Templates and Samples

Annex I - Request for Proposal Sample

The <XYZ> Association, a new organisation in <Location>, is seeking a consultant or consultants to assist in its initial set-up, implementation and in the analysis of possible awareness programme. See the associated "Agreement for Services" which would typically follow this proposal, assuming the client finds a consultant that he or she likes and enters into an agreement with them.

Situation

<*XYZ*> was established in <*Date*> to assist several existing local governmental groups in <Location> and to promote and coordinate <*Activity*> in the area. <*Location*> is a town of 17,500 people. To date, <*XYZ*> has non-profit and tax-exempt status and a board of directors, but no staff or office space. A maximum budget for the consultancy work of <*Amount*> has been established at this time.

Tasks to be accomplished

Continue development of the Association and plan for its future work with a task force of member organisations to determine what joint needs the <*XYZ*> should address and how and to develop a campaign to build awareness. Specifically:

- Design work plan based on stated goals and objectives.
- Design a <*XYZ*> newsletter and publish the first issues.
- Develop annual <*XYZ*> budget projections for the campaign over the next three years.
- Develop means to measure the effectiveness of the campaign.
- Design methodology for capture of lessons learned and communications feedback and incorporate those into an updated work plan.

This campaign should begin in <*Date*> and be completed no later than <*Date*>*.*

How to submit a proposal

Interested consultants should submit the following, no later than <*Date*>*,* to <*Person*> at <*XYZ*>*.* For more information, contact <*Persons*>*.*

1. A proposal describing your qualifications (or the qualifications of the team of consultants) and how the tasks described above would be carried out
2. A firm estimate of fees to be charged, and an estimate of expenses that would be incurred
3. CVs of all consultants who would be involved in the project
4. Names, phone numbers and contact people at three non-profit organisations who have been your clients during the last 18 months, whom we can all on as references.
5. Interviews with finalists will be held during the week of <*Date*>*.*

Annex II - Weekly Status Report Template

Weekly Status Report

DATE

PROJECT / PROGRAMME

People and Organisation

Tasks completed last week

Tasks planned for next week

Risks

Things that may happen to impact our plans and activities

Description	Source	Potential severity	Probability	Mitigation plan(s)

Issues

Things that are happening that impact our plans and activities

Description	Source	Severity	Status	Mitigation plan(s)

Calendar Forecast for next week

Where you are and what you are doing (on leave / training / workshop / other client commitment etc.)

Day	Morning	Afternoon
Monday		
Tuesday		
Wednesday		
Thursday		
Friday		

Annex III – Work Plan Sample

Activities	Target Activity Start Date	Target Activity Completion Date	Outputs
List each activity and provide a brief description of the activity and any sub-activities (main purpose, etc.)			For each activity listed, indicate what will be produced.
I. Plan and Assess			
- Establish initial programme team	April 2006	April 2006	- team identified.
- Take change management approach	April 2006	April 2006	- programme principles identified.
- Obtain appropriate management support and funding	April 20066	June 2006	- explicit management support and budget approval
- Identify personnel and material needed for programme	May 2006	May 2006	- shortlist of personnel and materials
- Evaluate potential solutions	May 2006	June 2006	- decision to keep in-house or outsource - prioritised list of options - programme policy and procedures - programme templates for reporting - roles and responsibilities
- Select solution and procure	July 2006	July 2006	- signed contract
- Prepare work plan	June 2006	June 2006	- work plan
- Define goals and objectives	June 2006	July 2006	- programme goals and objectives formalised and agreed
- Define target groups	June 2006	July 2006	- target groups identified and needs documented
- Define the programme and checklist of tasks	June 2006	July 2006	- programme developed
- Develop communications concept	June 2006	July 2006	- message established - message detailed - message tested - communications partners determined - communications channels selected - detailed communications plan - feedback mechanism.
- Define indicators to measure the success of the programme	June 2006	July 2006	- evaluation metrics
- Establish baseline for evaluation	June 2006	July 2006	- assessment of present situation
- Document lessons learned	July 2006	July 2006	- lessons learned recorded
II. Execute and Manage			
- Confirm programme team	August 2006	August 2006	- team confirmed
- Review work plan	August 2006	August 2006	- final work plan
- Launch and implement programme	October 2006	January 2007	
- Deliver communications	October 2006	January 2006	- communications plan implemented
- Document lessons learned	January 2007	January 2007	- lessons learned recorded
III. Evaluate and Adjust			
- Conduct evaluations	February 2007	March 2007	- survey results
- Incorporate communications feedback	February 2007	March 2007	- communications feedback

- Review programme objectives	February 2007	March 2007	-programme objectives
- Implement lessons learned	March 2007	April 2007	- updated lessons
- Adjust programme as appropriate	March 2007	April 2007	-updated work plan
- Re-launch the programme	May 2007		

Annex IV - Target Group Data Capture Template

Target Group			
Definition			
Category		Interests, Needs	
Sub Category		Knowledge	
Size / Dimension		Channel	
Geography			

Sample/ Recommendations	

Annex V - Awareness Questionnaire Sample - for Use by a Public Authority

[*Name of organisation*] is conducting a study to help determine ways of educating citizens of [*Name of community*] about information security issues. We would appreciate if you could spare 10 minutes to answer a few brief questions regarding information security?

1. How to you access the internet:
a. ____A dial-up connection
b. ____ADSL (broadband) connection
c. ____Company Internet

2. Where do you use your computer (check all that applies):
a. ____Home
b. ____Office
c. ____Public-access location (school, library, community centre)
d. ____Internet Café
e. ____Internet / Phone Centre
f. ____Other (please indicate where)______________________________

3. Many people define safety as protection from adverse effects. With this in mind, on a scale of one to five, with one being very concerned, and five being the least concerned, how concerned are you about the safety of your information technology assets (computer, peripherals, electronic data, etc)?

1	2	3	4	5
Very		Somewhat		Least

4. Which of the following do you think poses the greatest threat to your information technology? You may select any that applies:
a. ____viruses and worms
b. ____spam and other unsolicited emails
c. ____hackers
d. ____fraudulent schemes
e. ____malicious software (e.g. spyware)
f. ____faulty computer hardware
Other____

5. Are you aware that the [*Public Authority*] will evaluate the potential threats to the public's information technology, and that the information could help you design a plan to protect you from potential threats?

Yes, I am aware of this

No, I am not aware of this

6. On a scale of one to five, with one being very knowledgeable and five being the least knowledgeable, please rank your knowledge of the steps that can be taken to protect your information technology assets:

1	2	3	4	5
Very		Somewhat		Least

7. Do you have any of the following is in place to protect your computer and electronic data? Please indicate all that apply.

a. ____Anti-virus software that is updated regularly

b. ____Firewall

c. ____Anti-spam filter

d. ____Good password practices

e. ____Process of regular backup of data

f. ____ Up-to-date Internet browser with encryption

g. ____Others please indicate___________________________________

8. Which would be the best way to provide you with information on how protect yourself from potential dangers? In other words, are you most likely to pick up information from the:

a. ____Radio

b. ____Television Adverts

c. ____Your local newspaper

d. ____Newsletters that come to your home

e. ____Civic and neighbourhood meetings

f. ____ Posters

g. ____Other (please describe) ____

Thank you so much for participating in this survey. We plan to use your answers to help us develop information in order to raise awareness of the importance of information security.

Please check here if you would like to receive additional information on information security

o **Yes**

o **No**

Annex VI - Lessons Learned Capture Form Template

<table>
<tr><td colspan="4" rowspan="2"><b>LESSONS LEARNED</b></td><td>FILE NO.</td><td>Page of</td></tr>
<tr><td colspan="2">CATEGORY (Primary/Alternate):</td></tr>
<tr><td colspan="4">TITLE/SUBJECT:</td><td colspan="2">KEYWORDS:</td></tr>
<tr><td colspan="6">EVENT DESCRIPTION:</td></tr>
<tr><td colspan="6">LESSONS LEARNED:</td></tr>
<tr><td colspan="6">RECOMMENDATIONS:</td></tr>
<tr><td colspan="3">ATTACHMENTS:</td><td colspan="3">REFERENCES:</td></tr>
<tr><td>SUBMITTED BY:</td><td>PROJECT/OFFICE:</td><td colspan="2">ORG./COMPANY:</td><td>LOCATION:</td><td>DATE OF OCCURRENCE:</td></tr>
<tr><td>TELEPHONE:</td><td>EMAIL:</td><td colspan="2">SPECIALISATION:</td><td>BUILDING/ROOM:</td><td>DATE SUBMITTED:</td></tr>
</table>

European Network and Information Security Agency
P.O. Box 1309
71001 Heraklion
Greece
Tel: +30 2810 39 1280
http://www.enisa.europa.eu