The new users' guide:

How to raise information security awareness

November | 10

enisa
European Network and Information Security Agency

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the Agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details:

For general enquiries on information security awareness matters, please use the following details:

e-mail: Isabella Santa, Senior Expert Awareness Raising — awareness@enisa.europa.eu

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

The new users' guide:
How to raise information security awareness

November 2010

Contents

Executive summary

Two years after the publication of *The new users' guide: How to raise information security awareness*, the European Network and Information Security Agency (ENISA) reviewed this document in the light of new research and analysis conducted in the field. This version contains new activities and case studies as well as templates and samples.

We have overcome several obstacles to make four major improvements. We have added more detailed descriptions of activities and statistics from research organisations, reviewed subprocesses, included new recommendations, improved the layout, and allowed for more flexibility in reading. To this end an index has been included.

Of the four major improvements, the one with a visual impact is the introduction of the breakdown of the subprocesses where the core processes covering a single business area are described. The guide describes the main processes necessary to plan, organise and run information security awareness raising initiatives: plan, assess and design, execute and manage, evaluate and 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 and tasks as well as the execution and assessment of any programme. The guide aims to deliver a consistent and robust understanding of major processes, activities and tasks among readers.

The second major improvement, probably the most important and helpful for some users, is the identification of key activities to obtain support and funding from senior management. Programme costs and business benefits should be identified to allow organisations to assess the effectiveness of awareness initiatives in order to fund them. In particular some financial tools are described to be able to identify and capture value to the stakeholders. Samples of financial calculations motivating information security awareness initiatives are included.

The third major improvement is the provision of case studies and experiences from other organisations dealing with different awareness matters, to enable readers to identify key problems, issues, solutions, making the suggested activities and recommendations more effective and presented in concrete ways.

The fourth major improvement is the inclusion of a more complete set of templates and samples of suggested tools. They are included to help the readers to prepare and implement awareness initiatives. These include, among others, a lessons learned template, an information security awareness baseline worksheet, an awareness questionnaire, a target group data capture form and a poster sample.

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 the main factors for success of any information security initiative.

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

PART 1: THE IMPORTANCE OF INFORMATION SECURITY AWARENESS

Introduction

In today's digital age where we live and work, citizens and businesses find information communication technologies (ICTs) invaluable for carrying out daily tasks. At the same time, more and more citizens and businesses are the most likely to suffer security breaches. This is due to vulnerabilities in these new and existing technologies, together with device convergence, the significant increase in '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 other malicious software, system failure or data corruption, or they may be socially motivated, for example through theft of assets or other incidents caused by staff. In an age ever more reliant on digital information, there is an increasing number of dangers.

Recent stories have highlighted that a considerable number of end-users are unaware of their exposure to security risks. Given the rising level of breaches seen recently, it is more critical than ever that organisations raise security awareness by turning users into a first line of defence. All industry sectors have experienced staff-related breaches, though technology companies fared better than most. For example, in the United Kingdom, four computer discs containing the details of 17 990 current and former staff were lost when they were sent between Whittington Hospital NHS Trust in north London and a firm providing IT payroll services; a large charity was infected by the Conficker worm after it was brought in on an infected USB stick; a Midlands-based technology company lost a USB stick containing a customer's test data; two computer discs holding the personal details of all families in the UK with a child under 16 have gone missing; a courier carrying a large financial services provider's backup tapes was robbed; a charity infringed data protection laws when it disposed of an old computer without wiping the hard drive ([1]); in Sweden, a misplaced USB flash drive containing both unclassified and classified information, such as information regarding improvised explosive devices (IEDs) and mine threats in Afghanistan, was found on a public computer and handed over to the Swedish armed forces ([2]); in the United States, USB flash drives with US Army classified military information were up for sale at a bazaar outside Bagram, Afghanistan ([3]); details of three million British learner drivers were lost in the United States

([1]) 'UK's families put on fraud alert', *BBC News*, 20 November 2007, available at http://news.bbc.co.uk/2/hi/7103566.stm (last visited on 29 October); PricewaterhouseCoopers LLP (UK), *Information security breaches survey 2010*, available at http://www.pwc.co.uk/eng/publications/isbs_survey_2010.html (last visited on 29 October 2010); Simpson, Aislinn, 'NHS: Personal details of 18,000 staff 'lost in the post'', *Telegraph.co.uk*, 15 September 2008, available at http://www.telegraph.co.uk/health/2965231/NHS-Personal-details-of-18000-staff-lost-in-the-post.html (last visited on 25 November 2010); see also ENISA*, Secure USB flash drives,* 2008, available at http://www.enisa.europa.eu/act/ar/deliverables/2008/secure-usb-flash-drives-en/at_download/fullReport (last visited on 19 November 2010).

([2]) Jevans, Dave, *Privacy and identity theft,* IronKey, available at http://blog.ironkey.com/?cat=9&paged=2 (last visited on 20 May 2008).

([3]) Watson, Paul, 'US military secrets for sale at Afghanistan bazaar', *Los Angeles Times*, 10 April 2006*.*

([4]) Ford, Richard, 'Disc listing foreign criminals lost for year', *The Times,* 20 February 2008, available at

[4]; a Californian public employees' retirement system mailing that exposed members' social security numbers underscores the need to place equal emphasis on securing business and customer data — whether it resides in data centres, networks, or print and mail operations [5]; in Iran, Indonesia, India, Ecuador, the United States, Pakistan, and Taiwan, infected USB flash drives were used to penetrate control systems of industrial facilities and utilities [6].

The security landscape is continually changing. With the advancement and proliferation of security threats, the information security solutions of today will be obsolete tomorrow. Most analysts report that the human component of any information security framework is the weakest link. A lack of awareness among staff reduces the strength of the first line of defence [7]. In this case, only a significant change in user perception or organisational culture can effectively reduce the number of information security breaches.

Purpose

ENISA recognises that awareness of the risks and available safeguards is the first line of defence for security of information systems and networks [8]. This document aims at providing practical and effective advice to public and private organisations allowing the reader to prepare and implement information security awareness initiatives [9] that apply to them.

In particular, the information covered features step-by-step advice to help form the basis of designing, developing and implementing an effective and targeted awareness programme, through evaluation of the programme. The document includes guidelines on how identify awareness needs, develop a plan, and get organisational buy-in for the funding of awareness initiative efforts. Furthermore, it also describes how to:

- ✓ Select awareness topics.
- ✓ Build a business case.
- ✓ Build a communication framework.
- ✓ Implement an awareness initiative, using a variety of channels.
- ✓ Evaluate the effectiveness of the programme.
- ✓ Update and improve the programme.

[4] Ford, Richard, 'Disc listing foreign criminals lost for year', *The Times,* 20 February 2008, available at http://www.timesonline.co.uk/tol/news/politics/article3399712.ece (last visited on 15 July 2008).

[5] ENISA*, Secure printing,* 2008, available at http://www.enisa.europa.eu/doc/pdf/ENISA_secure_printing.pdf (last visited on 19 November 2010); Pete Basiliere, *Information breach highlights production print and mail vulnerabilities,* Gartner, 18 September 2007.

[6] Clayton, Mark, 'Stuxnet spyware targets industrial facilities, via USB memory stick', *The Christian Science Monitor*, 23 July 2010, available at http://www.csmonitor.com/USA/2010/0723/Stuxnet-spyware-targets-industrial-facilities-via-USB-memory-stick (last visited on 17 November 2010).

[7] PricewaterhouseCoopers LLP (UK), *Information security breaches survey 2010*, available at http://www.pwc.co.uk/eng/publications/isbs_survey_2010.html (last visited on 29 October 2010).

[8] OECD, *Implementation plan for the OECD guidelines for the security of information systems and networks: Towards a culture of security,* DSTI/ICCP/REG(2003)5/REV1, Working Party on Information Security and Privacy, OECD, 2003, available at http://www.oecd.org/dataoecd/23/11/31670189.pdf (last visited on 25 November 2010); Herold, Rebecca, *Addressing the insider threat,* IT Compliance in Realtime, Realtime publishers, May 2008, Volume I, Number 3, available at http://nexus.realtimepublishers.com/RTITC.htm (last visited on 31 July 2008).

[9] Within the guide, we refer to awareness initiative and programme indistinctly.

This new guide relies on the basis of studies and analysis conducted by ENISA and on information that is publicly available or has been supplied to ENISA by organisations and members of the ENISA Awareness Raising (AR) Community ([10]).

Scope

The scope of this guide is for ENISA to:

- ✓ Illustrate a forward-thinking methodology on how to plan, organise and run an information security awareness raising and training initiative.
- ✓ Provide a common approach to executing and managing an awareness raising and training initiative and establish a common language.
- ✓ Highlight potential risks associated with the awareness initiative in an effort to avoid such issues in future programmes.
- ✓ Serve as a jumpstart for awareness programme development.
- ✓ 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.

Audience

A few years ago, companies still viewed information security as a technology cost centre. One sign of this was the fact that the most common reporting channel for the Chief Information Security Officer (CISO) was the Chief Information Officer (CIO). Nowadays, information security is a much broader concept than technology as it is recognised that information security is more aligned with the business than with IT. Thus, at present the CISO reports to the business, typically to the Board and the Chief Executive Officer (CEO) ([11]).

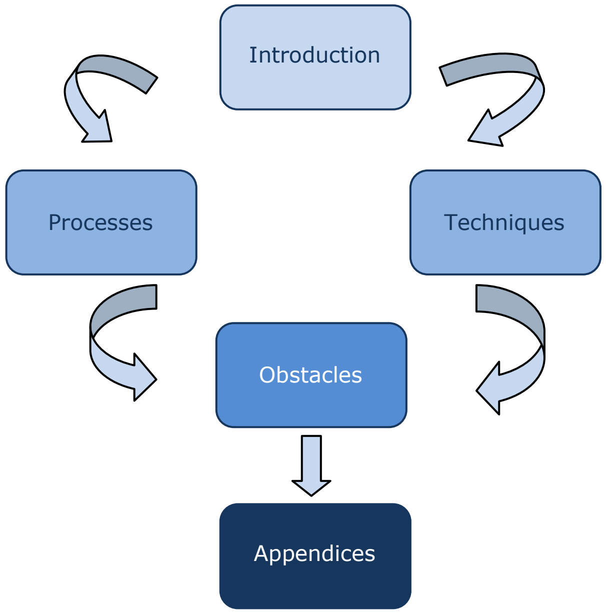
As a result, the guide is intended to several key audiences in either public or private, large or small organisations, including CEOs, CISOs, CIOs, IT security managers and staff, middle managers, contractors, and human resources personnel.

Structure of the guide

There are five major parts to this guide, as shown below.

([10]) The Awareness Raising (AR) Community is a subscription-free community open to experts who have an interest in engaging in raising information security awareness within their organisations. The AR Community was launched in February 2008 and is designed to engage with the awareness raising section of ENISA in its mission to foster a culture of information security, with the aim of supporting the section in its activities. See ENISA, *Key facts and figures about the AR Community and its members (May 10)*, 2010, available at http://www.enisa.europa.eu/act/ar/deliverables/2010/facts-and-figures-may-10 (last visited on 19 November 2010).

([11]) PricewaterhouseCoopers LLP, *2011 Global state of information security survey*, 2010, available at http://www.pwc.com/gx/en/information-security-survey/index.jhtml (last visited on 29 October 2010).



Introduction presents the basic principles governing information security and how awareness addresses them; it also shows how awareness fits with external and internal factors.

Processes describes the ENISA process model, explaining what has to be done to manage an awareness programme by bringing together and applying the principles in a successful manner.

Techniques explains some techniques that are specific to awareness raising.

Obstacles explains and describes the major barriers and obstacles and how to overcome them during the planning and implementation phases of the programme. These components represent the basics of project management, including quality management and management of risk.

Appendices offers samples and templates including target group description, a series of health check questions for organisations to ask themselves when planning an awareness programme, as well as suggested forms and baseline worksheet for capturing information and documenting the programme.

In addition there is a comprehensive index of terms.

Using the guide

This guide is aimed at people who will be playing a part in an awareness project or those who wish to understand how awareness contributes to the raising of information security; this would include senior management responsible for the overall direction of a project, project managers, and members of the project team. In addition, line managers of project personnel may find it useful to gain an appreciation of their staff's involvement in an awareness project by reviewing an introduction to the overall strategy for managing information security awareness programmes.

This guide has been designed to provide a complete reference to the ENISA awareness methodology. In practice, organisations are expected to tailor this methodology to their own needs. This essentially involves assessing the value of individual activities by taking into context the size and maturity level of the organisation and by adapting the planning accordingly. As a reference work, the entire manual provides essential reading for all project managers. However, the following is offered as a focus for specific groups:

- ✓ Project managers coming to awareness for the first time should:
  - ○ Read and understand *An introduction to* awareness, Part 1 to appreciate the overall approach that this methodology takes to creating and managing an awareness programme.
  - ○ Use the process descriptions in the *Process* section, Part 2 as the basis for planning a project and deciding on resource requirements.
  - ○ Read and understand the *Activities* section to familiarise themselves with the interaction between the activities and the processes; and pay particular attention to activities more specific to awareness programmes, such as *Assess organisation's level of awareness & needs (A-033)*, *Define target groups (A-040), Assess TG's level of awareness & needs (A-043), Determine desired behaviours (A-044)* and *Define communications concept (A-110).*
- ✓ Project managers already familiar with awareness programmes should read and understand the process model described in the *Process* section, Part2 to appreciate the changes of emphasis and process-driven approach.
- ✓ Staff without any prior experience in project management should read and understand the ENISA process modelling, in particular activities such as *Identify personnel and material needed for programme (A-050)*, *Obtaining appropriate management support and funding (A-080), Define indicators to measure success of programme (A120), Document lessons learned (A-140 and B-050),* and *Conduct evaluations (C-010).*
- ✓ Senior managers who will be involved in an awareness programme at project board level should gain appreciation of information security awareness and their roles within a programme by reviewing the *Introduction*, Part 1*;* the business case, as a result of the activity *Make a formal business case (A-084)*; the Organisation, as a result of the activity *Review list of PT members* (B-011).
- ✓ Programme managers with awareness initiatives in their programme should gain a clear understanding of the approach that ENISA suggests to take to create and manage an awareness programme.

Adapting the method to the organisation

Organisations are expected to adapt the methodology described in this document to their own needs. In this sense, this document describes a collection of activities, organised in a structured fashion, that should be considered when designing and executing an awareness raising programme. The activities described however are not necessarily needed, nor the right ones, for all organisations and should not be taken as a recipe to be followed 'as is'.

For example, if the task of running the awareness programme is immediately delegated to a team of people, there is less need for the activities in the subprocesses *Establish initial programme team (A-*

010) and *Identify personnel and material needed for the programme (A-050)*. Similarly, smaller organisations may well be able to make the simplifying assumption of a single homogeneous target group, which greatly reduces the complexity of the subprocess *Define communications concepts* (A-110).

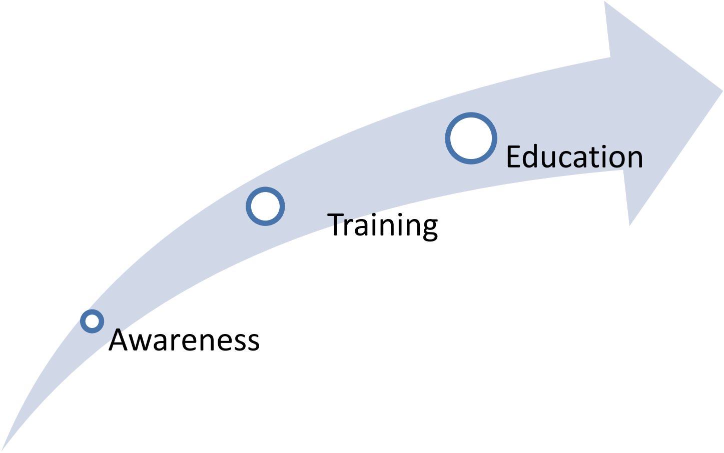
Also, depending on the scale of the programme, available budget and size of the organisation, it should be decided how, and in how much detail, to follow the activities in *Define indicators to measure the success of the programme (A-120)* and *Gather data (C-020)*. For example, a small and medium enterprise (SME) may wish to rely on a small sample of qualitative data – or even informally taking the temperature of the information security awareness level of the organisation by having chats with users, IT-support and managers. A large multi-national organisation may wish to gather quantitative data over time and in a more structure way to measure success of an awareness programme deployed globally and, subsequently, evaluate and plan future activities.

Organisations must find the best way for them to follow the main process: plan, assess and design, execute and manage, evaluate and adjust. This guide provides a detailed methodology and is a good starting point for planning, organising and running successful security awareness initiatives.

Awareness: a definition

Awareness is the 'what' component of the education strategy of an organisation which tries to change the behaviour and patterns in how targeted audience (e.g. employees, general public, etc.) use technology and the Internet and it is a distinct element from training. It consists of a set of activities which turn users into organisations' first line of defence. This is why the awareness activities occur on an ongoing basis, using a variety of delivery methods and are less formal and shorter than training.

Awareness is defined in NIST Special Publication 800-16 as follows: 'Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognise IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance' ([12]).



[12] NIST, *Information technology security training requirements: A role- and performance-based model,* NIST — SP 800-16, USA, 1998, available at http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf (last visited on 21 July 2008).

Training is one of the 'how' components to implement security. A training programme should be designed and developed according to the learning objectives set by the organisation. Thus the training seeks to teach skills which allow a person to perform a specific function, while awareness seeks to focus an individual's attention on an issue or set of issues. The skills acquired during training are built upon the awareness foundation, in particular upon the security basics and literacy material ([13]).

Awareness programmes start with awareness, build eventually to training, and evolve into education. They should be customised for the specific audience they are targeting. Thus it will be very important to define the users who will attend both programmes. Different methods could be used to define the target audience. ENISA developed a simple tool to better identify a target group and capture the related data, as described in the section 'Define target group' ([14]).

When information security programmes are necessary

The possible events and situations which result in organisations —private or public, large or small — engaging in any information security awareness activity are different. They vary mainly from internal to external factors which influence the organisation itself.

Thus, we distinguish between measures which are reactive, launched for example in response to a data loss incident, and initiatives which are planned as part of an overall information security policy or strategy. The following are some of the major events and situations which may require an information security awareness programme.

External factors

- ✓ New laws.
- ✓ New government.
- ✓ National awareness day and/or week.
- ✓ New national, regional or local basic information security programme for citizens.
- ✓ Etc.

Internal factors

- ✓ New laws and regulations relevant for the organisation.
- ✓ New security policy and/or strategy.
- ✓ Updates or changes in information security policies, procedures, standards and guidelines.
- ✓ New technology implementation.
- ✓ New employees, contractors or outsourced personnel working in-house.
- ✓ New management.
- ✓ More automation.
- ✓ Basic information security training for all personnel.

[13] NIST, *Information technology security training requirements: A role- and performance-based model,* NIST — SP 800-16, USA, 1998, available at http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf (last visited on 21 July 2008).

[14] Herold*,* Rebecca, *Information security and privacy awareness program,* Auerbach Publications, USA, 2005; NIST, *Building an information technology security awareness program*, NIST — SP800-50, NIST, 2003, available at http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf (last visited on 17 July 2008).

- ✓ Product portfolio.
- ✓ Launch of new products and services.
- ✓ Launch of new systems.
- ✓ Acquisitions, mergers and divestitures.
- ✓ Recent security breaches, threats and incidents.
- ✓ New risks ([15]).
- ✓ Certification.
- ✓ Etc.

([15]) Social networking represents one of the fastest emerging new areas of risk according to the 2011 Global state of information security survey.

PART 2: MAIN PROCESSES FOR MANAGING AWARENESS PROGRAMMES

Overall strategy for managing information security awareness programmes

ENISA identified three main processes in the development of an information security awareness programme: plan, assess and design, execute and manage, and evaluate and adjust ([16]).

Process	Description
Plan, assess and design	Awareness programmes must be designed with the organisation mission in mind. It is important that they support the business needs of the organisation and be relevant to the organisation's culture and eventually IT architecture. The most successful programmes are those that users feel are relevant to the subject matter and issues presented. In the design step of the programme, the awareness needs are identified, an effective awareness plan is developed, organisational buy-in is sought and secured, and priorities are established.
Execute and manage	This process includes any activity necessary to implement an information security awareness programme. The initiative can be executed and managed only when: ✓ A needs assessment has been conducted. ✓ A strategy has been developed. ✓ An awareness programme plan for implementing that strategy has been completed. ✓ Material has been developed.
Evaluate and adjust	Formal evaluation and feedback mechanisms are critical components of any security awareness programme. Continuous improvement cannot occur without a good sense of how the existing programme is working. In addition, the feedback mechanism must be designed to address objectives initially established for the programme. Once the baseline requirements have been solidified, a feedback strategy can be designed and implemented.

This process modelling 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, activities and tasks. Moreover, it provides a visual representation of the core activities.

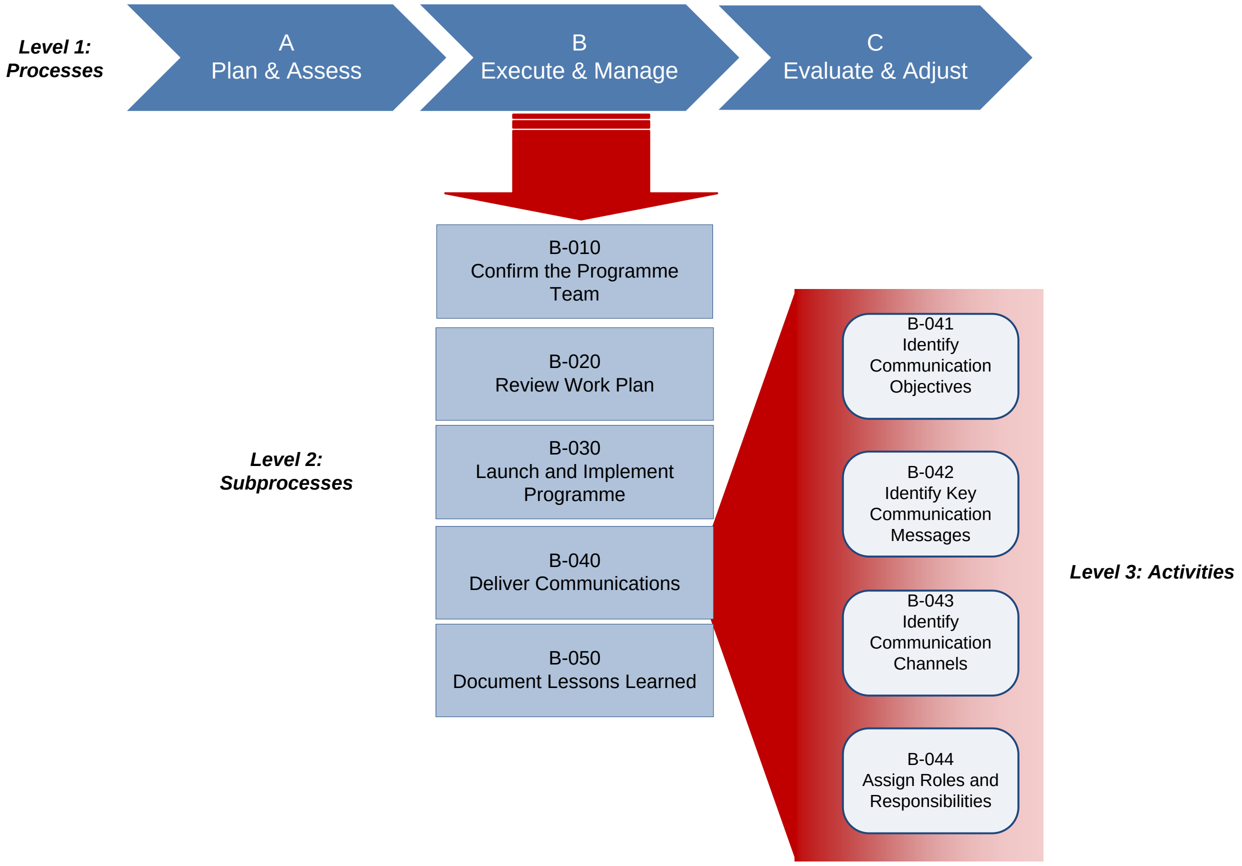
The complete process mapping is included in the Appendices XIII to XV.

Process mapping hierarchy

ENISA uses a model that illustrates processes in three levels of details:

- ✓ Process: a representation of time-related actions and dependencies that transfer a set of inputs into a set of outputs.
- ✓ Subprocess: a segment of a core process covering a single business area.
- ✓ Activity: a breakdown of a subprocess that produces a measurable result.

[16] Wilson, Mark and John Hash, *Building an information technology security awareness program*, NIST, USA, 2003, available at http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf (last visited on 17 July 2008).



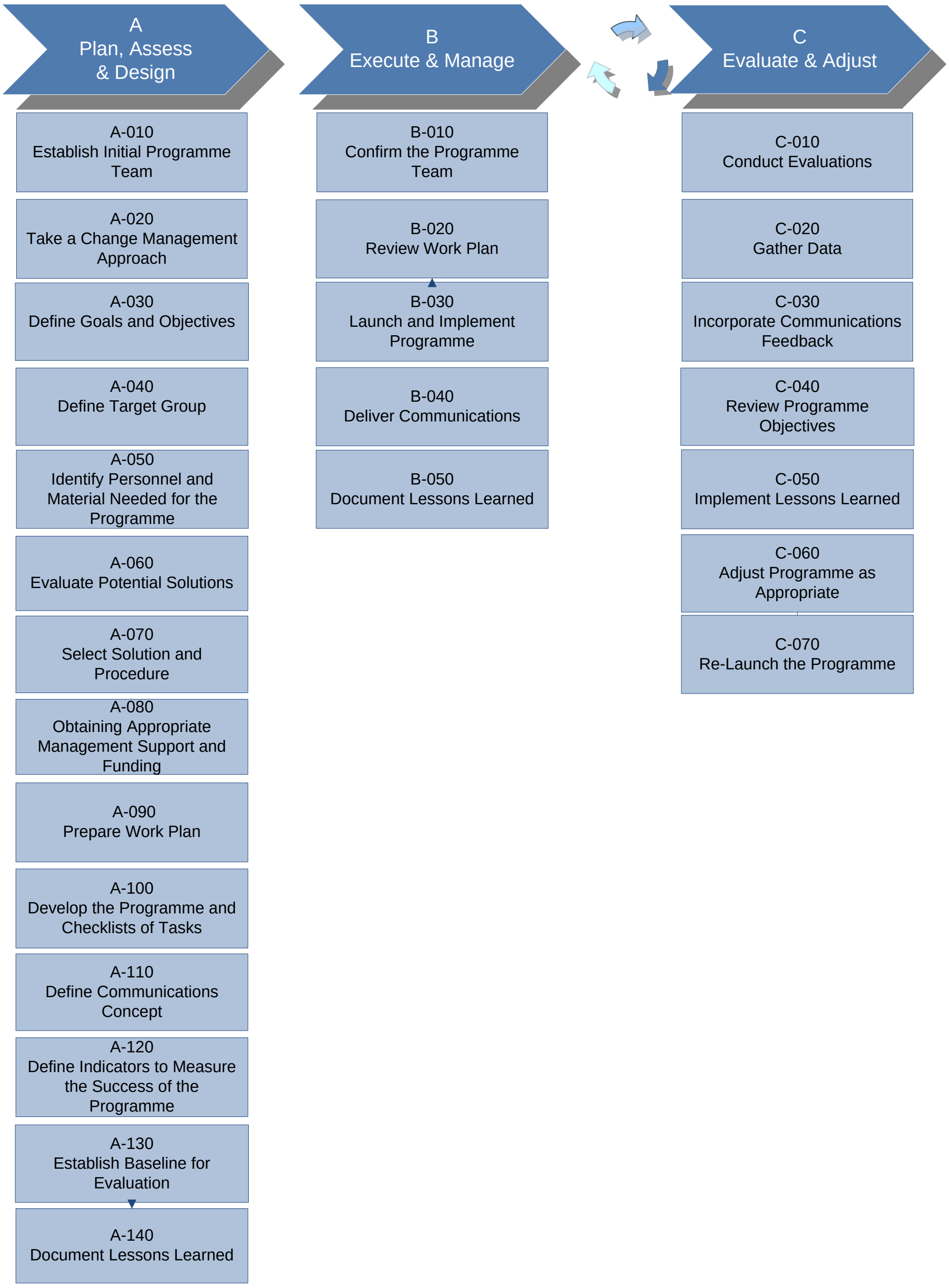
The objects in the diagram have been numbered using the following numbering code to reflect the hierarchy:

		Code
Process name	e.g. Execute & manage	B
Subprocess name	e.g. Deliver communications	B-040
Activity name	e.g. Identify communication objectives	B- 041
	e.g. Identify key communication messages	B-042
	….	…

Main processes and subprocesses for managing information security awareness programmes

The processes appear in a row across the top of the diagram and are blue in colour. Under each process is a vertical column listing the associated subprocesses which are light blue in colour.

The three processes and related subprocesses can be represented as follows:

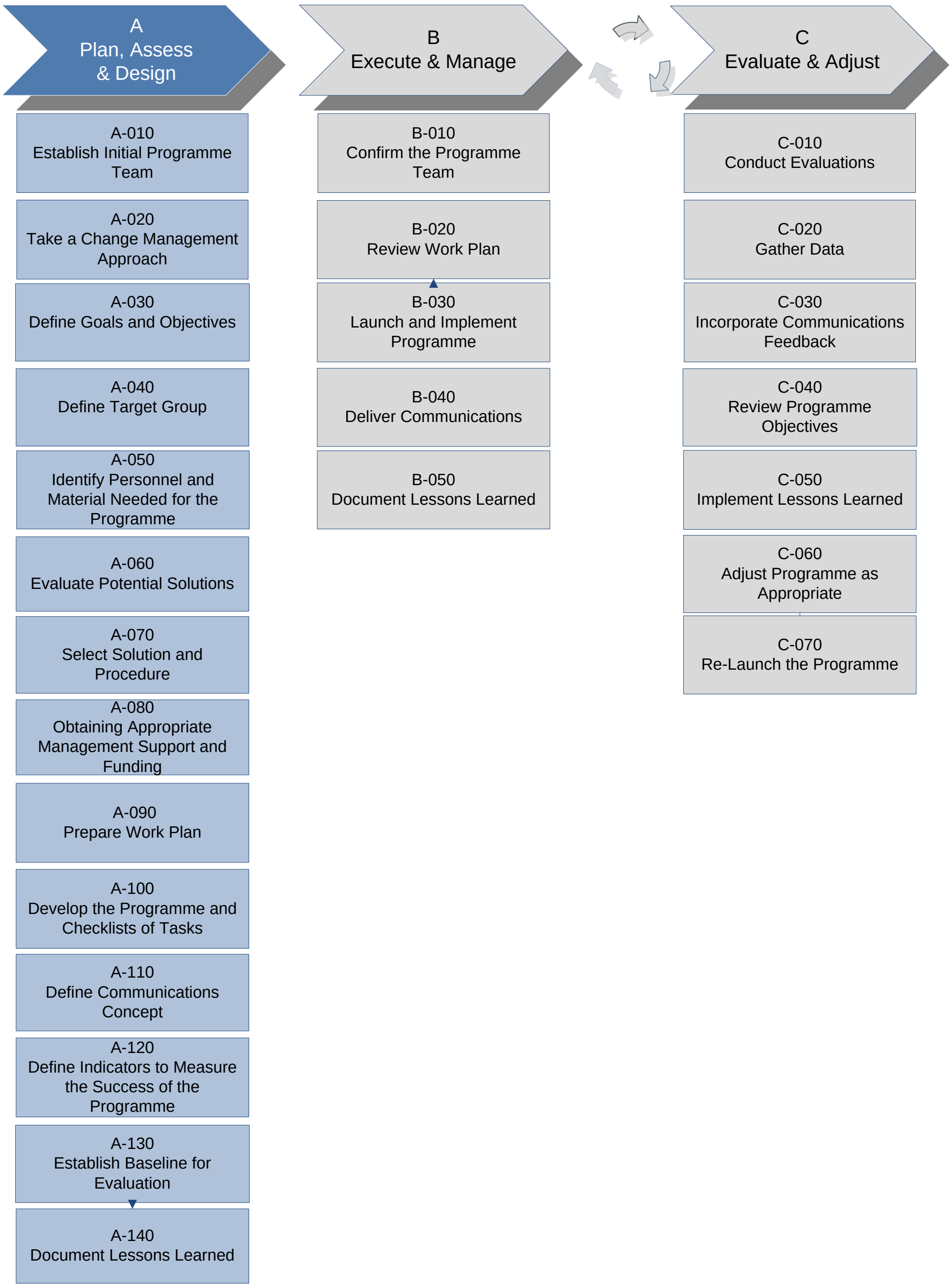


A Plan, Assess & Design	B Execute & Manage	C Evaluate & Adjust
A-010 Establish Initial Programme Team	B-010 Confirm the Programme Team	C-010 Conduct Evaluations
A-020 Take a Change Management Approach	B-020 Review Work Plan	C-020 Gather Data
A-030 Define Goals and Objectives	B-030 Launch and Implement Programme	C-030 Incorporate Communications Feedback
A-040 Define Target Group	B-040 Deliver Communications	C-040 Review Programme Objectives
A-050 Identify Personnel and Material Needed for the Programme	B-050 Document Lessons Learned	C-050 Implement Lessons Learned
A-060 Evaluate Potential Solutions		C-060 Adjust Programme as Appropriate
A-070 Select Solution and Procedure		C-070 Re-Launch the Programme
A-080 Obtaining Appropriate Management Support and Funding		
A-090 Prepare Work Plan		
A-100 Develop the Programme and Checklists of Tasks		
A-110 Define Communications Concept		
A-120 Define Indicators to Measure the Success of the Programme		
A-130 Establish Baseline for Evaluation		
A-140 Document Lessons Learned		

Subprocesses and activities description

Phase I — Plan, assess and design

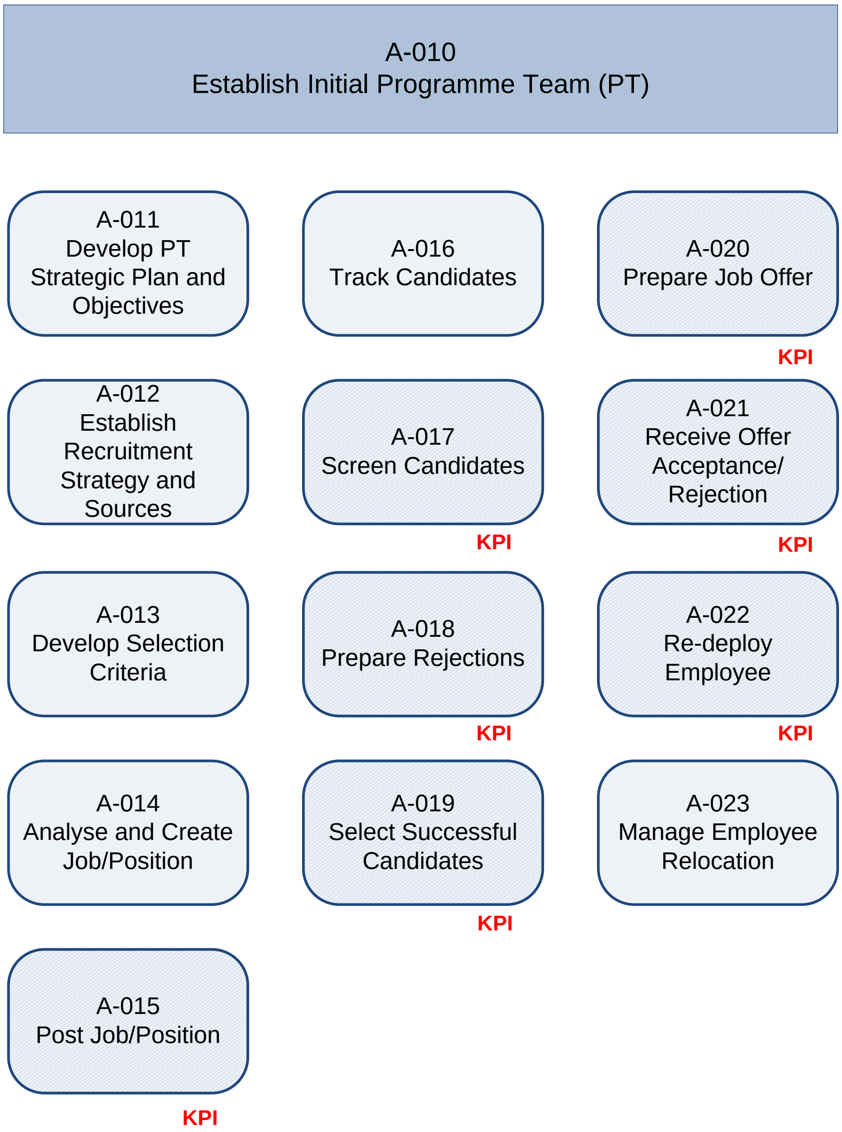
This section describes the steps in the development of a programme in order to identify time-related activities and dependencies.



A Plan, Assess & Design	B Execute & Manage	C Evaluate & Adjust
A-010 Establish Initial Programme Team	B-010 Confirm the Programme Team	C-010 Conduct Evaluations
A-020 Take a Change Management Approach	B-020 Review Work Plan	C-020 Gather Data
A-030 Define Goals and Objectives	B-030 Launch and Implement Programme	C-030 Incorporate Communications Feedback
A-040 Define Target Group	B-040 Deliver Communications	C-040 Review Programme Objectives
A-050 Identify Personnel and Material Needed for the Programme	B-050 Document Lessons Learned	C-050 Implement Lessons Learned
A-060 Evaluate Potential Solutions		C-060 Adjust Programme as Appropriate
A-070 Select Solution and Procedure		C-070 Re-Launch the Programme
A-080 Obtaining Appropriate Management Support and Funding		
A-090 Prepare Work Plan		
A-100 Develop the Programme and Checklists of Tasks		
A-110 Define Communications Concept		
A-120 Define Indicators to Measure the Success of the Programme		
A-130 Establish Baseline for Evaluation		
A-140 Document Lessons Learned		

The light blue subprocesses that are displayed vertically in the process diagram above will be displayed across the top of the diagram at the next level. Under each subprocess is a vertical column(s) listing the associated activities which are grey in colour. Objects that are striped indicate measuring capabilities. The acronym KPI (key performance indicator) is marked below these activities.

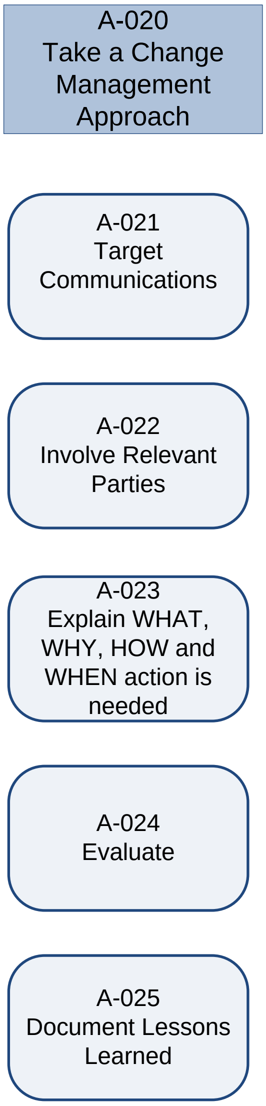
Establish initial programme team (A-010)


A-010
Establish Initial Programme Team (PT)
A-011
Develop PT Strategic Plan and Objectives
A-016
Track Candidates
A-020
Prepare Job Offer
KPI
A-012
Establish Recruitment Strategy and Sources
A-017
Screen Candidates
KPI
A-021
Receive Offer Acceptance/ Rejection
KPI
A-013
Develop Selection Criteria
A-018
Prepare Rejections
KPI
A-022
Re-deploy Employee
KPI
A-014
Analyse and Create Job/Position
A-019
Select Successful Candidates
KPI
A-023
Manage Employee Relocation
A-015
Post Job/Position
KPI

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

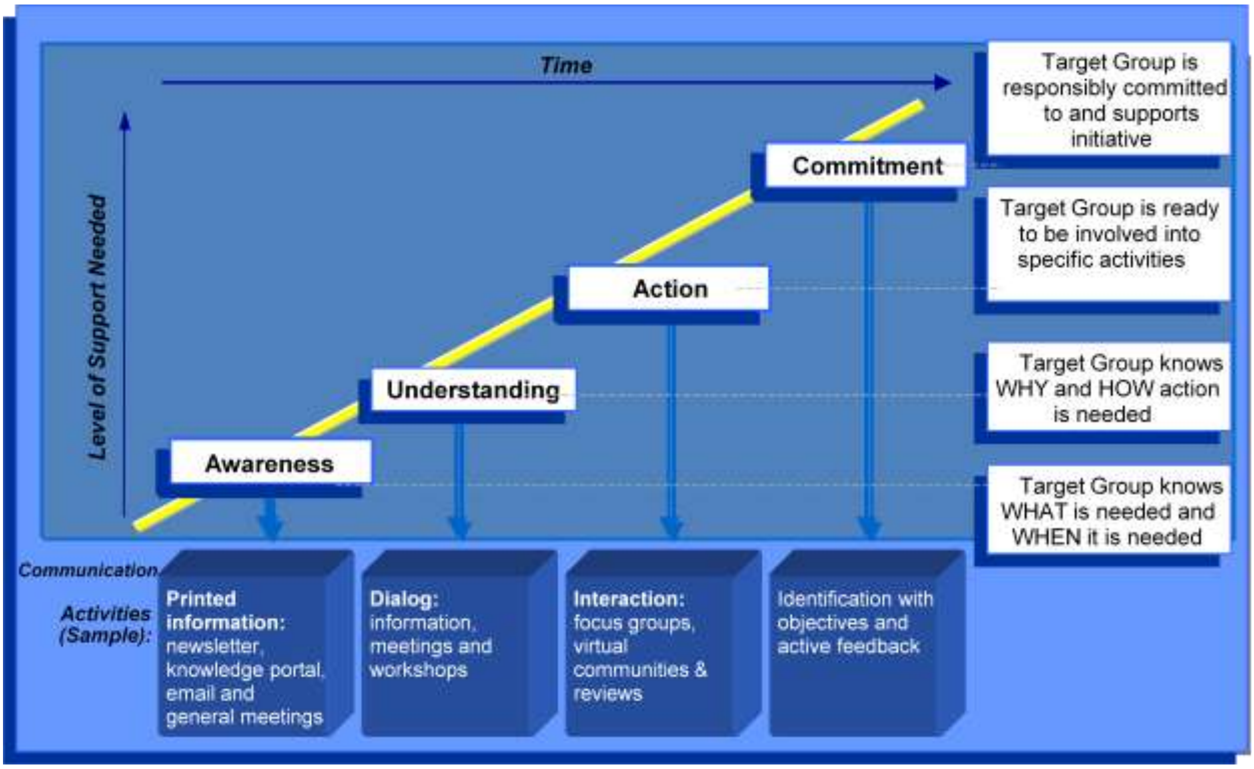
Recent data show that in private organisations the initial programme team is composed of members of the IT department. This can cause problems when other departments, such as risk management, human resources, finance, etc., are not involved at the beginning of the project. This is most likely to happen in multinationals and/or very large enterprises. Ensure to engage with the right people from the beginning.

Take a change management approach (A-020)



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.

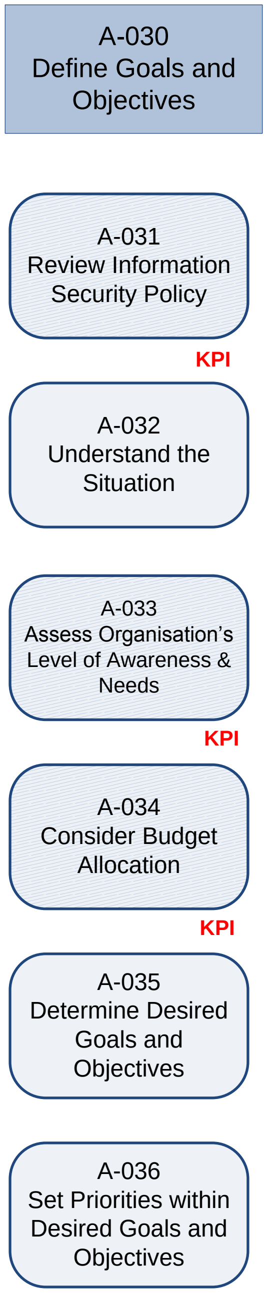
Using the main principles of change management (e.g. targeted communications, involvement, training and evaluation) will help ensure that awareness initiative objectives are met, as well as provide a sound platform for future or follow-up programmes.


Time
Level of Support Needed
Awareness
Understanding
Action
Commitment
Target Group is responsibly committed to and supports initiative
Target Group is ready to be involved into specific activities
Target Group knows WHY and HOW action is needed
Target Group knows WHAT is needed and WHEN it is needed
Communication
Activities (Sample):
Printed information: newsletter, knowledge portal, email and general meetings
Dialog: information, meetings and workshops
Interaction: focus groups, virtual communities & reviews
Identification with objectives and active feedback

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.

Define goals and objectives (A-030)


A-030
Define Goals and Objectives
A-031
Review Information Security Policy
KPI
A-032
Understand the Situation
A-033
Assess Organisation's Level of Awareness & Needs
KPI
A-034
Consider Budget Allocation
KPI
A-035
Determine Desired Goals and Objectives
A-036
Set Priorities within Desired 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 are listed 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?

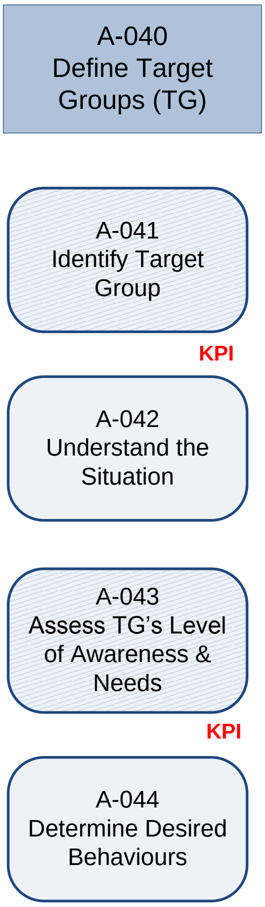
Once you have answers to the questions above, additional points should be considered:

- ✓ 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!

While defining goals and objectives, think and plan for the possibility that insufficient funds will be granted to properly support the programme ([17]). Some possible scenarios described in the section 'Obtain the budget' will give you some pointers and ideas for putting together an information security programme with limited budget, while also taking into consideration all the elements of a good initiative ([18]).

Define target groups (A-040)



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?

[17] Herold, Rebecca, *Information security and privacy awareness program*, Auerbach Publications, USA, 2005.
[18] Herold, Rebecca, *Information security and privacy awareness program*, Auerbach Publications, USA, 2005.

✓ 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 Appendix I.

Examples of groups that can be targeted for information security awareness initiatives and programmes are:

No	Target group	Description
1	Home user	Citizens with varying age and technical knowledge who use ICTs for personal use anywhere outside their work environment. This user group can be further divided into different categories: kids, teenagers, youths, adult and silver surfers.
2	Employee	All organisations' personnel.
3	Mid-level manager	Mangers throughout the organisation responsible for personnel activities and performance. Often not technically oriented, this group needs to be educated and understand the importance of information security. This will allow them to implement the relevant security policies and controls within their business areas.
4	Executive management	Executive managers are the key decision-makers for investment in security.
5	System administrator	Technically inclined personnel, usually responsible for the settings and security of network servers and security systems.
6	Third party	Partners, suppliers, consultants contracted to perform a work in an organisation. Gartner reported that a troubling new California data security breach demonstrates the urgent need for enterprises to require more rigorous security practices from outside contractors ([19]).
7	……	

([19]) Girard, John and Avivah Litan, *New data loss highlights problems with contractors and laws,* Gartner, 4 February 2008.

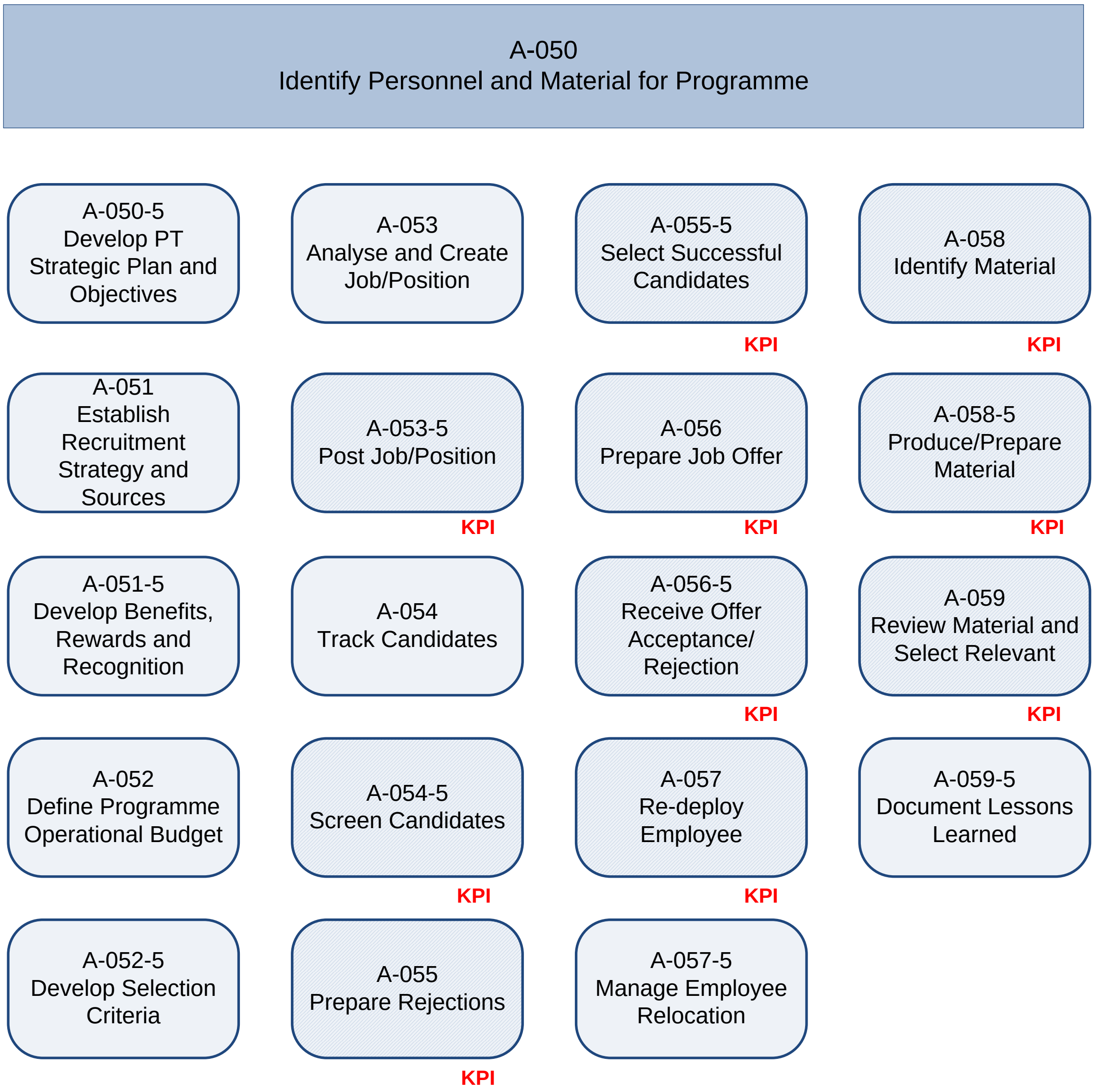
When designing an awareness programme, it is imperative that all the roles are clearly defined. The RACI model ([20]) will be beneficial to do so. The graph below shows a sample of the RACI model with the activities down the left-hand side and across the top the roles responsible for carrying out the initiative or playing a part in it.

	Director	IT Security manager	Human resources	Staff and contractors	....
Activity 1	AR	C	I	I	...
Activity 2	A	R	C	I	...
Activity 3	I	A	I	I	...
Activity *n*	I	A	C	I	...

It is worthwhile to emphasise the need to define the specific audience that is targeted by the awareness initiative in order to tailor the message content to their knowledge or technical aptitude using the most effective communication channels. This will maximise the appeal of the message and persuade the audience to take action, especially if the message fits with the target group's interests and needs. The message should be proactive, topical for the target group and consistent.

[20] RACI is an acronym for responsible, accountable, consulted and informed.

Identify personnel and material needed for the programme (A-050)



A-050
Identify Personnel and Material for Programme

A-050-5
Develop PT Strategic Plan and Objectives

A-051
Establish Recruitment Strategy and Sources

A-051-5
Develop Benefits, Rewards and Recognition

A-052
Define Programme Operational Budget

A-052-5
Develop Selection Criteria

A-053
Analyse and Create Job/Position

A-053-5
Post Job/Position
KPI

A-054
Track Candidates

A-054-5
Screen Candidates
KPI

A-055
Prepare Rejections
KPI

A-055-5
Select Successful Candidates
KPI

A-056
Prepare Job Offer
KPI

A-056-5
Receive Offer Acceptance/ Rejection
KPI

A-057
Re-deploy Employee
KPI

A-057-5
Manage Employee Relocation

A-058
Identify Material
KPI

A-058-5
Produce/Prepare Material
KPI

A-059
Review Material and Select Relevant
KPI

A-059-5
Document Lessons Learned

At this stage in the process, it is time to determine what is needed in terms of personnel and materials. Internally developed programmes rarely have sufficient time and devoted resources as they are considered important but not urgent.

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 information security awareness programme. Organisations should consider implementing a shared governance responsibility across multiple functions to ensure security awareness does not fall through the gaps. This is particularly important when the budget to run such initiatives is not held by the security function ([21]).

Advice and lessons learned from colleagues and/or organisations 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 and material available both free of charge and on a fee basis. There are a number of free forums and communities specifically focused on security awareness. It could be useful to become a member, especially as members are granted access to archives. In this regard, it is important to mention the ENISA AR Community launched in 2008.

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

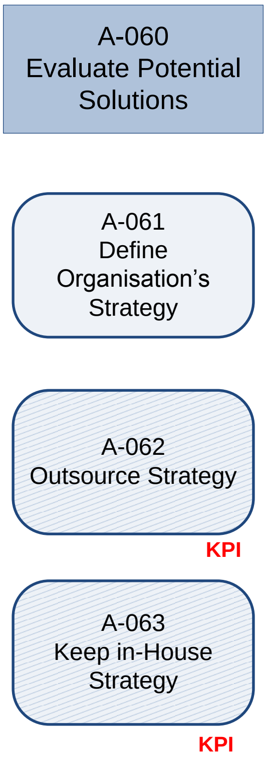
With all the information collected, a thorough review of the list of internal and external resources is in order. Specific focus should be identifying those pieces that might be useful for and suit the needs of the programme. A typical reaction is to discard information that appears unsuitable, but exercise 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 a shortlist of potential solutions that will be evaluated as part of the next step.

Organisations should consider implementing a shared governance responsibility across multiple functions to ensure security awareness does not fall through the gaps. This is particularly important when the budget to run such initiatives is not held by the security function.

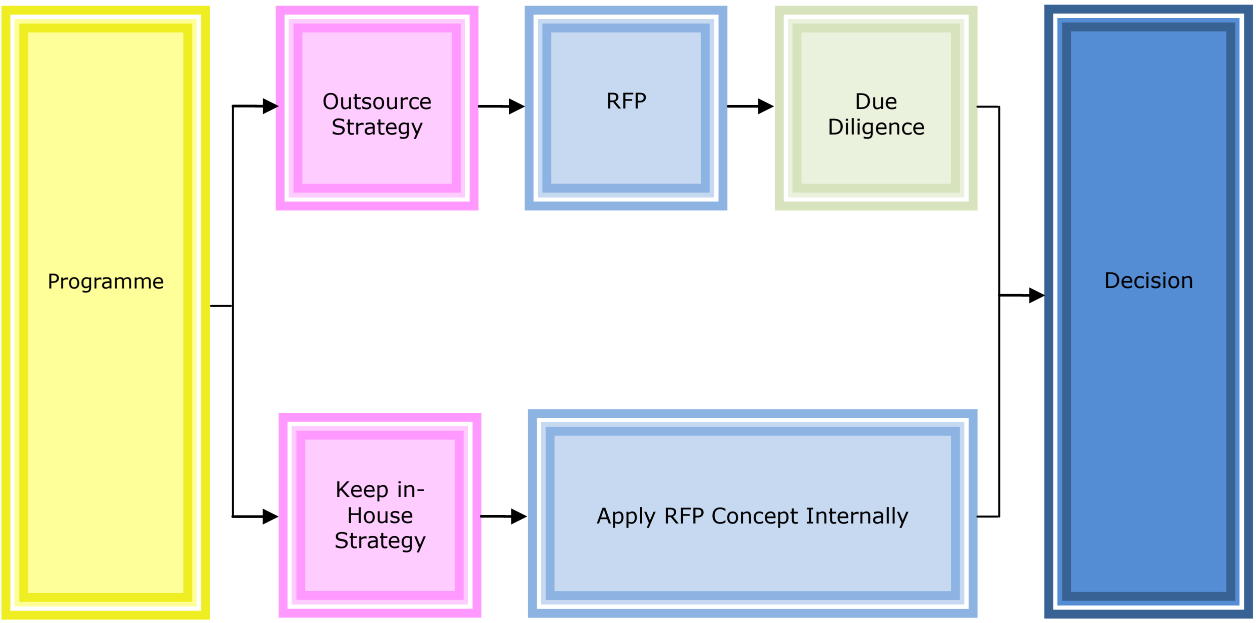
([21]) PricewaterhouseCoopers LLP (UK), *Protecting your business – Security awareness: Turning your people into your first line of defence*, 2010, available at http://www.pwc.co.uk/eng/publications/protecting_your_business_security_awareness.html (last visited on 29 October 2010).

Evaluate potential solutions (A-060)



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

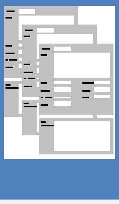
The complete evaluation and assessment process is derived from the traditional tendering sub-process.

1. Prepare a formal request for proposal (RFP) containing precise requirements derived from the first two steps of this process. The composition of the programme team needs to be determined along with desired experience and attributes, roles and responsibilities and reporting structures.
2. Programme procedures and policies need to be determined and formalised. Included in this are approaches for weekly status reporting, financial reporting and issues management.
3. Send RFP to potential bidders indicating the deadline for responses.
4. Compile questions received by bidders and respond in a timely manner to all bidders without disclosing the originator of the questions.
5. When the deadline expires, reject any further proposals but begin systematically evaluating and scoring the offers used on the checklist written earlier.
6. Focus on essential requirements first; this may lead immediately to exclusion of some bidders if they do not meet essential needs.
7. 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.
8. 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 the quality of bidders.
9. 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%.
10. 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.
11. 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.

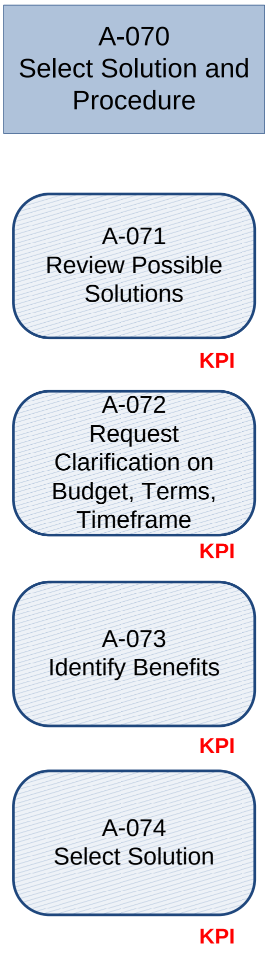
In case the solution will be outsourced, ensure the awareness programme and material is modified and customised according to the organisation's requirements. It is not advisable, for example, to purchase a ready-made training module and material, or copy the awareness programme for a specific topic from another organisation. Information security awareness programmes should be built around the business environment of the organisation ([22]).

The RFP should contain precise requirements. An RFP sample is available in Appendix II. 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 Appendix III.



([22]) Herold, Rebecca, *Information security and privacy awareness program*, Auerbach Publications, USA, 2005.

Select solution and procedure (A-070)


A-070
Select Solution and Procedure
A-071
Review Possible Solutions
KPI
A-072
Request Clarification on Budget, Terms, Timeframe
KPI
A-073
Identify Benefits
KPI
A-074
Select Solution
KPI

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, and to 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.

In this phase, it is important to look at the programme benefits while selecting the solution.
Finally, a decision is made, the purchase order is created and the contract signed.

Identify programme benefits

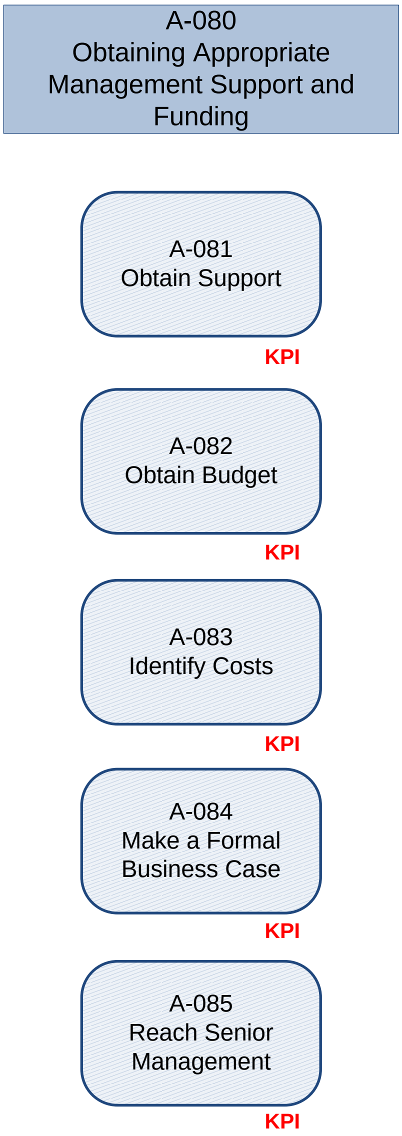
In order to obtain appropriate management support and funding, it is very important to identify the programme benefits.

An information security awareness programme will:

- ✓ 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.

- ✓ Communicate important recommended guidelines or practices required to secure information resources.
- ✓ Provide general and specific information about information security risks and controls to people who need to know.
- ✓ Make individuals aware of their responsibilities in relation to information security.
- ✓ Motivate individuals to adopt recommended guidelines or practices.
- ✓ Create a stronger culture of security, one with a broad understanding and commitment to information security.
- ✓ Help enhance the consistency and effectiveness of existing information security controls and potentially stimulate the adoption of cost-effective controls.
- ✓ 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.

Obtain appropriate senior management support and funding (A-080)



Gaining management support and sponsorship for the awareness programme is perhaps the most crucial aspect of the entire initiative ([23]). It is vital to build consensus amongst decision-makers that the awareness programme is important and worthy of funding.

[23] ENISA*, Obtaining support and funding from senior management*, 2008, available at http://www.enisa.europa.eu/act/ar/deliverables/2008/obtaining-support (last visited on 19 November 2010); Herold, Rebecca, *Information security and privacy awareness program*, Auerbach Publications, USA, 2005; IT Governance Institute, *Information security governance: Guidance for boards of directors and executive management*, second edition, USA, 2006.

This is where the concept of IT governance 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 as it will encounter passive resistance from the personnel. There is a strong correlation between the importance senior management place on information security and how well staff perceives awareness initiatives. It is therefore crucial to communicate the importance of everyone's participation prior to any initiative and programme rollout.

International insurer — Senior management commitment makes a big difference

An insurance company explained why information security is important to their business. They collect, store and process significant amounts of financial, medical and personal information. This information is their number one asset; confidentiality breaches could put their reputation at risk, as well as exposing them to harmful litigation. Unfortunately, the threats (such as identity theft and scams) are rising; this makes staff awareness vital.

The main challenge has been to develop an approach that is suitable for over 10 000 employees speaking many different languages. To counteract this, the company engaged an external provider to help them build suitable training plans and materials. To create the greatest impact with staff, training materials were translated into the local mother tongues of the countries concerned.

There is a continual programme to adjust and promote the key messages. The objectives of this are to try to change people's behaviour and perception of risk. Numerous techniques are used to reach the audience, since different people learn by different mechanisms.

The most effective technique has been face-to-face time with staff through workshops and training sessions. Being able to put a face to a name or function is more personable and people are more receptive to messages being face to face. The training is mandatory. Senior management actively support the awareness schemes, making sure training events are at convenient times for the business and promoting them to staff. There is good attendance at sessions since missing the events results in escalation to the employee's manager. This senior management support across the business has proved to be critical to the success of the awareness programme.

Other non-interactive mechanisms, such as intranet articles, e-mails, posters and publications, are used to reinforce important messages. However, it has proved difficult to gauge how many people have read or understood the messages and people can easily ignore them. So, they are used as a complement to, rather than a substitute for, classroom training.

Telecommunications provider — Engaging with staff

A telecommunications provider's IT systems are vital to servicing its customers. Any problems with information security could quickly damage the company's reputation. Having a security awareness training programme in place is, therefore, an executive level concern.

In this international organisation, the first stage was to get local management to endorse the main messages. Ultimately, it is them engaging with their staff face to face that makes the most difference to behaviour. Getting the support of the right people is essential to the programme's success.

The company has a diverse range of people, with different levels of understanding and training needs. A central team provides baseline mandatory policies and training that provides a uniform and consistent set of messages. This includes e-learning modules and quizzes. Additional information and optional training materials are also available. These enable local entities to tailor group security policy and training to the local environment and their staff's needs. The extra material includes posters, screensavers and quizzes.

A global security portal provides all this information. It has proved to be the most effective way to distribute messages across the whole world. For users, the portal is easy to access and quick. For the central team, it is simple to keep up to date with relevant content.

At a country level, getting staff actively discussing issues face to face has been the best way to improve awareness. Both induction and ongoing training are used to achieve this.

Regular security risk assessments and gap analyses are carried out for each significant operation. These take place before new major initiatives; the results are used to hone the training, target messages, and help to measure the effectiveness.

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. How to build a business case is very important to the success of an awareness initiative.

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.

Government — The importance of having a code of conduct

A government agency explained why codes of conduct are increasingly important and used in public–private partnerships. The government agency wants to ensure that any awareness initiatives is viewed as an act of responsibility for keeping people safe online.

A big challenge is retaining the right balance in the content. The purpose of public–private partnerships is not to promote any product or service but to educate users and change their behaviour. It is important that there is a joint government and industry approach and understanding to promoting Internet safety and security.

Obtain the budget

There are several different approaches organisations take to budgeting activities and managing funding in general. Indeed methods of obtaining the budget for information security awareness initiatives vary greatly from one organisation to another. Some methods include ([24]):

- ✓ Obtaining a percentage of the corporate training budget.
- ✓ Obtaining a percentage of the information technology budget.
- ✓ Obtaining a percentage of each business unit's budget based on number of personnel.
- ✓ Allocation of a set amount per user according to the role and the participation within the education programme.
- ✓ Allocation of a set amount regardless of the awareness goals and objectives.
- ✓ Explicit allocations based on the defined awareness goals and objectives.

Budget is already allocated

If the budget is already allocated it may be necessary to reassess the feasibility of the defined goals and objectives of the awareness initiative. With an insufficient budget, some of the awareness goals and objectives may have to be curtailed. To this end, priority should be given to those goals and objectives which were identified as critical for the programme.

Eventually, it may be considered asking for additional funding.

Prepare the budget

Ideally, with the defined awareness strategy the budget is determined to implement the defined goals and objectives. The last part of this task is to identify the costs related to the initiative. This will be part of the next activity.

([24]) Herold, Rebecca, *Information security and privacy awareness program*, Auerbach Publications, USA, 2005.

Identify costs

To run a successful awareness programme, a formal request for funds has to be submitted to support the initiative. In order to do so, both fixed and variable costs related to an awareness initiative should be identified.

The costs will vary greatly from one organisation to another depending on their structure, availability of supporting assets (such as e-learning systems), previous projects and so forth. The table below provides some of the most common cost elements for information security awareness initiatives, including illustrative cost estimations based on actual figures given from an airline corporation ([25]):

Cost	Description		€ Estimate
Personnel	Personnel working on the information security awareness initiative. Whether they are full or part-time depends largely on the size of the organisation and the importance of information security relative to other priorities.		60 000
Operational Costs	The operational costs include rent, website maintenance – extranet and intranet -, information security awareness materials – posters, briefing papers, office miscellaneous costs.		25 000
Advertisement and Promotion	Branded coasters, pens, prizes for information security tests, quizzes and competitions, coffee for brown-bag meetings and so on.	Promo material cost	2 000
		Promo distribution cost	
		Advertisement creative cost	
		Advertisement media cost	
Training	In the event an organisation organises awareness training sessions.	Individual materials cost	
		Training rooms cost per session	100
Contingency	Further funds may be needed to purchase additional security awareness materials, external training courses and so on.		20% on total
Total budget request			**TOTAL**

The main expenses will be incurred by the information security awareness programme team. If appropriately experienced staff already exist within the organisation, those individuals would need to be seconded to the initiative. Otherwise, expenses need to include a manager's salary, any additional staffing costs for those assigned to the awareness programme team and any other associated costs, as well as the costs associated with the development, production and delivery of awareness materials, external training courses and training classrooms, etc. Typical cost elements can be summarised as follows:

([25]) ENISA, *Obtaining Support and Funding from Senior Management,* 2008, available at http://www.enisa.europa.eu/act/ar/deliverables/2008/obtaining-support (last visited on 19 November 2010); Noticebored, *Business case for an Information Security Awareness Program*, 2008, available at http://www.noticebored.com/NB_generic_business_case_for_infosec_awareness_program.pdf (last visited on 17 July 2008).

- ✓ Full- or part-time information security programme manager and assistants (salaries and benefits plus potential recruitment costs);
- ✓ Awareness materials (subscriptions to best practice experts such as Gartner, IsecT, etc.) if these have not already been acquired;
- ✓ Promotional materials (themed items such as screensavers, pens, posters, mouse pads, quizzes with prizes, etc.);
- ✓ Printing (for all materials not sent electronically).

While considering the costs of an initiative, the possible contribution of third parties should be considered. This is valid when an information security awareness programme is part of a public–private partnership.

When the cost elements have been identified, they need to be put into the proper financial context for the organisation. Remember that if investments in information security are assessed alongside other investment projects, it helps to consider them on an equal footing, implying the use of similar (and ideally the same) methods of financial cost projection.

Even though benefits are not identified at this stage, it is possible to perform a 'total cost of ownership' (TCO) calculation, should this be relevant to the organisation. The only variables to be added are how many training sessions are performed (in this example, twenty training sessions were run at a cost of € 100 each for a period of two years) and how long the awareness initiative is run for. The TCO formula would look like this:

$$\mathrm{TCO} = \frac{\sum_{\mathrm{t=1}}^{\mathrm{t=end\ of\ awareness\ initiative}} \mathrm{one\ time\ costs} + \mathrm{recurring\ costs\ (t)}}{\mathrm{awareness\ initiative\ duration}}$$

In the case of the airline corporation, the results of the TCO formula look like this:

$$TCO = \frac{60000 + 25000 + 2000 + (100 \times 20) + (0{,}2 \times 89000)}{2} = 53400$$

Bank – awareness programme costs

A bank explained that in 2004 they had a year one awareness budget of $200 000 and planned to increase it by 20% per year over a three-year period. Costs were relatively low because they had internal developers write an awareness application to test developers' knowledge. Otherwise, the costs for an awareness application to be used across the organisation would be approximately. $500 000. This is in comparison to an annual information security budget of $10 million.

In 1999-2002, the bank had similar numbers although they spent quite a bit on filming an awareness video and printing high-quality materials. They spent $750,000 on printed materials for an awareness booklet for each employee. They decided to stop printing the materials and made them available electronically.

The figure below provides an example from a European headquartered technology company of financial calculations motivating an information security awareness initiative. The programme is planned to run for eight months, involving approximately 2 000 employees at a national retail company with a little more than 100 stores. After the initial round of training, there will be a follow-up period of reminders and additional training sessions where needed. The follow-up activities are called contingency cost. In total, the awareness programme in this example will be a two-year investment. The expected benefit of the initiative is improved operational efficiencies by lowering the amount of time spent on corrective controls. The company will measure the improvements over a two-year period.

Investment Rationale: *To increase the effectiveness in daily operations by lowering the costs related to time spent on corrective controls, per annum.*	
Projected Costs	
One-time costs	€ 87 000
External cost for training during project	€ 11 000
Cost of employee time for training	€ 20 328
Initial cost (sum of cost elements above)	€ 118 328
Project duration (months)	8 months
Recurring costs after project (contingency), per annum	€ 35 498
Projected Benefits	
Current average total cost for corrective controls, per annum	€458 784
Expected improvement	22%
Cost-reduction in corrective controls, per annum	€ 101 887
Improvement period (months)	24 months
Company prerequisites	
Time to measure costs and benefits	24 months
Company's rate of return	10%

In this information security awareness initiative, the value of employee-time was calculated. A prerequisite for all the calculations to be relevant is that the time being freed up due to the awareness initiative really is put into useful work. If things are seen from a different perspective, it will appear that you have only added cost without gaining any operational efficiency.

Make a formal business case

While security expenditure has increased over the last years, the techniques used to justify it have barely changed. The UK Department of Business, Enterprise and Regulatory Reform (BERR) reports that 48% of large businesses always make a formal business case for security expenditure and 41% of large businesses sometimes make a formal business case. Organisations that always prepare a formal business case are most likely to quantify the benefits (32%) and very few (16%) evaluate the return on investment, possibly because their greatest asset is their reputation, which is very hard to quantify [26]. The figures shown in the 2011 Global state of information security survey confirm this tendency; 14% (10% in 2009) of the respondents have a brand or reputation compromised [27].

The discipline of making a formal business case does pay off as the proportion of the IT budget spent on security expenditure is estimated to be 9–10% on average [28].

Building a persuasive business case for senior management by showing the quantitative and qualitative benefits of awareness programmes also forms the basis of a successful awareness initiative. Business cases significantly improve the odds of project success because they help management understand the value of the investment and decide whether to fund it. Furthermore, they generate stakeholder commitment (not just support) because they are credible and guide the work to ensure that expected benefits are realised.

Business cases are also known as cost-benefit analysis, ROI study, feasibility study, project proposal, capital expenditure request, case for action and project funding request.

Information security awareness initiatives require a well-structured approach to business case development that will guide the project from initial feasibility through design and implementation to successful results. A well-structured and consistent approach to formatting business cases sets the stage for sound portfolio management, from initial project evaluation to successful implementation [29]. They differ depending on the size of the investment and governance bodies involved in the decision-making process. However, the investment appraisal process usually follows a similar pattern.

The table below provides a comprehensive model for building a business case, documenting the benefits, costs and rationale of the awareness initiative [30] in the hope that it will build brilliant business cases by avoiding common shortfalls and focusing on results.

Steps	Description
Use a business-driven and inclusive process	✓ Involve all stakeholders to ensure approval and ongoing support. The success of an organisation's awareness initiative depends on the ability of stakeholders to work toward a common goal. ✓ Focus on how the business will achieve changes related to both processes and people. ✓ Identify all potential benefits and who will achieve them.
Set the stage	✓ What is the opportunity or challenge to be discussed? ✓ What is the business context? ✓ What are the effected practices, products or services?
	✓ Provide a description of the business problem or opportunity.

[26] BERR, *2008 Information security breaches survey*, 2008, available at http://www.security-survey.gov.uk (last visited on 25 November 2010).
[27] PricewaterhouseCoopers LLP, *2011 Global state of information security survey*, 2010, available at http://www.pwc.com/gx/en/information-security-survey/index.jhtml (last visited on 29 October 2010).
[28] BERR, *2008 Information security breaches survey*, 2008, available at http://www.security-survey.gov.uk (last visited on 25 November 2010).
[29] Roberts*,* John P., *Toolkit sample template: An effective business case,* Gartner, 11 July 2007; McMurchy, Neil, *Toolkit: Building the business intelligence business case — Identifying and calculating benefits,* Gartner, 25 April 2008; McMurchy*,* Neil, *Take these steps to develop successful bi business cases,* Gartner, 1 February 2008.
[30] Heidt*,* Erik T., *Basics of the quick business case: How to champion your next information security initiative,* RSA Conference Europe 2007, 2007, available at http://artofinfosec.com/22/art-of-info-sec-001-quick-business-case/ (last visited on 22 July 2008).

Document your understanding	✓ Demonstrate that you understand the practices, products or services that will participate in or be impacted by your initiative. ✓ Ask questions about and discuss the history. ✓ Validate and deepen your own understanding. ✓ Seek feedback, listen and confirm.
Fully document the case study	✓ Identify the opportunity and benefits of the awareness programme. ✓ List as well any weakness, vulnerability or threat the initiative could seek to address. ✓ Describe the related risks and how they will be mitigated. ✓ Package the business case well, boosting its credibility.
Identify the business benefits	✓ Identify the value of the proposal to the organisation. ✓ In the balance between technical details and business impacts, emphasise the value to the business and stakeholders. ✓ Be honest and clear about real costs and impacts. ✓ Discuss risks associated with not taking this action, and alternatives. ✓ Do not over-commit!
Present the initiative	✓ Link the business case to business plans and context. ✓ Only discuss the essentials of what it is and how it works. ✓ Put details in addendums and appendices, not in your main presentation.

The business case could be used as well to guide and assess the project execution and the realisation of benefits.

Identify business benefits

An overview of the business benefits linked to an information security initiative will help and lead the organisation to reach an informed decision. The following benefits have been identified.

- ✓ Comply with confidentiality, availability, integrity, privacy and security standards.
- ✓ Defend the organisation from information leakage.
- ✓ Enforce mandatory organisation-wide security policies.
- ✓ Provide both a focal point and a driving force for a range of awareness, training and educational activities relating to information security, a few of which are already in place but are not well coordinated or particularly effective.
- ✓ Communicate and clarify the organisation's overall strategic intent to secure its information resources, both to its employees and externally (information security awareness is an essential requirement for ISO/IEC 27001 certification for example, and is increasingly required for legal and regulatory compliance).
- ✓ Provide general and specific information about security risks and controls to those who need to know it.
- ✓ Make staff, managers and IT professionals aware of their respective responsibilities in relation to information security.
- ✓ Motivate employees to comply with the organisation's information security policies, procedures, standards and guidelines, and with applicable laws, thereby increasing compliance in practice.
- ✓ Create a strong security culture, that is to say a broad understanding of, and demonstrable commitment to, information security right across the organisation.
- ✓ Help improve the utility, consistency and effectiveness of existing information security controls, and where appropriate stimulate the adoption of additional cost-effective controls (and possibly lead to the relaxation of excessive or unnecessary controls).
- ✓ Help reduce the number and extent of information security breaches, reducing costs both

directly (for example information damaged by viruses; sensitive information disclosed; compliance failures leading to fines etc.) and indirectly (such as less need to investigate and resolve breaches).

- ✓ Compliance with increasing numbers of laws and regulations that require some form of training and awareness activities.
- ✓ To gain and keep customer and employee trust and satisfaction.
- ✓ To support compliance with the organisation's documented information security policies.
- ✓ To demonstrate due diligence that management is following a standard of due care to ensure adequate protection of corporate assets.
- ✓ To preserve corporate reputation, this is a valuable business asset.
- ✓ To establish accountability for employee activities.

Benefits that are identified but cannot be measured with quantitative values may mean less to senior management. Therefore, when analysing awareness initiatives that improve the internal controls of the organisation, the principles for effective governance defined by the Massachusetts Institute of Technology's Sloan School of Management can be applied. The expected effectiveness of the information security investment can then be assessed by how well it meets four objectives weighted by their importance to the organisation ([31]).

The approach is based on asking the senior management team – the Institute recommends at least ten managers – to answer questions by giving them a score between 1 and 5 as mentioned in the table below. Then take an average of the results and look at variation by business units and level of management to meet the stakeholder composition for the investment decision.

Importance of information security investment

How important are the following outcomes of your information security governance, on a scale from 1 (not important) to 5 (very important)

	Importance	Outcome
		Cost-effective use of information security
		Effective use of information security for growth
		Effective use of information security for asset utilisation
		Effective use of information security for business flexibility

Importance of information security investment

What is the anticipated influence of the proposed information security investment in your business on the following measures of success, on a scale from 1 (not successful) to 5 (very successful)

	Importance	Outcome
		Cost-effective use of information security
		Effective use of information security for growth
		Effective use of information security for asset utilisation
		Effective use of information security for business flexibility

The first question assesses the importance of a particular outcome related to information security governance and the second question assesses how well the proposed information security awareness investment contributes to meeting that outcome.

Since not all organisations rank the outcomes with the same importance, the answers to the first question are used to weight the answers to the second question. Then the weighted scores for the

[31] Weill, Peter and Jeanne W. Ross, *Governance Arrangements Matrices By Industry,* Harvard Business School Press, Boston (MA), 2004 (II).

four questions are added and divided by the maximum score attainable by that organisation. Therefore, mathematically, information security governance performance =

$$Governance\ effectiveness = \frac{(\sum_{n\,1\,to\,4} \text{(importance of information security governance outcome}\{Q1\} \times \text{influence of proposed awareness investment}\{Q2\})) \times 100}{\sum_{n=1\,to\,4} (5 \times \text{(importance of information security governance outcome))}}$$

Given that there are four objectives, the maximum score for the investment is 100 and the minimum score is 20.

The table below provides an example from a consumer products' manufacturing company of how to present the relevance of a proposed information security awareness programme from a governance effectiveness perspective. It is suggested that the programme run for three months, involving approximately 100 employees working in the financial controlling functions throughout the business units of an organisation in the airline industry. The purpose of the training will be to strengthen the commitment to manual internal controls within the financial reporting processes. The Chief Financial Officer (CFO) and six other senior managers were interviewed on how this awareness initiative could fit with the corporate agenda.

Importance of information security investment	
How important are the following outcomes of your information security governance, on a scale from 1 (not important) to 5 (very important)	
Importance	**Outcome**
4.2	Cost-effective use of information security
2.2	Effective use of information security for growth
4.6	Effective use of information security for asset utilisation
3.2	Effective use of information security for business flexibility
Importance of information security investment	
What is the anticipated influence of the proposed information security investment in your business on the following measures of success, on a scale from 1 (not successful) to 5 (very successful)	
Importance	**Outcome**
4.0	Cost-effective use of information security
1.1	Effective use of information security for growth
3.5	Effective use of information security for asset utilisation
3.0	Effective use of information security for business flexibility

$$Governance\ effectiveness = \frac{(4{,}2 \times 4 + 2{,}2 \times 1{,}1 + 4{,}6 \times 3{,}5 + 3{,}2 \times 3{,}0) \times 100}{5 \times (4{,}2 + 2{,}2 + 4{,}6 + 3{,}2)} = 63$$

To provide value to management, the result of the governance effectiveness assessment needs to be compared in relation with other competing investment requests, or against a baseline where no initiatives with anticipated governance effectiveness below a specified amount such as 50 are accepted.

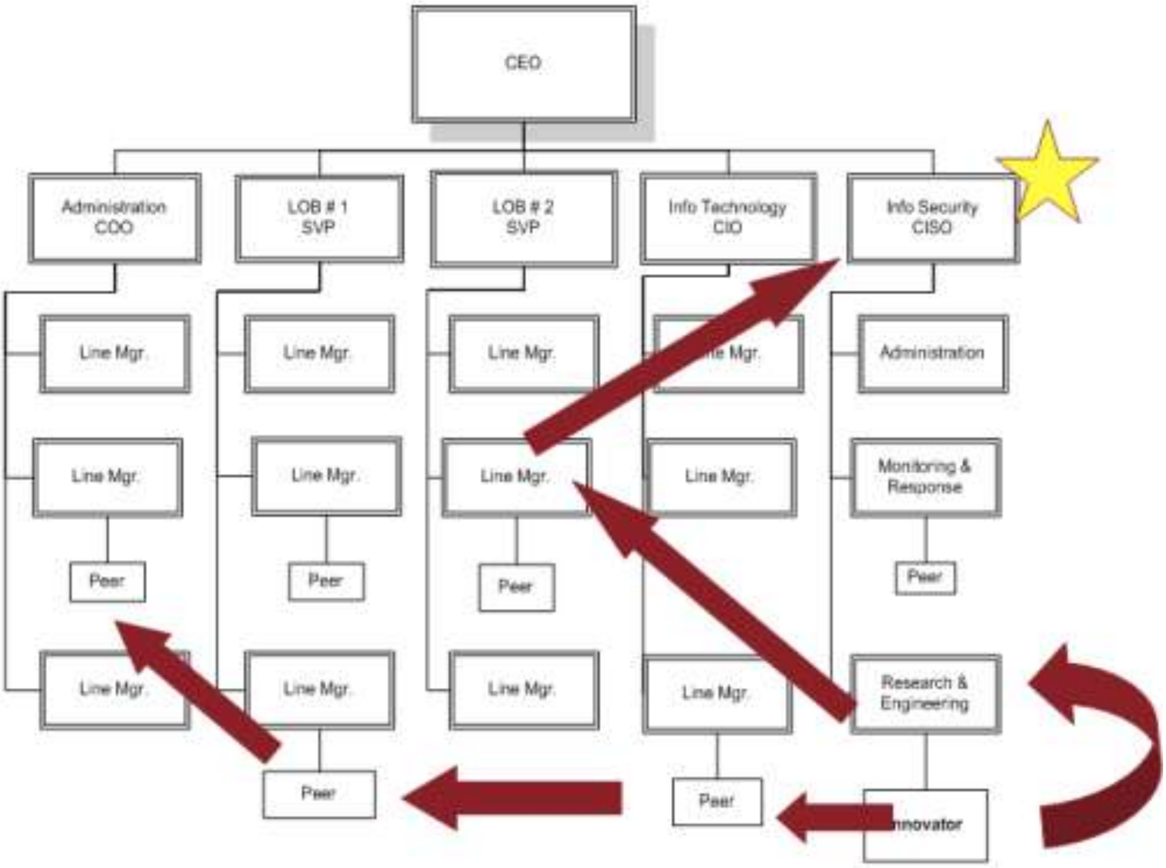
Validate investment rationale

Before presenting the investment request to the senior management, it is very important to ensure an understanding of how the proposed investment will fit with the decision-makers' key strategies and goals. Questions to help validate the investment rationale include:

- ✓ What process changes or enhancements that are strategically important are included in the proposed investment?
- ✓ What are the distributions in the current and proposed project portfolios? Will the acceptance of this investment keep the portfolios consistent with the organisation's strategic objectives?
- ✓ What is the relative importance of enterprise-wide versus business unit investments? Does the proposed investment reflect their relative importance?

Reach senior management

A typical path to reach corporate executives is illustrated below [32].

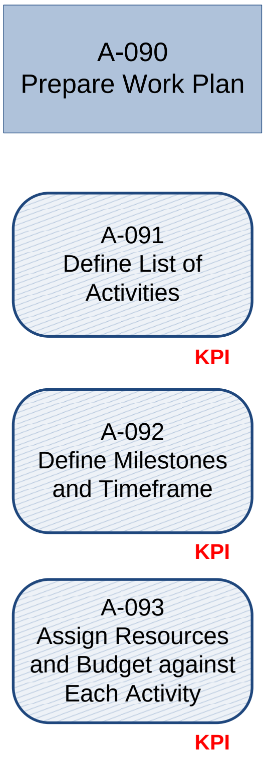


[32] Heidt, Erik T., *Basics of the quick business case: How to champion your next information security initiative*, RSA Conference Europe 2007, 2007, available at http://artofinfosec.com/22/art-of-info-sec-001-quick-business-case/ (last visited on 22 July 2008).

Below are some key recommendations for ensuring the support and funding of senior management.

#	Recommendations	Details
1	Raising information security awareness is not a one time effort	As there is continual change, it is hugely important to ensure an on-going programme to raise awareness in employees on the value of proper information security management.
2	Analyse your target group	It is important to analyse the needs, interests, information security knowledge of the target group of the initiative and prepare an investment rationale accordingly.
3	Prepare a business case	A business case is a decision support and planning tool that could be used to obtain funding from senior management. Financial analysis is generally central for a good business case, and will help awareness investments competing for limited funds. Ensure the team preparing the business case has the skills and experience needed to cover both information security and business knowledge.
4	Plan how to measure success	Non-financial measures that can be used include: ✓ Impact on a core information security metric. ✓ Impact on a knowledge benchmark. ✓ Less employee-time spent on corrective controls. ✓ Incident avoidance benefits. ✓ Incident cost-reductions. Financial measures should be related to standard calculations, for example Return On Investment (ROI), Net Present Value (NPV), Investment Rate of Return (IRR) or Discounted Cash Flow (DCF).
5	Plan and implement the awareness initiative appropriately	Use plans and phases to help make the tasks and activities more manageable. Also create a communication plan. The whole awareness initiative should be an on-going and not a static process.
6	Keep senior management interested in the initiative	Offering regular updates on topical subjects or directly contacting senior management can be an effective method of keeping the senior management involved and supportive.
7	Ensure to have senior management support during the entire lifecycle of the initiative	Involve senior management during all phases of the initiative and always ensure you their support. Otherwise the initiative will not go forward as it will encounter passive resistance from employees.
8	Show results	Follow up on the metrics you have chosen and communicate these regularly.
9	Share success	Celebrate success and use the intranet and management meetings to ensure that a successful initiative is noticed.

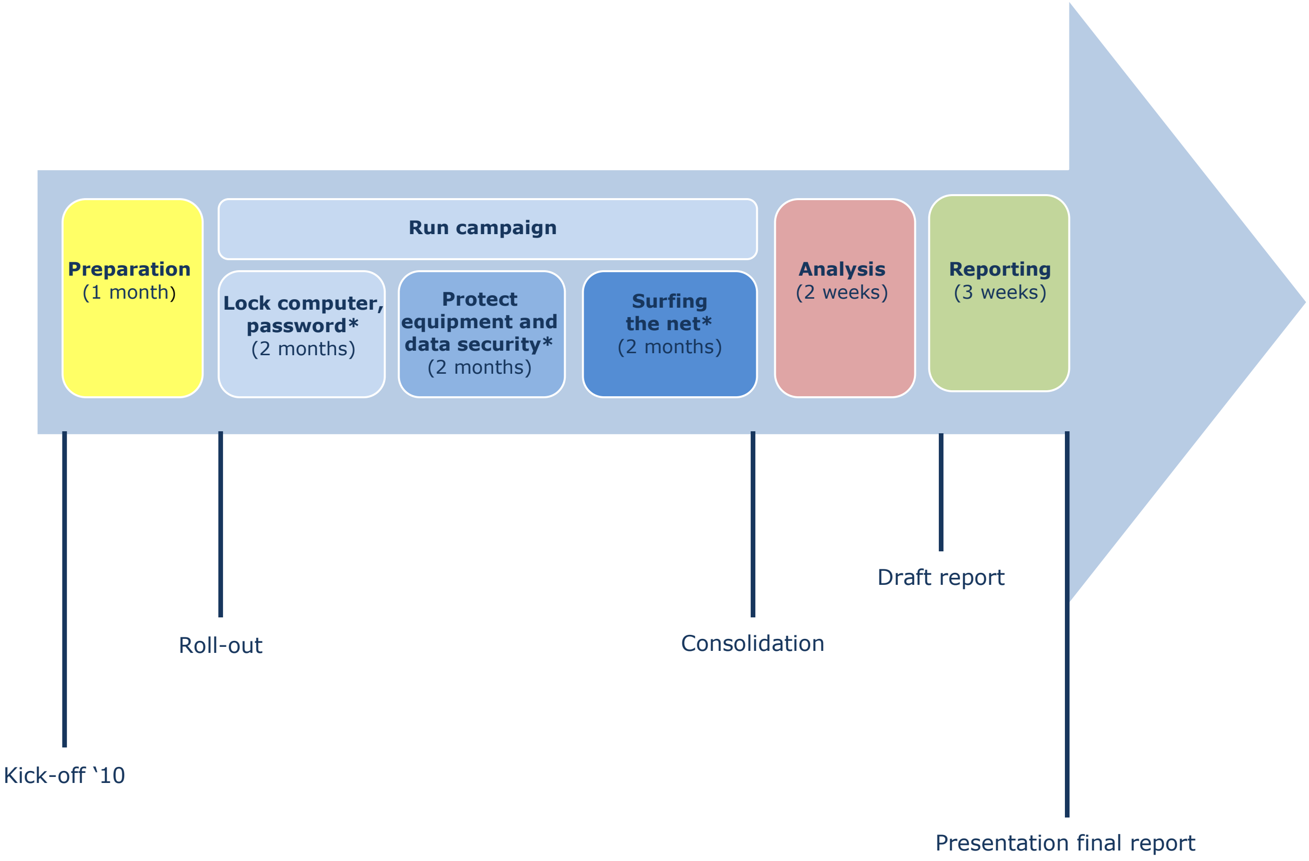
Prepare work plan (A-090)


A-090
Prepare Work Plan
A-091
Define List of Activities
KPI
A-092
Define Milestones and Timeframe
KPI
A-093
Assign Resources and Budget against Each Activity
KPI

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, timelines and milestones will be identified. The work plan will be reviewed as soon as the detailed programme is developed.

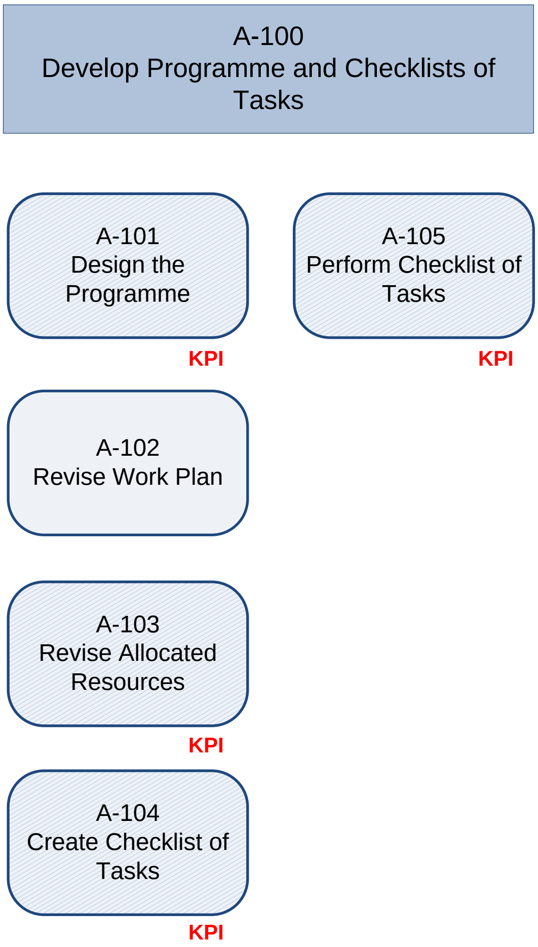
It is important to prepare a work plan identifying activities, resources, timescales, and, eventually, relevant milestones. The use of a tool is recommended to effectively manage the work. A work plan sample is available in Appendix IV.

The graph below shows a sample of programme's timelines:



*Samples of security topics for which awareness could be raised. Regardless of the channel of communication used (e.g. security posters, stickers, etc.), the topic of the awareness campaign should be the same for a given period of time (i.e. minimum 2 months).

Develop the programme and checklists of tasks (A-100)


A-100
Develop Programme and Checklists of Tasks
A-101
Design the Programme
KPI
A-105
Perform Checklist of Tasks
KPI
A-102
Revise Work Plan
A-103
Revise Allocated Resources
KPI
A-104
Create Checklist of Tasks
KPI

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, revising the allocated resources, and finally managing it effectively to ensure that the projected benefits are realised.

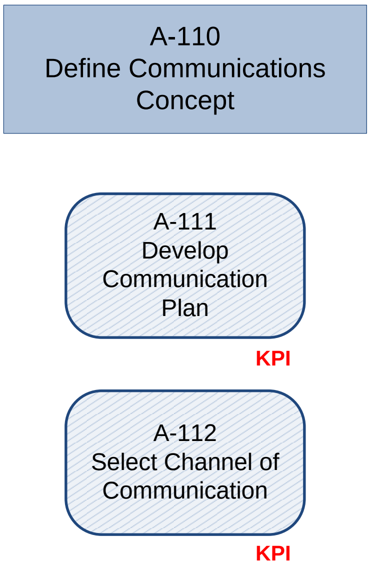
If the list of information security topics is long, it is recommended to plan the programme in separate sections spread out over a period of time. This will allow the effort to focus on specific topics in a way that makes sense to each target audience, without overloading or adding confusion. For example, 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.

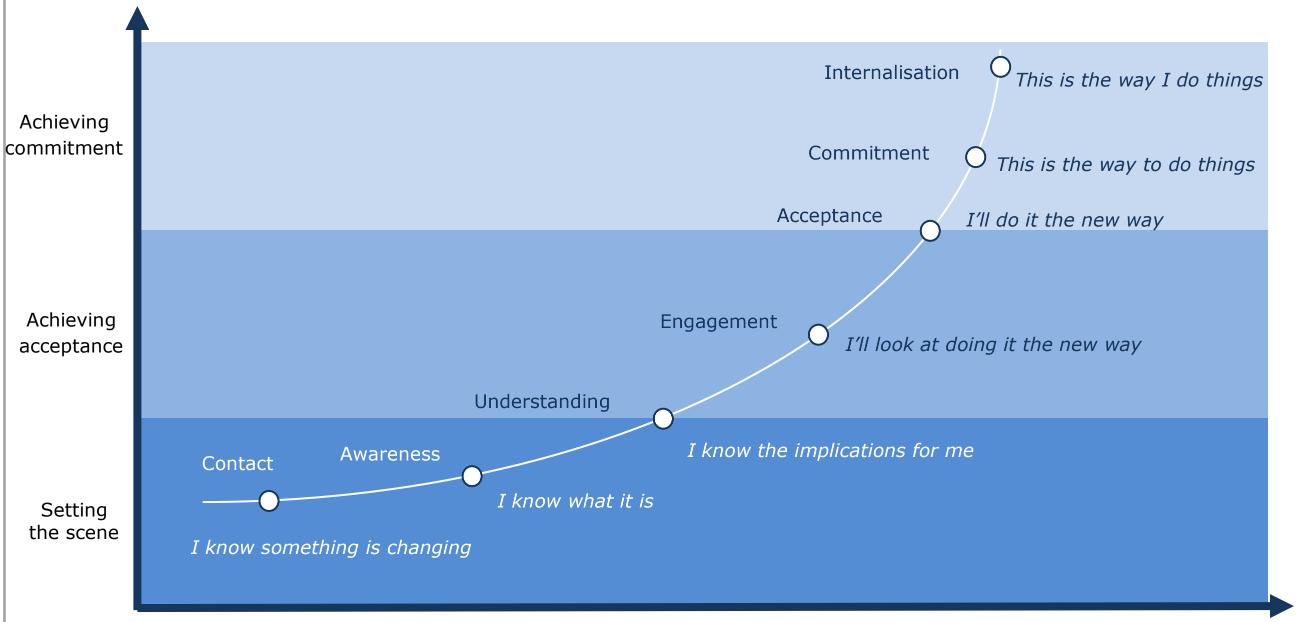
After a full list of topics to be covered during the programme is developed, it is important to evaluate each one and rank them in order of importance. A simple method of evaluating topics is to assign a weight to each one, for example with 3 = crucial, 2 = important and finally 1 = nice to have. This 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.

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. The topic of the awareness campaign should be the same for a given period of time (i.e. minimum 2 months).

Define a communications concept (A-110)


A-110
Define Communications Concept
A-111
Develop Communication Plan
KPI
A-112
Select Channel of Communication
KPI

Communications is crucial for the success of any awareness programme. Effective communication planning is critical to a programme's success. The communication and commitment curve below illustrates the important role of communication in an awareness initiative to achieve its goals.



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.

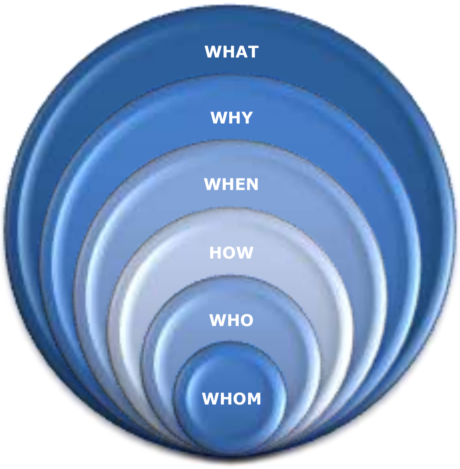
Effective communication

Following the analysis of many information security initiatives executed in different countries, some key points are apparent for any organisation that embarks on an information security related awareness raising initiative.

Below are some key recommendations for an effective campaign.

The basics

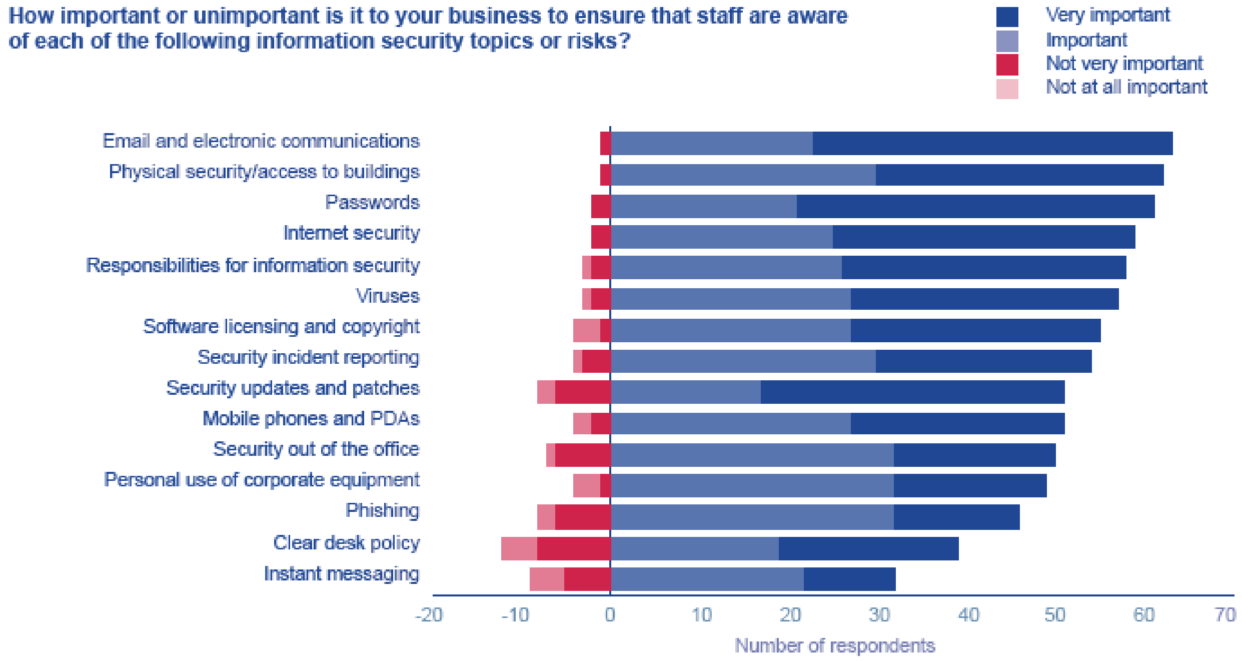
- ✓ Reach out to as broad an audience as possible. It is advantageous to look at the multiplier criteria to maximise the reach of the message.
- ✓ Do not be alarmist or overly negative about a situation. If issues or risks need to be detailed, then it is often easier for the audience to understand in 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.
- ✓ Ensure the initiative is flexible and adaptable as external factors can often change the landscape.
- ✓ Ensure basic communications include [33]:
  - o WHAT is expected of the audience receiving the communication.
  - o WHY target audience should participate in the awareness programme and what are the benefits.
  - o WHEN the recipient should perform the requested actions.
  - o HOW the actions relate to the target audience's work responsibilities and performance and/or life.
  - o WHO sponsor the programme.
  - o WHOM to contact for further information.



The topic

Identifying the topics related to information security that are critical for the organisation and the target audience is the first step of many while organising an awareness initiative. A recent report of ENISA showed that e-mail and electronic communication, passwords, security updates and patches are very important to businesses. They are followed amongst others by security incident reporting, personal use of corporate equipment, and security out of the office [34]. The graph below provides a more complete illustration of the data available within the report.

[33] Herold, Rebecca, *Information security and privacy awareness program*, Auerbach Publications, USA, 2005.
[34] ENISA, *Information security awareness initiatives: Current practice and the measurement of success*, 2007, available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf (last visited on 19 November 2010).



The following is a list of relevant information security awareness topics which should not be considered as exhaustive but as a starting point to identifying the topic for your awareness programme:

- ✓ Information security policies and procedures.
- ✓ Workstation security.
- ✓ Website policies.
- ✓ e-mail security.
- ✓ Social engineering.
- ✓ Third-party and partner security.
- ✓ Identity verification.
- ✓ Technical security mechanisms.
- ✓ Information classification and controls.
- ✓ Incident response.
- ✓ Asset management (e.g. USB flash drives, printing devices, PDA, mobile phones);
- ✓ Etc.

Once the topics are identified, it is recommended to map each target audience to the corresponding topics. From this simple mapping it will be possible to determine the course content that should be given to the appropriate roles.

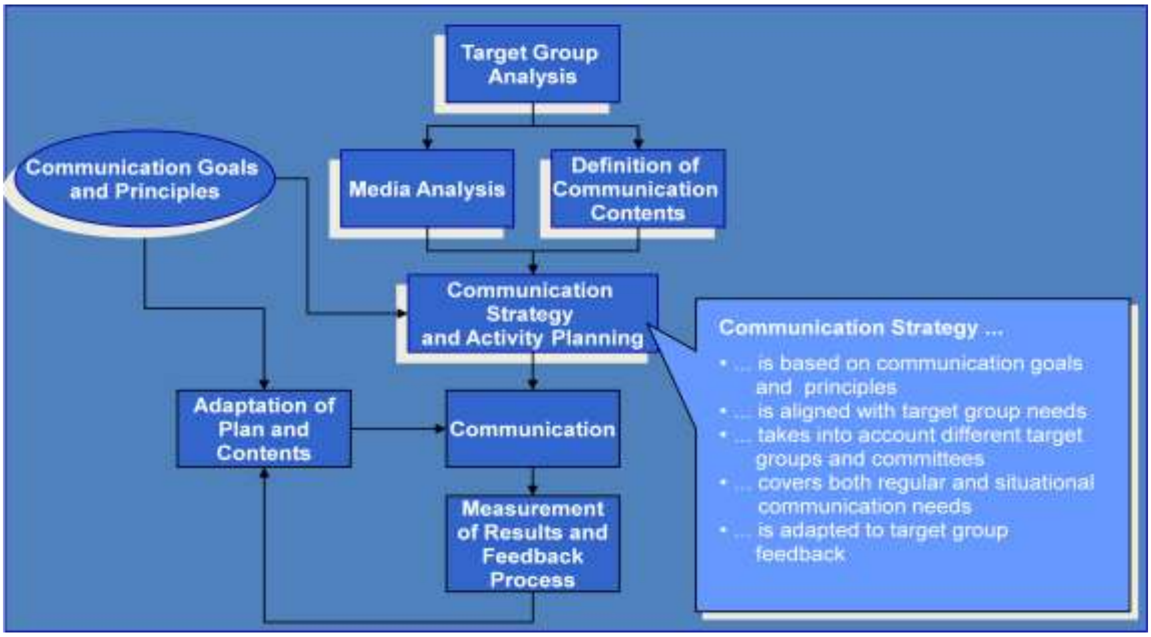
From the simple mapping of the topics to roles and target groups, it will be possible to determine the course content that should be given to the appropriate roles. A roles to topic mapping example is available in Appendix V.

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 the audience 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 publication 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 other organisations with a similar user landscape for examples of good practice and specific awareness raising initiatives.
- ✓ A communication strategy is at the centre of any awareness activity but it needs to be adapted to the specific context.


Target Group Analysis
Communication Goals and Principles
Media Analysis
Definition of Communication Contents
Communication Strategy and Activity Planning
Adaptation of Plan and Contents
Communication
Measurement of Results and Feedback Process

Communication Strategy ...

- ... is based on communication goals and principles
- ... is aligned with target group needs
- ... takes into account different target groups and committees
- ... covers both regular and situational communication needs
- ... is adapted to target group feedback

The strategy can be constructed highlighting the main process steps in any effective awareness raising and training initiative.

Main process	Description
Establish aims and objectives of the initiative and 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 them. • 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 the existence of 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 what will 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 by means of focus groups, interviews, questionnaires or omnibus surveys.

The most effective way to deliver the message as part of any awareness raising and training 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.
- ✓ ISPs.
- ✓ Leading academics.
- ✓ Libraries.
- ✓ Local trade organisations.
- ✓ Media.
- ✓ NGOs.
- ✓ Parent teacher associations.
- ✓ Universities.

Channels of communication

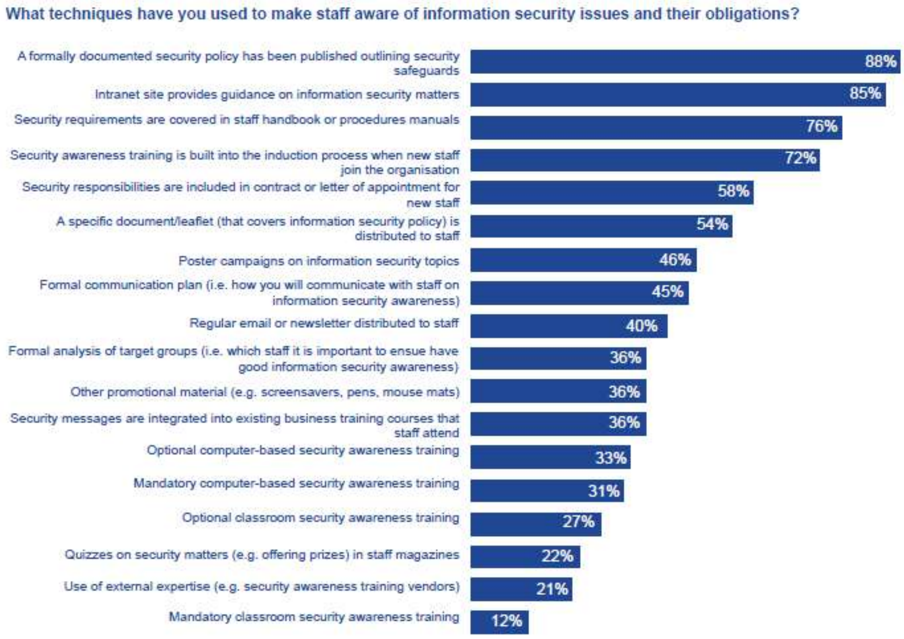
The following matrix details some of the main channels available to help raise users awareness as part of an information security related initiative. The table only lists a selection of advantages and disadvantages and, as such, should not be viewed as a comprehensive guideline.

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.	× Difficult to incorporate messages with more detail.

	✓ Message content can be more abstract in nature.	× May only appeal to a select target group.
Distance 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.
E-mail	✓ Relatively cheap channel to target mass audience. ✓ Allows target group to digest information in own time	× Message may be undermined due to volume of e-mails and spam. × E-mail 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.
E-newsletter	✓ Has similar advantages as the e-mail 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.	× With abundance of information material, message may be

	✓ Information can be universally available when put up on walls.	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 cannot show your subject nor 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.
Screensaver	✓ 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. × Cannot 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 programmes 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.

A poster sample is available in Appendix VI.


What techniques have you used to make staff aware of information security issues and their obligations?
A formally documented security policy has been published outlining security safeguards
88%
Intranet site provides guidance on information security matters
85%
Security requirements are covered in staff handbook or procedures manuals
76%
Security awareness training is built into the induction process when new staff join the organisation
72%
Security responsibilities are included in contract or letter of appointment for new staff
58%
A specific document/leaflet (that covers information security policy) is distributed to staff
54%
Poster campaigns on information security topics
46%
Formal communication plan (i.e. how you will communicate with staff on information security awareness)
45%
Regular email or newsletter distributed to staff
40%
Formal analysis of target groups (i.e. which staff it is important to ensue have good information security awareness)
36%
Other promotional material (e.g. screensavers, pens, mouse mats)
36%
Security messages are integrated into existing business training courses that staff attend
36%
Optional computer-based security awareness training
33%
Mandatory computer-based security awareness training
31%
Optional classroom security awareness training
27%
Quizzes on security matters (e.g. offering prizes) in staff magazines
22%
Use of external expertise (e.g. security awareness training vendors)
21%
Mandatory classroom security awareness training
12%

A survey carried out by ENISA reported that, within the top techniques used to make staff aware of their obligations regarding security issues, a formally documented security policy, a staff handbook, an induction programme and face-to-face training are the most common as illustrated by the graph ([35]).

The figures shown in the 2010 Information security breaches survey confirm this tendency; 90% (88% in 2008) of large respondents have a formally documented and defined security policy; 52% (26% in 2008) provide staff with ongoing education on security; four fifths of UK businesses make their staff aware of their obligations regarding security threats via induction programmes or as part of ongoing education; a third of UK businesses rely on induction alone ([36]).

Guide to communication planning

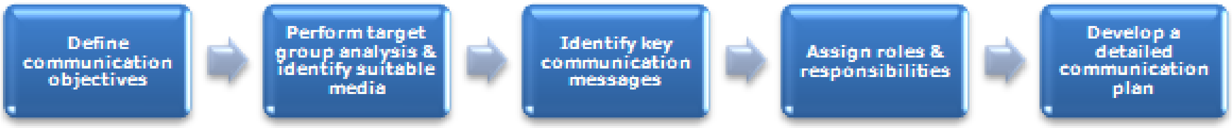
This section presents a process and approach that can be used to develop a comprehensive communication plan by any organisation. The templates and tools presented are intended to be used as starting points by the awareness raising team.

([35]) ENISA, *Information security awareness initiatives: Current practice and the measurement of success*, 2007, available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf (last visited on 19 November 2010).

([36]) PricewaterhouseCoopers LLP (UK), *Information security breaches survey 2010*, available at http://www.pwc.co.uk/eng/publications/isbs_survey_2010.html (last visited on 29 October 2010); BERR, *2008 Information security breaches survey*, 2008, available at http://www.security-survey.gov.uk (last visited on 25 November 2010).

The process

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


Define communication objectives
Perform target group analysis & identify suitable media
Identify key communication messages
Assign roles & responsibilities
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. 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 ICTs.
- ✓ Key concerns.
- ✓ Where they currently receive information.

Information on target groups' experience and knowledge should be taken into consideration while defining the content of the awareness initiative. 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 that 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 its 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 behaviour	Define what types of behaviour 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 completed, 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	√	√		

(*) Sample goals and channel	**Website E-mail**	**Presentations Meetings**	**Workshops Q&A sessions**	**Workshops Face-to-face**

types only.	**Newsletter Publications**	**Conferences**		**seminars Memos**

Suitable channels (*)

Identify key communication messages

The message and the target group are tightly linked; each affects the other. A communication approach should be tailored to ensure topics are relevant to each individual, based on their role and where they work. 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 ICTs. 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	Target group 7
Importance of back-ups	√	√	√	√	√	√	√
Protection of personal information when online (shopping, banking, voting, etc.)	√	√	√	√	√	√	√
Ensuring children reap the benefits of the online world	√			√	√		
Don't be detectable to Bluetooth intruders	√	√		√	√		
…	√	√				√	√
…	√	√		√	√		
…	√	√		√	√		

Illustrative only

A recent study conducted by ENISA reported that there is a strong correlation between the importance employees place on awareness programmes and how well staff understand their messages. The level of engagement of the workforce and, in the long-term, the compliance with the organisation's security practice and procedures is very high when they are provided with not only the key rules for their organisation but also advice for them and their families.

> *Users want to know how they can protect themselves and their families from becoming a victim at home and at work. Raising information security in this manner is an extremely effective method of achieving long-lasting behavioural change.*

Assign roles and 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 communication plan ✓ Ensuring appropriate dissemination of communications ✓ Ensuring adequate sponsorship across all levels ✓ Holding organisation accountable for dissemination of information
Awareness sponsor	✓ Supporting the communication 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 communication strategy and plan ✓ Coordinating the collection of content from the appropriate content experts within the programme ✓ Developing and in some cases delivering communications content against communication plan activities ✓ Ensuring delivery of all required communication activity against the plan

Illustrative only

Develop detailed communication plan

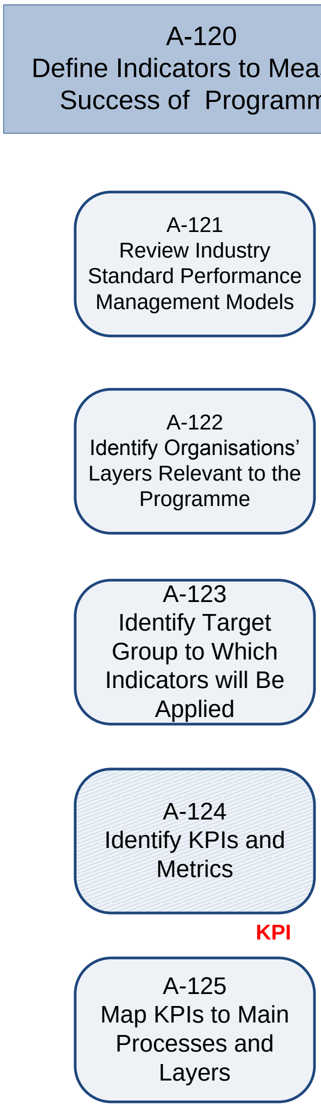
Once communication objectives, channels, key messages, roles and responsibilities are clearly defined, the awareness raising team will be well positioned to build a detailed communication plan. Developing and executing a targeted communication strategy and customised plans will identify, address and 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	Protection of personal	Information	Awareness team	Increase understandin	Coincide with	E-mail

	low to non-existent As the citizens have not grown up with ICTs they may be more doubtful or mistrust technology	information when online	distribution through healthcare solutions Information in cooperation with social security institution		g of issue and solutions available	National Seniors Week	Telephone

Define indicators to measure the success of the programme (A-120)


A-120
Define Indicators to Measure Success of Programme
A-121
Review Industry Standard Performance Management Models
A-122
Identify Organisations' Layers Relevant to the Programme
A-123
Identify Target Group to Which Indicators will Be Applied
A-124
Identify KPIs and Metrics
KPI
A-125
Map KPIs to Main Processes and Layers

The effectiveness of an awareness programme and its ability to improve information security can be measured ([37]). The need for security awareness is widely recognised, but not many public or private organisations have tried to quantify the value of awareness programmes.

[37] ENISA, *Information security awareness initiatives: Current practice and the measurement of success*, 2007, available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf (last visited on 19 November 2010).

Airport operators — The role of metrics and audit

Airport operators are subject to an increasing threat from terrorists and other malicious attacks. They regularly transfer large volumes of information between their systems and third parties. Their key control systems are networked. All of this means information security is of critical importance to their business.

They employ a large number of staff from diverse backgrounds, including lots of temporary and contracting staff. As a result, they choose to use a wide range of techniques to raise security awareness. Since some of the staff are not very computer literate, regular topical e-mails and communications have proved very effective. Monitoring incidents within and outside the organisation allows staff to provide up-to-date guidance.

They have implemented policies and procedures in line with ISO standards. This has not, on its own, improved awareness. Policy is a necessary component of the framework for control, but is simply not very exciting to staff.

Where practical, requirements from the policies have been built into electronic or automated processes. These help staff comply with policy, and produce better activity logs than equivalent manual processes. Reviewing these logs is a quick way to check people's behaviour against policy.

Internal and external audits have played a major role in examining behaviour and checking adherence to process and policy. The audits have successfully highlighted areas where awareness of good practice or policy has been lacking. Since audit reports go to senior management, deficiencies are taken seriously. This makes the approval of new security initiatives and awareness training go more smoothly.

Tracking incidents also sheds light on awareness levels. Investigating the root causes of incidents and downtime has highlighted trends in behaviour. These are then analysed to identify any particular gaps in awareness or training and then addressed in the planning of future awareness initiatives.

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 situations differ greatly.

Which are the indicators?

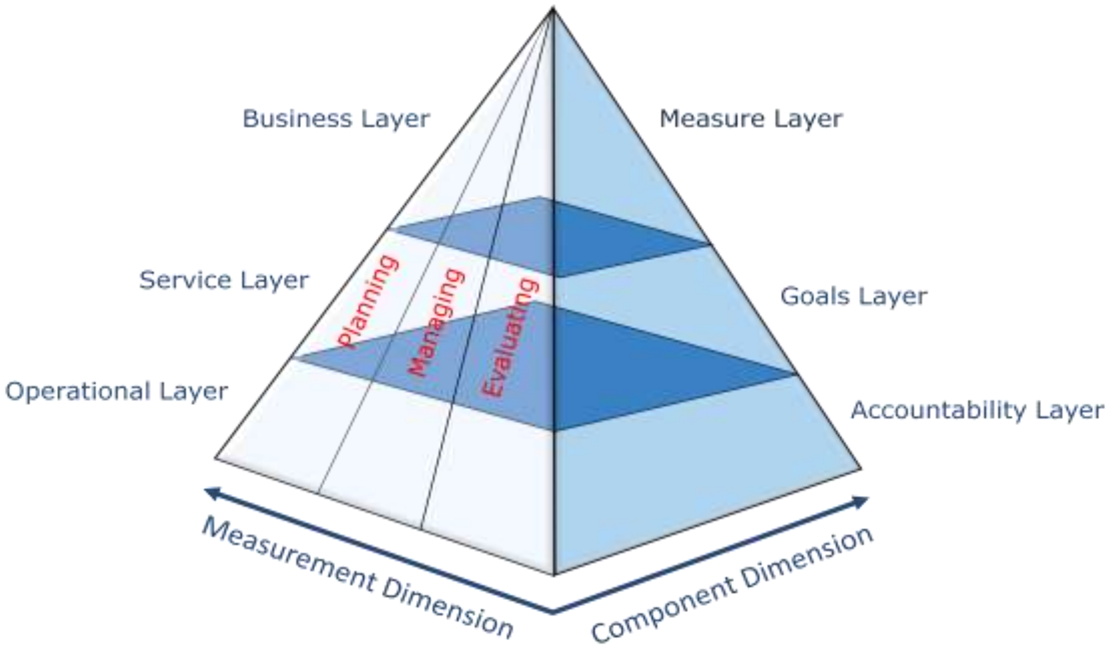
Indicators are metrics and key performance indicators (KPIs). They can be defined as follows:

✓ Metrics: a system of parameters or methods of quantitative assessment of a process that is to be measured, along with the processes to carry out such measurement. Metrics can develop and change based on growing insight over time. Some metrics are stand-alone whereas others are interdependent. They can be further broken down or detailed through key performance indicators.

✓ KPIs): quantifiable metrics used to evaluate objectives to reflect the performance of an organisation. KPIs differ depending on the nature of the organisation. Different layers and dimensions should be taken into consideration. KPIs can constitute both quantitative and qualitative measures; however, the most useful and common types are quantitative based. These include amongst others a focus on metrics such as number of citizens targeted, number of security incidents in the last year compared with the previous year, and number of hits to the website.

To help define performance targets and measurements (including use of metrics and KPIs), several industry standard performance management models, such as Balanced Scorecard or Six Sigma, can be used.

While identifying metrics and KPIs, different layers and dimensions should be taken into consideration as illustrated below.



Layer	Description	Example
Business layer	Measurement of the impact of the function as a whole (e.g. finance, HR) on business objectives	✓ Customer satisfaction ✓ Employee satisfaction ✓ Business specific outcomes ✓ Financial ratios (e.g. cost per FTE)
Service layer	Measurement of the activities and outputs that make up a service	✓ Service level agreement (SLA) ✓ Operator level agreement (OLA)
Operational layer	Detailed processes or technical measurements that are required to run the organisation	✓ Error rate for batch process x ✓ Time to follow procedure

Dimension	Description
Planning	Plan any activity related to an initiative and programme which aims at raising information security awareness.
Managing	Execute and manage any activity related to an initiative and programme which aims at raising information security awareness.

Evaluating	Evaluate and eventually adjust any activity related to an initiative and programme which aims at raising information security awareness.

Below are some of the indicators which were identified.

No	KPIs (*)
1	% of budget spent on awareness training
2	% of time spent on awareness training per FTE
3	age of employees attending an awareness training/average age of total employees
4	cycle time in days between organisation of awareness activities and completion of campaign
5	n. FTEs IT-security trained/total users
6	n. of qualified hits/month
7	total cost of awareness initiative per year
8	total costs of awareness training per FTE
9	total personnel cost of the planning and management awareness initiatives
10	% customer satisfaction with service delivery (i.e. timelines and quality)
11	% employee capability to perform roles
12	% employee satisfaction
13	% increase confidence for elderly
14	% senior management/executives; middle management/professionals; operational works/staff that attended management development programmes
15	% senior management/executives; middle management/professionals; operational works/staff that received a security review
16	% service delivery performance targets achieved
17	% stakeholder satisfaction with communication about the programme
18	% stakeholder satisfaction with governance arrangements
19	% stakeholder understanding of initiative benefits
20	% stakeholders' resistance to change
21	% stakeholders' satisfaction with ability of the system to meet business requirements
22	% employees understanding their role in achieving security goals
23	average number of learning days per employee
24	average personnel cost per FTE for the process 'change management'
25	average personnel cost per FTE for the process 'raising awareness'
26	frequency/relevance of surveys
27	n. benefits realised as stated in business case
28	n. employees per 'develop and counsel-learning' FTE
29	n. of changes in managers' roles
30	n. of changes in staff activities
31	n. of correct answers on self security assessments/total questions
32	n. of employees in charge of development/total employees
33	n. of FTEs for the process 'develop and counsel-learning' per EUR 1 000 cost of continuing operations

34	n. of participants in the awareness survey/total employees
35	n. of self security assessment done/year
36	total cost of the process 'develop and counsel-learning' per EUR 1 000 cost of continuing operations
37	total internal personnel cost of the process 'develop and counsel-learning' per EUR 1 000 cost of continuing operations
38	contribution of ICT training to value added per person engaged in % points
39	n. of employees who passed the exam or certification/total n. of employees
40	n. of organisations adopting the tools/year
41	n. of people who passed the exam or certification/total n. of people interviewed
42	n. of tools downloaded/month
43	n. of topics on security in high school and education/total topics
44	n. of topics on security in standard primary and secondary school education/total topics
45	% of budget allocated to awareness training
46	% of employees born after 1950
47	% of businesses with 10 or more employees using Internet
48	n. access lines and channels in total/per 100 inhabitants
49	n. households with access to home computer/country
50	n. households with access to Internet/country
51	n. mobile subscribers in total/per 100 inhabitants
52	n. broadband subscribers/per 100 inhabitants
53	training cost per FTE
54	cycle time in days to resolve a security problem
55	mean time between discovery and notification of a new threat
56	n. identified fault/year
57	n. of alerts, advisories, notifications, recommendations/month
58	n. of communications with other countries/year
59	n. of systems without implemented password policy/total n. of systems
60	n. of tokens/certificates/eID cards issued/total population
61	n. reported incidents per category/year
62	n. certification scheme adopted by local or international companies
63	n. of e-government projects using the standards/total projects
64	n. of editions/year
65	n. of events listed/month
66	n. of material distributed/edition
67	n. of material distributed/year
68	n. of people attending awareness trainings per campaign
69	n. of training days per staff/year
70	n. of unique visitors/month
71	time to organise an awareness initiative

(*) *Most KPIs are expressed on a pro rata basis (i.e. number of units per FTE or per EUR 1 000 of spend) rather than in absolute terms.*
n. = number of; FTE = full-time equivalent.

Deal with different target groups

It is important to understand that the same evaluation metrics cannot be universally applied to all target groups since interests and needs, as well as the user's situation, differ greatly between the different groups.

When trying to identify metrics for evaluating campaigns aimed, for example, at home user and SME target groups (the most widely targeted groups in information security awareness initiatives), a couple of key observations should be noted.

- ✓ Awareness programmes aimed at SMEs 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 for organisations in the public sector.
- ✓ Public authorities are not necessarily in a position to develop information security policies for home users. Focus should therefore be on developing 'recommended guidelines' or 'best practices' in information security and to promote them to the public.

Tools used primarily in business such as the Pestel (political, environmental, social, technological, ecological and legal) analysis can be used for better understanding the various external influences on the target groups.

By contrast, public authorities will never be in a 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.

Map KPIs to processes and layers

Once KPIs and metrics are identified, in addition to the processes and activities, is it possible to match the indicators to the corresponding processes and layers with which organisations are fulfilling their tasks.

This process will ensure that every relevant step is appropriately tracked and measured. The table below summarises the result of the exercise. The KPIs are taken from the table earlier in this section.

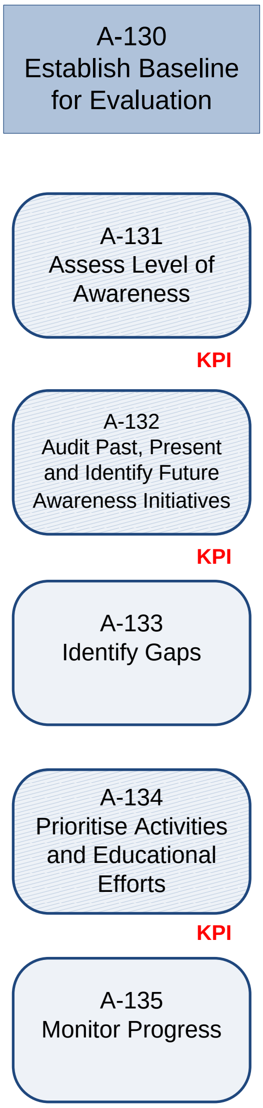
Level	Process	No	KPIs
Business	Evaluating	1	% of budget spent on awareness training
Business	Evaluating	2	% of time spent on awareness training per FTE
Business	Evaluating	3	age of employees attending an awareness training/average age of total employees
Business	Evaluating	4	cycle time in days between organisation of awareness activities and completion of campaign
Business	Evaluating	5	n. FTEs IT-security trained/total users
Business	Evaluating	6	n. of qualified hits/month
Business	Evaluating	7	total cost of awareness initiative per year
Business	Evaluating	8	total costs of awareness training per FTE
Business	Evaluating	9	total personnel cost of the planning and management awareness initiatives
Business	Evaluating	10	% customer satisfaction with service delivery (i.e. timeliness and quality)
Business	Evaluating	11	% employee capability to perform roles

Business	Evaluating	12	% employee satisfaction
Business	Evaluating	13	% increase confidence for elderly
Business	Evaluating	14	% senior management/executives; middle management/professionals; operational works/staff that attended management development programmes
Business	Evaluating	15	% senior management/executives; middle management/professionals; operational works/staff that received a security review
Business	Evaluating	16	% service delivery performance targets achieved
Business	Evaluating	17	% stakeholder satisfaction with communication about the programme
Business	Evaluating	18	% stakeholder satisfaction with governance arrangements
Business	Evaluating	19	% stakeholder understanding of initiative benefits
Business	Evaluating	20	% stakeholders' resistance to change
Business	Evaluating	21	% stakeholders' satisfaction with ability of the system to meet business requirements
Business	Evaluating	22	% employees understanding their role in achieving security goals
Business	Evaluating	23	average number of learning days per employee
Business	Evaluating	24	average personnel cost per FTE for the process 'change management'
Business	Evaluating	25	average personnel cost per FTE for the process 'raising awareness'
Business	Evaluating	26	frequency/relevance of surveys
Business	Evaluating	27	n. benefits realised as stated in business case
Business	Evaluating	28	n. employees per 'develop and counsel-learning' FTE
Business	Evaluating	29	n. of changes in managers' roles
Business	Evaluating	30	n. of changes in staff activities
Business	Evaluating	31	n. of correct answers on self security assessment/total questions
Business	Evaluating	32	n. of employees in charge of development/total employees
Business	Evaluating	33	n. of FTEs for the process 'develop and counsel-learning' per EUR 1 000 cost of continuing operations
Business	Evaluating	34	n. of participants in the awareness survey/total employees
Business	Evaluating	35	n. of self security assessments done/year
Business	Evaluating	36	total cost of the process 'develop and counsel-learning' per EUR 1 000 cost of continuing operations
Business	Evaluating	37	total internal personnel cost of the process 'develop and counsel-learning' per EUR 1 000 cost of continuing operations
Service	Evaluating	38	contribution of ICT training to value added per person engaged in % points
Service	Evaluating	39	n. of employees who passed the exam or certification/total n. of employees
Service	Evaluating	40	n. of organisations adopting the tools/year
Service	Evaluating	41	n. of people who passed the exam or certification/total n. of people interviewed

Service	Evaluating	42	n. of tools downloaded/month
Service	Evaluating	43	n. of topics on security in high school and education/total topics
Service	Evaluating	44	n. of topics on security in standard primary and secondary school education/total topics
Business	Planning	45	% of budget allocated to awareness training
Business	Planning	46	% of employees born after 1950
Operational	Planning	47	% of businesses with 10 or more employees using Internet
Operational	Planning	48	n. access lines and channels in total/per 100 inhabitants
Operational	Planning	49	n. households with access to home computer/country
Operational	Planning	50	n. households with access to Internet/country
Operational	Planning	51	n. mobile subscribers in total/per 100 inhabitants
Operational	Planning	52	n. broadband subscribers/per 100 inhabitants
Business	Planning/Evaluating	53	training cost per FTE
Operational	Planning/evaluating	54	cycle time in days to resolve a security problem
Operational	Planning/evaluating	55	mean time between discovery and notification of a new threat
Operational	Planning/evaluating	56	n. identified fault/year
Operational	Planning/evaluating	57	n. of alerts, advisories, notifications, recommendations/month
Operational	Planning/evaluating	58	n. of communications with other countries/year
Operational	Planning/evaluating	59	n. of systems without implemented password policy/total n. of systems
Operational	Planning/evaluating	60	n. of tokens/certificates/eID cards issued/total population
Operational	Planning/evaluating	61	n. reported incidents per category/year
Service	Planning/evaluating	62	n. certification scheme adopted by local or international companies
Service	Planning/evaluating	63	n. of e-government projects using the standards/total projects
Business	Planning/managing/evaluating	64	n. of editions/year
Business	Planning/managing/evaluating	65	n. of events listed/month
Business	Planning/managing/evaluating	66	n. of material distributed/edition
Business	Planning/managing/evaluating	67	n. of material distributed/year
Business	Planning/managing/evaluating	68	n. of people attending awareness trainings per campaign
Business	Planning/managing/evaluating	69	n. of training days per staff/year
Business	Planning/managing/evaluating	70	n. of unique visitors/month
Business	Planning/managing/evaluating	71	time to organise an awareness initiative

n. = number of; FTE = full-time equivalent.

Establish baseline for evaluation (A-130)


A-130
Establish Baseline for Evaluation
A-131
Assess Level of Awareness
KPI
A-132
Audit Past, Present and Identify Future Awareness Initiatives
KPI
A-133
Identify Gaps
A-134
Prioritise Activities and Educational Efforts
KPI
A-135
Monitor Progress

In the paragraph above, we presented 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. Establishing a baseline will help to audit the existing information security activities within the organisation, identify possible gaps for specific areas and topics, gain support and eventually funding from senior management, prioritise activities and educational efforts, and monitor progress in relation to the starting situation.

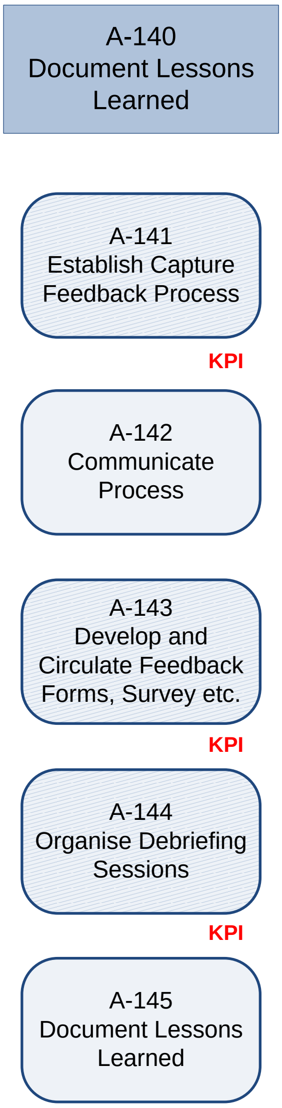
Furthermore, by determining the situation beforehand, it is possible to track the benefits brought about by the awareness programme. Evaluations provide an ideal opportunity to assess which components had the highest rate of success, as well as those that were less successful.

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

An inventory of everything related to information security awareness will help to identify gaps for specifics topics and areas, to provide up-to-date reports regarding the organisation's initiatives and activities in this filed. Furthermore, questionnaires and omnibus surveys provide the opportunity to evaluate the effectiveness of programmes.

An inventory and baseline worksheet together with an awareness questionnaire sample are available in Appendices VII, VIII and IX.

Document lessons learned (A-140)


A-140
Document Lessons Learned
A-141
Establish Capture Feedback Process
KPI
A-142
Communicate Process
A-143
Develop and Circulate Feedback Forms, Survey etc.
KPI
A-144
Organise Debriefing Sessions
KPI
A-145
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 a 'lessons learned' session and how to provide constructive criticism. Below 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 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 in future programmes, as well as it is to record what has or can go wrong and how it may be prevented or addressed in the future.

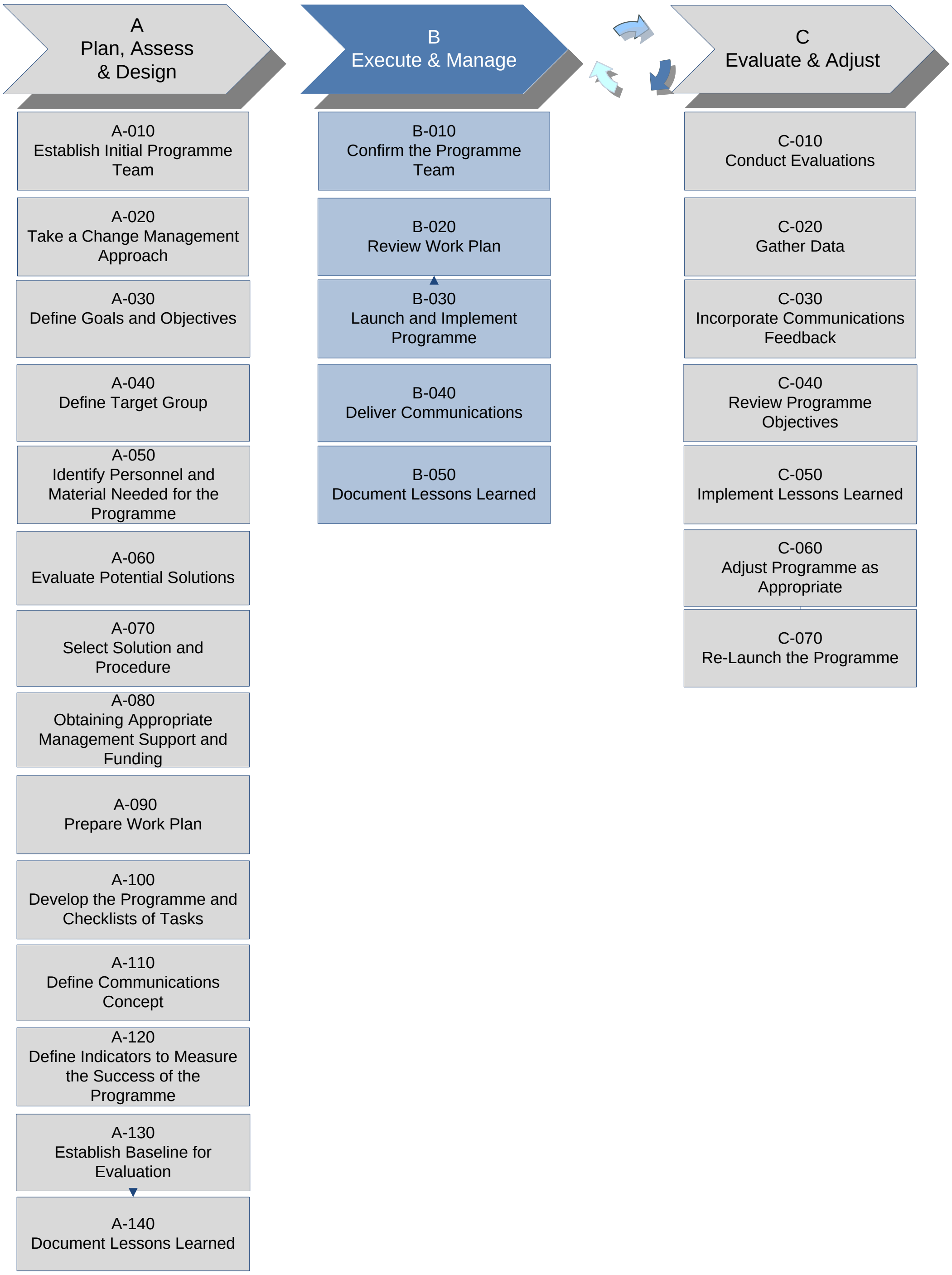
Tips for constructive feedback sessions

- ✓ 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 logs.
- ✓ 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 judgement 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.

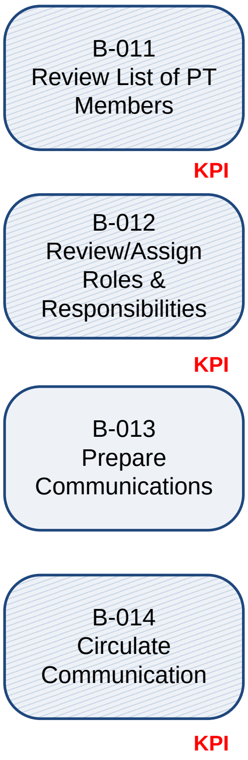
It is important to identify, document and submit lessons learned. The use of a tool is recommended to manage effectively the work. A lesson learned capture form template is available in Appendix X.

Phase II — Execute and manage

This section describes the steps in the execution of a programme in order to identify time-related actions and dependencies.

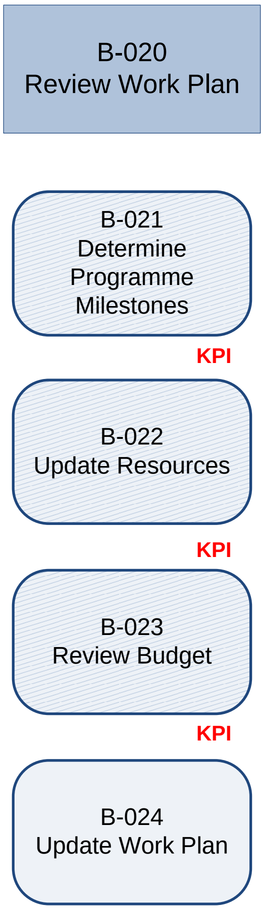

A
Plan, Assess & Design
B
Execute & Manage
C
Evaluate & Adjust
A-010
Establish Initial Programme Team
A-020
Take a Change Management Approach
A-030
Define Goals and Objectives
A-040
Define Target Group
A-050
Identify Personnel and Material Needed for the Programme
A-060
Evaluate Potential Solutions
A-070
Select Solution and Procedure
A-080
Obtaining Appropriate Management Support and Funding
A-090
Prepare Work Plan
A-100
Develop the Programme and Checklists of Tasks
A-110
Define Communications Concept
A-120
Define Indicators to Measure the Success of the Programme
A-130
Establish Baseline for Evaluation
A-140
Document Lessons Learned
B-010
Confirm the Programme Team
B-020
Review Work Plan
B-030
Launch and Implement Programme
B-040
Deliver Communications
B-050
Document Lessons Learned
C-010
Conduct Evaluations
C-020
Gather Data
C-030
Incorporate Communications Feedback
C-040
Review Programme Objectives
C-050
Implement Lessons Learned
C-060
Adjust Programme as Appropriate
C-070
Re-Launch the Programme

Confirm the programme team (B-010)



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.

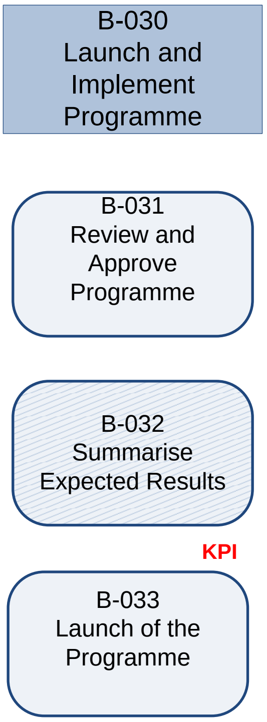
Review work plan (B-020)



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.

The work plan should be used to track progress. To this end the business case could be used as well to guide and assess the project execution and the realisation of benefits.

Launch and implement programme (B-030)


B-030
Launch and Implement Programme
B-031
Review and Approve Programme
B-032
Summarise Expected Results
KPI
B-033
Launch of the 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/or chosen external suppliers to build and deliver the programme with the goal of realising the benefits of information security awareness.

Consider using feedback forms to gather inputs from users who are involved in any awareness programme. Furthermore, encourage users to promptly report any unusual and suspect activity related to information security. Both forms will provide evidence on how behaviour, attitudes and habits have been altered as a result of any awareness efforts.

A feedback form and incident report samples are available in Appendices XI and XII.

If the available budget varies during the implementation of the programme, the suggested course of action would be to either review the desire goals and objectives of the entire programme (e.g. number of groups targeted by the information security initiative) or the selected channel of communications. It is essential to continue the momentum that was created. For example, an SME may wish to rely either on ready-to-use material [38] or to produce it in-house when possible (e.g. leaflet, newsletter, posters etc.).

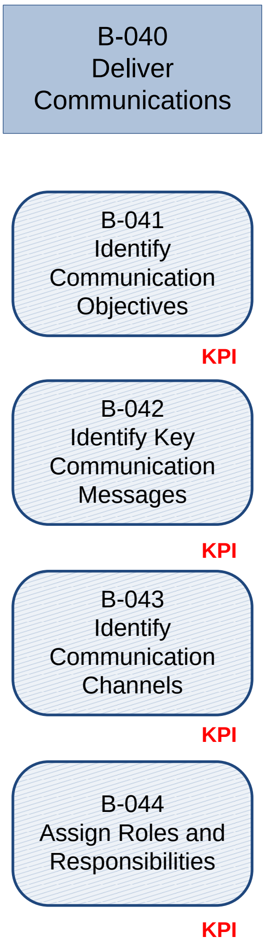
What makes a strong password? ...

.... Use the entire keyboard, not just the most common characters!

www.enisa.europa.eu

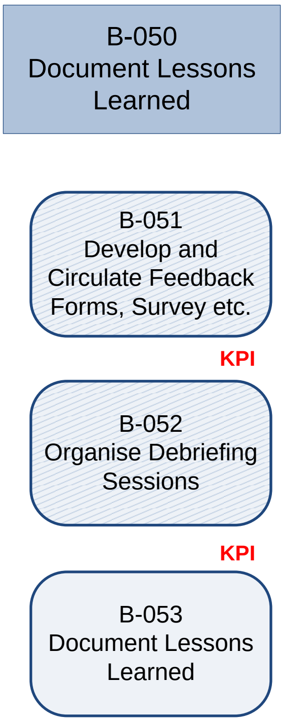
[38] See ENISA, *Training material for small and medium enterprises*, 2010, available at http://www.enisa.europa.eu/act/ar/deliverables/2010/training-material-SMEs (last visited on 25 November 2010).

Deliver communications (B-040)



Raising awareness is about communicating to the selected target groups. It is now time to implement the communication 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 (B-050)

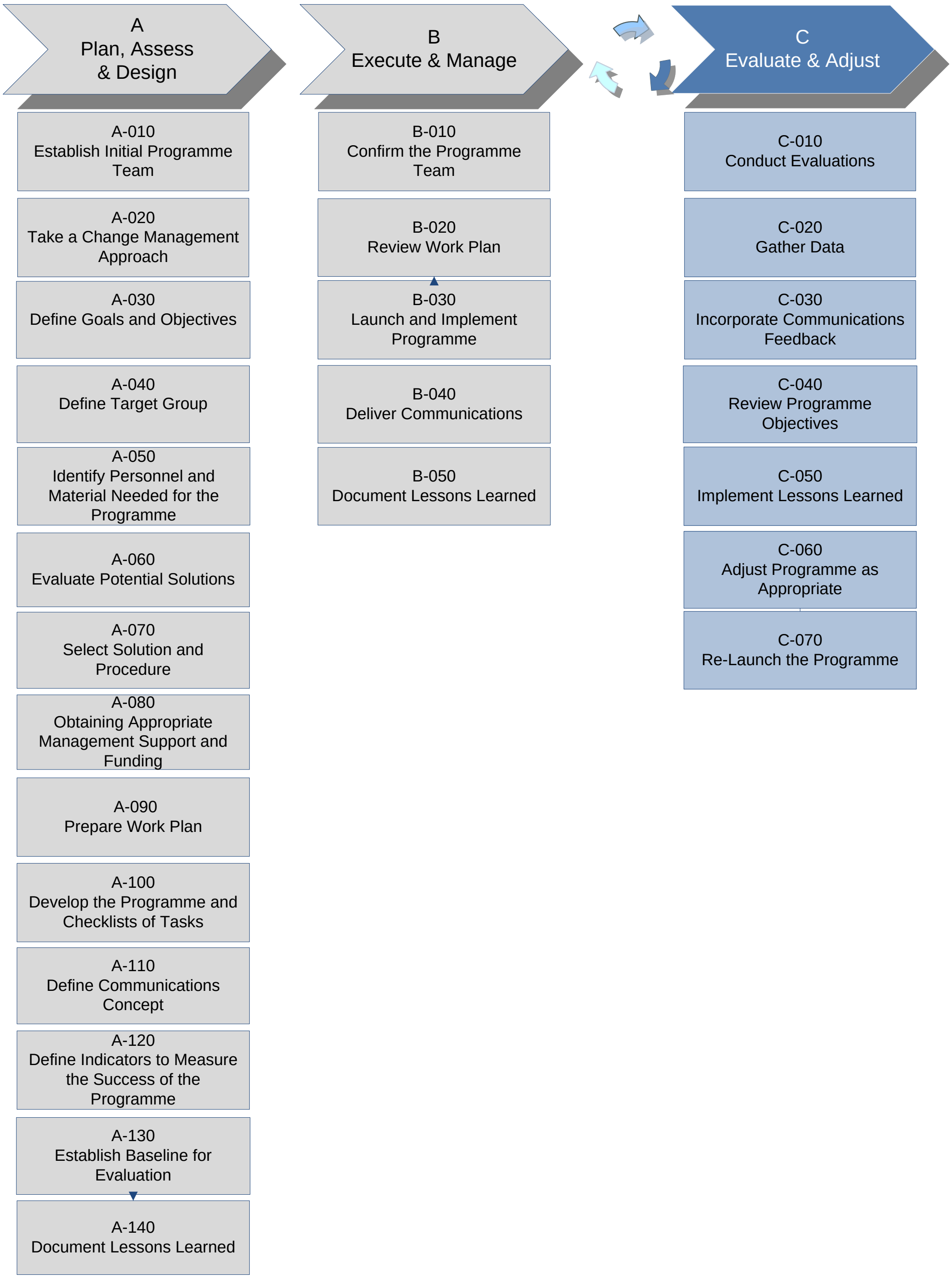


As the programme has been launched and implemented, it is important to capture lessons learned during this second phase. The procedure completed at the end of phase I should be repeated. It will be interesting to compare the historical evolution of the programme from this learning perspective.

Learn from previous and ongoing experiences, build capability for change and celebrate achievements.

Phase III — Evaluate and adjust

This section describes the steps in the evaluation and adjustment of a programme in order to identify time-related actions and dependencies.



A
Plan, Assess & Design

A-010
Establish Initial Programme Team

A-020
Take a Change Management Approach

A-030
Define Goals and Objectives

A-040
Define Target Group

A-050
Identify Personnel and Material Needed for the Programme

A-060
Evaluate Potential Solutions

A-070
Select Solution and Procedure

A-080
Obtaining Appropriate Management Support and Funding

A-090
Prepare Work Plan

A-100
Develop the Programme and Checklists of Tasks

A-110
Define Communications Concept

A-120
Define Indicators to Measure the Success of the Programme

A-130
Establish Baseline for Evaluation

A-140
Document Lessons Learned

B
Execute & Manage

B-010
Confirm the Programme Team

B-020
Review Work Plan

B-030
Launch and Implement Programme

B-040
Deliver Communications

B-050
Document Lessons Learned

C
Evaluate & Adjust

C-010
Conduct Evaluations

C-020
Gather Data

C-030
Incorporate Communications Feedback

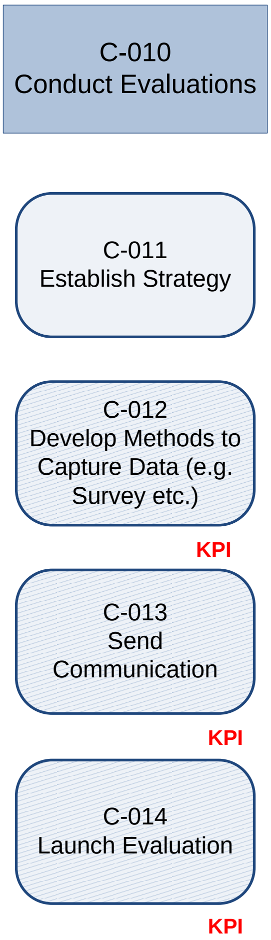
C-040
Review Programme Objectives

C-050
Implement Lessons Learned

C-060
Adjust Programme as Appropriate

C-070
Re-Launch the Programme

Conduct evaluations (C-010)

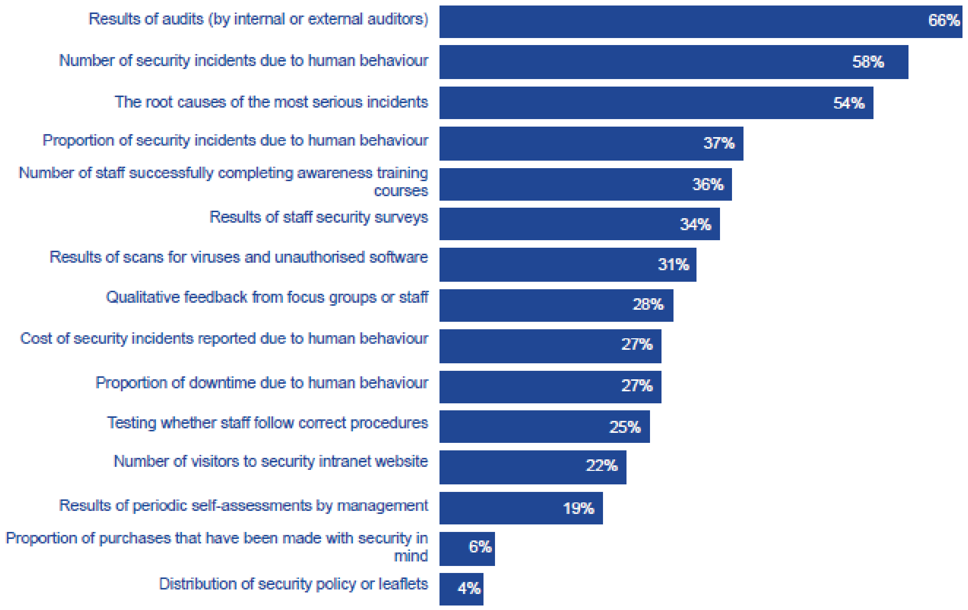


As stated in phase I, the effectiveness of an awareness programme and its ability to improve information security can be measured, despite some claims to the contrary.
The baseline determined prior to the launch of the programme provides a picture of the beginning situation within the target groups. Follow-up questionnaires and omnibus surveys allow the tracking of progress of awareness and help to determine how well users have retained the information presented.

A recent study of ENISA found that a wide variety of different methods are used to measure the effectiveness of information security awareness initiatives ([39]). Organisations appear to find it very difficult to put effective quantitative metrics in place. However, there is little consensus on the most effective measures. Ideally, organisations would like to be able to measure actual changes in staff behaviour resulting from the awareness activities.

([39]) ENISA, *Information security awareness initiatives: Current practice and the measurement of success*, 2007, available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf (last visited on 19 November 2010).

How do you measure the level of information security awareness in your organisation?

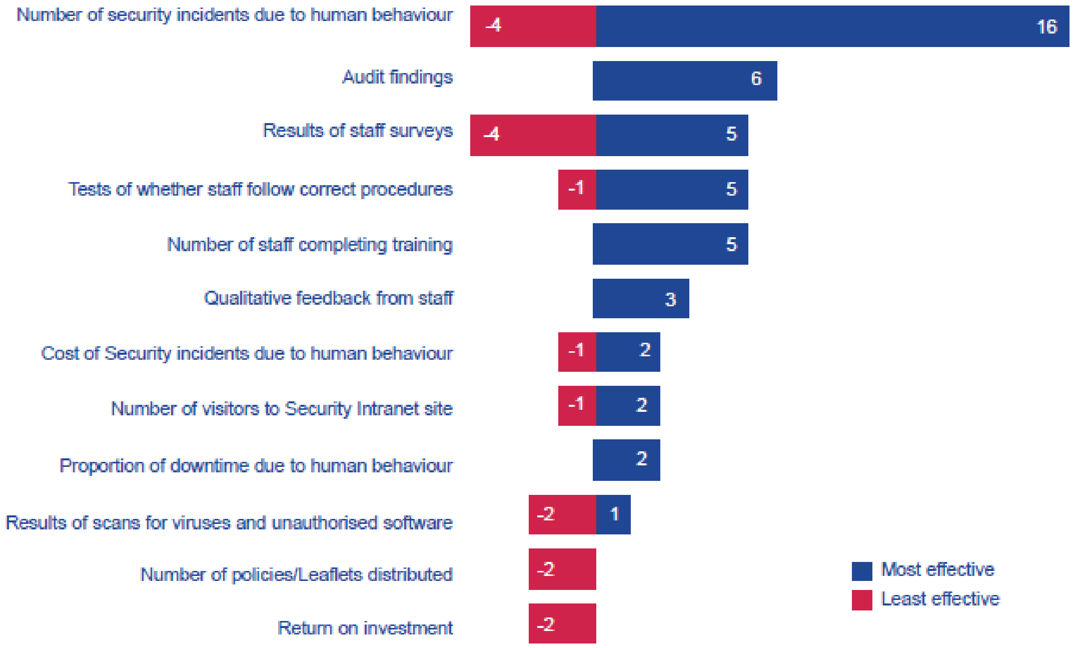


The most popular source of information on actual types of behaviour is audit (internal or external). The auditors' objective and systematic approach was felt to make these reports reliable sources of information.

Moreover, many organisations use their experience of security incidents, in particular the number of incidents caused by human behaviour and root cause analysis of the most serious incidents. Others, however, have abandoned security incident statistics as a measure of security awareness, due to the other factors involved. Thus some of them include questions on security awareness in staff surveys measuring awareness levels before and after initiatives take place. However, some organisations highlight issues with the complexity of collecting and processing this data. This is clearly an area where good practice is evolving.

Some metrics are used because they provide insight into actual types of behaviour (e.g. scans or tests). Others are adopted because they resonate with the senior management that sponsors awareness programmes (e.g. cost of incidents). PwC reports that in UK small organisations spent GBP 4 000 - 7 000 recovering from their worst security incident, while large organisations spent GBP 25 000 – 40 000. Overall the time spent to remediate incidents increased since 2008. A third of large businesses had at least one security incident that took more than ten man-days to deal with, up from 14% two years ago. However, three-fifths of small organisations were able to recover from their security breaches within a man-day each ([40]).

What metrics have proved effective at measuring the success of information security awareness activities?



Organisations have encountered problems in the past, putting effective quantitative measures in place, such as:

- ✓ Quality and comparability issues.
- ✓ Relevance of metrics.
- ✓ Availability of specific indicators.
- ✓ Weighting and processing of data.

Considering these common problems up front can help avoid them. Keeping the approach simple tends to keep it cost-effective. Each organisation needs to find the right balance for them; there is no 'one size fits all' solution.

[40] PricewaterhouseCoopers LLP (UK), *Information Security Breaches Survey 2010*, available at http://www.pwc.co.uk/eng/publications/isbs_survey_2010.html (last visited on 29 October 2010); BERR, *2008 Information security breaches survey*, 2008, available at http://www.security-survey.gov.uk (last visited on 25 November 2010).

A balanced set of metrics can provide real insight into the effectiveness of awareness programmes. Only with this insight are organisations able to change their programmes from a compliance activity to one that really benefits their operations.

Measure the success of the programme

There are four categories by which security awareness can be measured:

- ✓ process improvement;
- ✓ attack resistance;
- ✓ efficiency and effectiveness;
- ✓ internal protections.

Some of them are described below.

Process improvement

This category deals with the development, dissemination and deployment of recommended security guidelines as well as awareness training. Below are some examples of evaluation metrics.

- ✓ 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.)
- ✓ 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.)
- ✓ What percentage of individuals surveyed know that recommended security guidelines exist? How many

International commercial bank — Measuring is critical to targeting efforts

A large commercial bank has a central information security function. This team is responsible for driving awareness training across the world. They aim to get basic messages about security across to a large, geographically dispersed audience. They also need to send specific messages to smaller groups of staff with key roles in systems or security.

A big challenge faced by the bank has been how to measure awareness levels and the effectiveness of its awareness programme. Ideally, the bank wants to measure the change in people's behaviour. This is difficult to assess quantitatively. However, measurement is critical to targeting training efforts at weak areas, so the bank has invested in identifying practical metrics and key performance indicators.

A particularly successful technique has been the use of computer-based training (CBT). A centralised CBT library includes training courses and captures test results from the automated testing of staff. All new employees must complete the training as part of their induction. The training is updated regularly, and all staff must complete the updated training. Reports analyse the extent of completion of CBT training and the scores in tests; the central team monitors these and acts on any significant trends.

Password scans provide a useful direct quantitative measure of the attitude and behaviour of staff. The bank periodically runs software that scans password files on key systems and analyses the strength of individual passwords. The number of staff using easily guessable passwords is a key indicator of security awareness.

Other techniques that have proved effective include simulated phishing e-mails and competitions. These have made the targeted staff think carefully about why they are asked to be secure. They have also provided helpful statistics for trend analysis.

There are plans to introduce a new survey to gauge the level of security awareness and behaviour within the bank. An independent third party will gather responses from a random sample of staff (rather than self-select). This will enable the bank to use the survey results to draw statistically valid conclusions across the business.

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

- ✓ What percentage of individuals are confident that they understand the recommended security guidelines? (Expected change: increase.)
  For SMEs: What percentage of employees have demonstrated through automated testing or other processes that they understand the security policy? (Expected change: increase.)
- ✓ What percentage of individuals know the correct procedure to follow in case of an incident or whom they can call? (Expected change: increase.)
  For SMEs: What percentage of employees know whom to call if an incident occurs or know the correct procedure to follow? (Expected change: increase.)
- ✓ What is the average time for the authority/initiative to deliver a mass warning e-mail 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 e-mail after recognition of a new threat? (Expected change: decrease.)
- ✓ Has an awareness training programme been developed and deployed? (Expected answer: yes.)
  For SMEs: Has any awareness training been developed? (Expected answer: yes.)
- ✓ What percentage of individuals have attended the training? (Expected change: increase.)
  For SMEs: What percentage of employees have attended the training? (Expected change: increase.)
- ✓ 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.)

Attack resistance

This category is concerned with recognition of a security event and resistance to an attack. Below are some examples of evaluation metrics [41].

- ✓ To which extent do staff recognise attacks?
- ✓ To which extent do staff fall prey to attacks?
- ✓ What percentage of surveyed individuals recognise a security event scenario when tested? (Expected change: increase.)
- ✓ What percentage of surveyed individuals fell prey to the chosen scenario? (Expected change: decrease.)
- ✓ 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.)
- ✓ What percentage of users activated a 'test virus'? (Expected change: decrease.)

[41] ENISA, *Information security awareness initiatives: Current practice and the measurement of success*, 2007, available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf (last visited on 19 November 2010).

Efficiency and effectiveness

This category is focused on efficiency and effectiveness with regard to security incidents. Below are some examples of evaluation metrics.

- ✓ What percentage of security incidents experienced by individuals had human behaviour as a majority factor in the root cause? (Expected change: decrease.)
- ✓ 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.)

Internal protections

This category is concerned with how well an individual is protected against potential threats. Below are some examples of evaluation metrics.

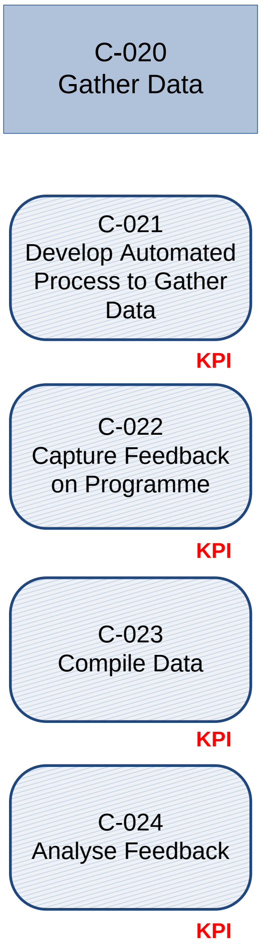
- ✓ What percentage of an individual's software and hardware purchases have been made with security in mind? (Expected change: increase.)

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

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

  For SMEs: What percentage of an SME's critical data is not protected according to the company's security standards? (Expected change: decrease.)
- ✓ What percentage of an individual's system surveyed had malicious software or semi-malicious spyware installed? (Expected change: decrease.)
- ✓ What percentage of an individual's system had any pirated software installed? (Expected change: decrease.)

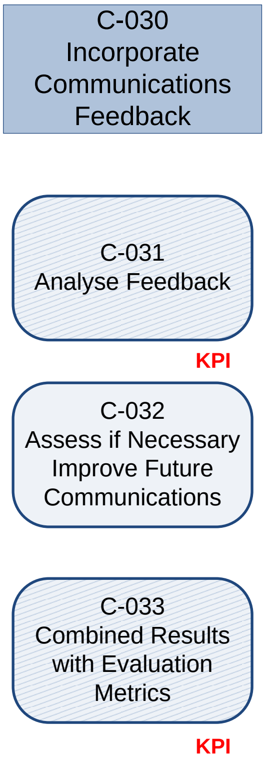
Gather data (C-020)



It is recommended that a combination of quantitative and qualitative information be captured when collecting data by which to measure the performance of awareness raising initiatives. The data should be continually captured (as measuring performance and monitoring the effectiveness of an initiative should be done during and after execution), and should ideally be caught through automated processes.

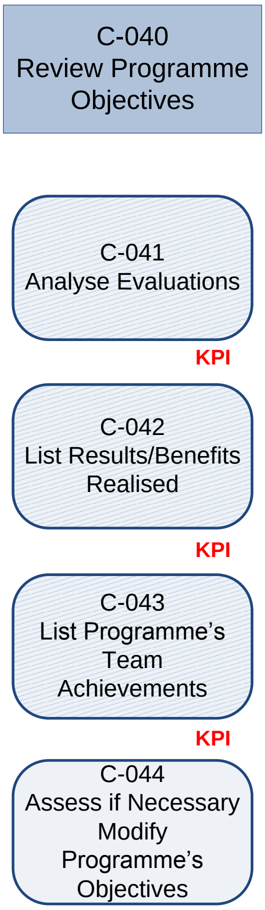
Methods to capture data include among others: questionnaires, website statistics, general observations, statistics from data centres, focus groups, data from call centres/hotlines, number of reports to IT support, press clippings, newsletters, press releases, number signed up to online services, and number of people trained.

Incorporate communications feedback (C-030)


C-030 Incorporate Communications Feedback
C-031 Analyse Feedback
KPI
C-032 Assess if Necessary Improve Future Communications
C-033 Combined Results with Evaluation Metrics
KPI

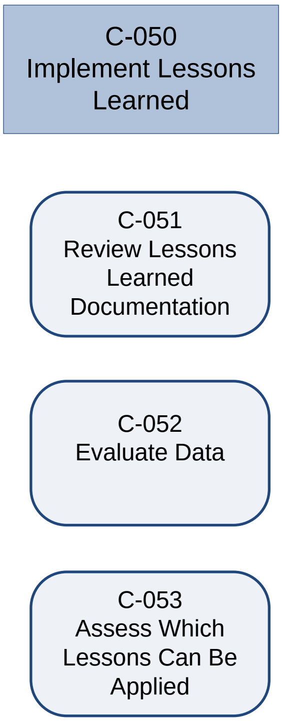
The feedback captured when delivering the programme's communications should be reviewed with a view to how future communications might be improved and made more effective. This information should be combined with the results derived from the evaluation metrics.

Review programme objectives (C-040)


C-040
Review Programme Objectives
C-041
Analyse Evaluations
KPI
C-042
List Results/Benefits Realised
KPI
C-043
List Programme's Team Achievements
KPI
C-044
Assess if Necessary Modify Programme's 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 (C-050)


C-050
Implement Lessons Learned

C-051
Review Lessons Learned Documentation

C-052
Evaluate Data

C-053
Assess Which Lessons Can Be Applied

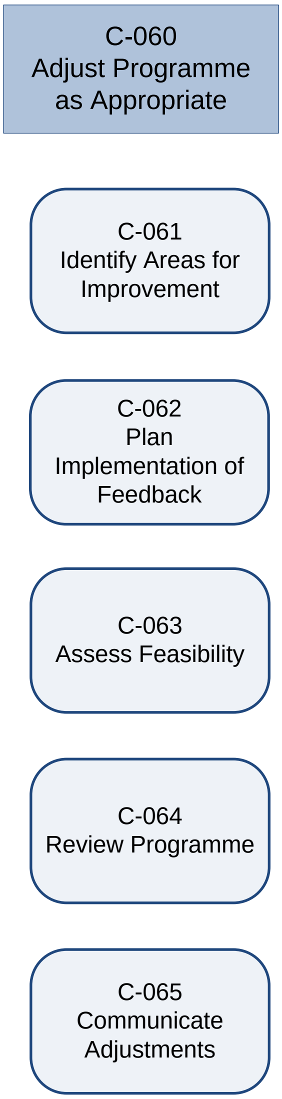
Evaluate the lessons learned from the awareness programme. Which lessons can be applied to increase the effectiveness and success of the programme in the future? The main focus should be to learn from past experiences both positive and less so, then to put that learning into practice.

Government — Implementing lessons learned

A government agency explained why documenting lessons learned is increasingly important for increasing the effectiveness and success of future programme. The government agency wants to ensure that any past experience, either positive or less so, is taken into consideration while planning future awareness initiatives.

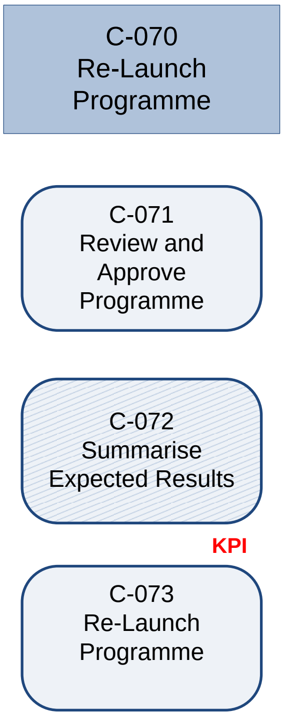
A particularly successful approach has been the use of an external company to run sessions to gather feedback from the awareness programme team. The whole programme team was required to attend the sessions. The external company helped the government agency to implement the findings in future planning phases.

Adjust programme as appropriate (C-060)


C-060
Adjust Programme as Appropriate
C-061
Identify Areas for Improvement
C-062
Plan Implementation of Feedback
C-063
Assess Feasibility
C-064
Review Programme
C-065
Communicate Adjustments

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 (C-070)



Now that the programme has made adjustments based on what was learned to date, the next step is to 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.

Learn from previous and ongoing experiences, build capability for change and celebrate achievements.

Part 3: Overcome obstacles to succeed

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.

	Description
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.
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.
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.
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 audience.
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 communication. 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.
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 the right audience can still be very

	difficult. E-mail 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.
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. This could also result from a budget cut.
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 types of behaviour 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, then users are much more likely to take ownership and follow the new guidelines.
Social engineering	Social engineering may not necessarily have an impact on the implementation of an awareness programme, but it 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 helpdesk, and then trick a gullible person into giving over sensitive information? Some of the most common social engineering methods include impersonation, flattery and a 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.
Changing long-established behaviour	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.
'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. For example, some of the largest and medium-sized US airports report close to 637 000 laptops lost each year, according to the Ponemon Institute survey released on June 2008. Laptops are most commonly lost at security checkpoints, according to the survey. Close to 10 278 laptops are reported lost every week at 36 of the largest US airports, and 65% of those laptops are not reclaimed, the survey said. Around 2,000 laptops are recorded lost at the medium-sized airports, and 69% are not reclaimed ([42]). In Europe in a typical month at Heathrow, up to 120 laptops are handed in to lost property. But apparently, 40% of electronic items are never claimed, and mobile phones make up the bulk of these ([43]).
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.

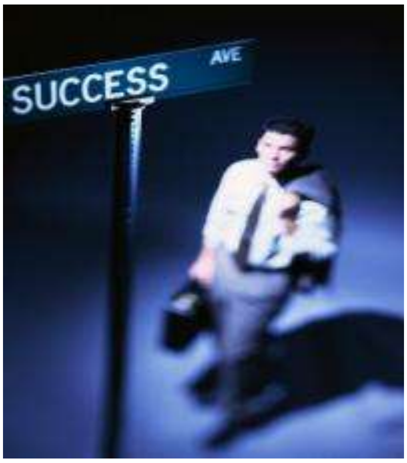
([42]) Shah, Agam, 'Laptops lost like hot cakes at US airports', *PC World*, 30 June 2008, available at http://www.pcworld.com/businesscenter/article/147739/laptops (last visited on 15 July 2008); US Research Ponemon Institute LLC, *Airport insecurity: The case of lost laptops, Executive summary*, 2008, available at http://www.dell.com/downloads/global/services/dell_lost_laptop_study.pdf (last visited on 15 July 2008).

([43]) Dabbs, Alistair, 'Where do all the missing laptops go?', *IT Week*, 18 September 2006, available at http://www.itweek.co.uk/itweek/comment/2164474/missing-laptops (last visited on 22 July 2008).

Critical success factors

Presented below are the main factors for success of any information security programme:

- ✓ A baseline of current status needs to be determined before implementing or relaunching 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.
- ✓ Establish public–private partnerships when required.
- ✓ Security awareness programmes will fail if they are counter to organisational culture or unsupported by senior management.
- ✓ Building continued support for programmes within organisations 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

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 user communities. However, this surge in push-and-pull communication also brings with it security issues that today's governments and companies 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 defence for the security of information systems and networks.

ENISA hopes this guide will provide both private and public organisations with a valuable tool to prepare and implement awareness raising and training 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.

References and sources for further reading

Ajzen, Icek and Martin Fishbein, *Undestanding attitudes and predicting social behaviour*, Prentice-Hall Inc., USA, 1980.

Ajzen, Icek, *Attidudes, Personality and behaviour*, Second edition, Open University Press, USA, 2005.

Basiliere, Pete, *Information breach highlights production print and mail vulnerabilities,* Gartner, 18 September 2007.

Bayan, Ruby, 'Success strategies for security awareness', *TechRepublic*, 2004, available at http://techrepublic.com.com/5100-10878_11-5193710.html# (last visited on 16 July 2008).

BERR, *2008 Information security breaches survey*, 2008, available at http://www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html (last visited on 25 November 2010).

Center for Internet Security
http://www.cisecurity.org/resources.html

CERT Virtual Training Environment, available at https://www.vte.cert.org/vtelibrary.html (last visited on 17 July 2008).

Clayton, Mark, 'Stuxnet spyware targets industrial facilities, via USB memory stick', *The Christian Science Monitor,* 23 July 2010, available at http://www.csmonitor.com/USA/2010/0723/Stuxnet-spyware-targets-industrial-facilities-via-USB-memory-stick (last visited on 17 November 2010).

Cybersecurity Awareness Resource Library
http://www.educause.edu/CybersecurityAwarenessResourceLibrary/8762

Dabbs, Alistair, 'Where do all the missing laptops go?', *IT Week*, 18 September 2006, available at http://www.itweek.co.uk/itweek/comment/2164474/missing-laptops (last visited on 22 July 2008).

Deloitte, *Bringing IT into the boardroom — Implementing technology as a strategic resource for the board,* 2006, available at www.hopewellventures.com/documents/BringingITintotheBoardroom.pdf (last visited on 25 November 2010).

Deloitte, *2008 Survey on the IT-business balance*, 2008, available at http://www.deloitte.com/dtt/cda/doc/content/IT%20Business%20Balance%20Report_2008_CMYK.pdf. (last visited on 21 July 2008).

ENISA, *Raising awareness in information security — Insight and guidance for Member States,* 2005, available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_cd_awareness_raising.pdf (last visited on 19 November 2010).

ENISA, *Information security awareness initiatives: Current practice and the measurement of success*, 2007, available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf (last visited on 19 November 2010).

ENISA, *Key facts and figures about the AR Community and its members (May 10),* 2010, available at http://www.enisa.europa.eu/act/ar/deliverables/2010/facts-and-figures-may-10 (last visited on 19 November 2010).

ENISA, *Secure USB flash drives*, 2008, available at http://www.enisa.europa.eu/act/ar/deliverables/2008/secure-usb-flash-drives-en/at_download/fullReport (last visited on 19 November 2010).

ENISA*, Secure printing,* 2008, available at http://www.enisa.europa.eu/doc/pdf/ENISA_secure_printing.pdf (last visited on 19 November 2010).

ENISA*, Obtaining support and funding from senior management*, 2008, available at http://www.enisa.europa.eu/act/ar/deliverables/2008/obtaining-support (last visited on 19 November 2010).

ENISA, *Training material for small and medium enterprises*, 2010, available at http://www.enisa.europa.eu/act/ar/deliverables/2010/training-material-SMEs (last visited on 25 November 2010).

Ford, Richard, 'Disc listing foreign criminals lost for year'*, The Times*, 20 February 2008, available at http://www.timesonline.co.uk/tol/news/politics/article3399712.ece (last visited on 15 July 2008).

Getsafeonline
http://www.getsafeonline.org/

Girard, John and Avivah Litan, *New data loss highlights problems with contractors and laws,* Gartner, 4 February 2008.

Heidt, Erik T., *Basics of the quick business case: How to champion your next information security initiative*, RSA Conference Europe 2007, 2007, available at http://artofinfosec.com/22/art-of-info-sec-001-quick-business-case/ (last visited on 22 July 2008).

Herold, Rebecca, *Addressing the insider threat,* IT Compliance in Realtime, Realtime publishers, May 2008, Volume I, Number 3, available at http://nexus.realtimepublishers.com/RTITC.htm (last visited on 31 July 2008).

Herold, Rebecca, *Information security and privacy awareness program*, Auerbach Publications, USA, 2005.

Hinson (Dr), Gary, 'The true value of information security awareness', *Noticebored*, 2008, available at http://www.noticebored.com/html/why_awareness_.html (last visited on 17 July 2008).

Housel, Thomas and Arthur H. Bell, *Measuring and managing knowledge*, McGraw-Hill international edition, Singapore, 2001.

Information Systems Security Association
http://www.issa.org/

Information Warfare Site, *Security awareness*, available at http://www.iwar.org.uk/comsec/resources/sa-tools/ (last visited on 5 July 2008).

IT Governance Institute, *Information security governance: Guidance for boards of directors and executive management*, second edition, USA, 2006.

Jevans, Dave, *Privacy and identity theft,* IronKey, available at http://blog.ironkey.com/?cat=9&paged=2 (last visited on 20 May 2008).

McMurchy, Neil*, Take these steps to develop successful BI business cases,* Gartner, 1 February 2008.

McMurchy, Neil, *Toolkit: Building the business intelligence business case — Identifying and calculating benefits,* Gartner, 25 April 2008.

National Cyber Security Alliance (NCSA)
http://www.staysafeonline.org/

NIST, *Information technology security training requirements: A role- and performance-based model*, NIST — SP 800-16, USA, 1998, available at http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf (last visited on 21 July 2008).

NIST, *Building an information technology security awareness program*, NIST — SP800-50, USA, 2003, available at http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf (last visited on 17 July 2008).

Noticebored, *Business case for an information security awareness program*, 2008, available at http://www.noticebored.com/NB_generic_business_case_for_infosec_awareness_program.pdf (last visited on 17 July 2008).

OECD, *Implementation plan for the OECD guidelines for the security of information systems and networks: Towards a culture of security,* DSTI/ICCP/REG(2003)5/REV1, Working Party on Information Security and Privacy, OECD, 2003, available at http://www.oecd.org/dataoecd/23/11/31670189.pdf (last visited on 25 November 2010)

Parmenter, David, *Key performance indicators – Developing, implementing and using winning KPIs*, John Wiley & Sons Inc., USA, 2007.

PricewaterhouseCoopers LLP, *2011 Global state of information security survey*, 2010, available at http://www.pwc.com/gx/en/information-security-survey/index.jhtml (last visited on 29 October 2010).

PricewaterhouseCoopers LLP (UK), *Information security breaches survey 2010*, available at http://www.pwc.co.uk/eng/publications/isbs_survey_2010.html (last visited on 29 October 2010).

PricewaterhouseCoopers LLP (UK), *Protecting your business – Security awareness: Turning your people into your first line of defence*, 2010, available at http://www.pwc.co.uk/eng/publications/protecting_your_business_security_awareness.html (last visited on 29 October 2010).

PricewaterhouseCoopers LLP (UK), *Revolution or evolution? Information security 2020*, 2010, available at http://www.pwc.co.uk/eng/publications/revolution_or_evolution_information_security_2020.html (last visited on 29 October 2010).

Rasmussen, Gideon, *Building a security awareness*, available at http://www.gideonrasmussen.com/article-01.html (last visited on 16 July 2008).

Roberts, John P., *Toolkit sample template: An effective business case,* Gartner, 11 July 2007.

SANS, *SANS InfoSec Reading Room — Security Awareness Section*, available at http://www.sans.org/rr/whitepapers/awareness (last visited on 17 July 2008).

SANS, *The SANS security policy project*, available at http://www.sans.org/resources/policies/ (last visited on 17 July 2008).

Shah, Agam, 'Laptops lost like hot cakes at US airports', *PC World*, 30 June 2008, available at http://www.pcworld.com/businesscenter/article/147739/laptops (last visited on 15 July 2008).

Simpson, Aislinn, 'NHS: Personal details of 18,000 staff 'lost in the post'', *Telegraph.co.uk*, 15 September 2008, available at http://www.telegraph.co.uk/health/2965231/NHS-Personal-details-of-18000-staff-lost-in-the-post.html (last visited on 25 November 2010).

'UK's families put on fraud alert', *BBC News*, 20 November 2007, available at http://news.bbc.co.uk/2/hi/7103566.stm (last visited on 29 October).

US-CERT, *Cyber security tips*, available at http://www.us-cert.gov/cas/tips/index.html (last visited on 17 July 2008).

US-CERT, *Home network security*, available at http://www.us-cert.gov/reading_room/home-network-security/ (last visited on 17 July 2008).

Maeesearch Ponemon Institute LLC, *Airport insecurity: The case of lost laptops, Executive summary*, 2008, available at http://www.dell.com/downloads/global/services/dell_lost_laptop_study.pdf (last visited on 15 July 2008).

Watson, Paul, 'US military secrets for sale at Afghanistan bazaar', *Los Angeles Times*, 10 April 2006.

Wooding, Steve, Anhal, Aarti and Lorenzo Valeri, *Raising citizen awareness of information security: A practical guide*, eAware project, RAND Europe, 2003, available at http://www.clusit.it/whitepapers/eaware_practical_guide.pdf (last visited on 17 July 2008).

Woody, Carol and Larry Clinton, *Common sense guide to cyber security for small businesses — Recommended actions for information security*, Internet Security Alliance, 2004, available at http://www.us-cert.gov/reading_room/CSG-small-business.pdf (last visited on 17 July 2008).

APPENDICES

Appendices — Templates and samples

Appendix I — Target group data capture template

Target group			
Definition			
Category		Interests	
Sub-category		Needs	
Size/dimension		Knowledge	
Geography		Channel	

Sample/ recommendations	

Appendix II — 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 a 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 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 call on as references.
5. Interviews with finalists will be held during the week of *<Date>.*

Appendix III — 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		

Appendix IV — Work plan sample

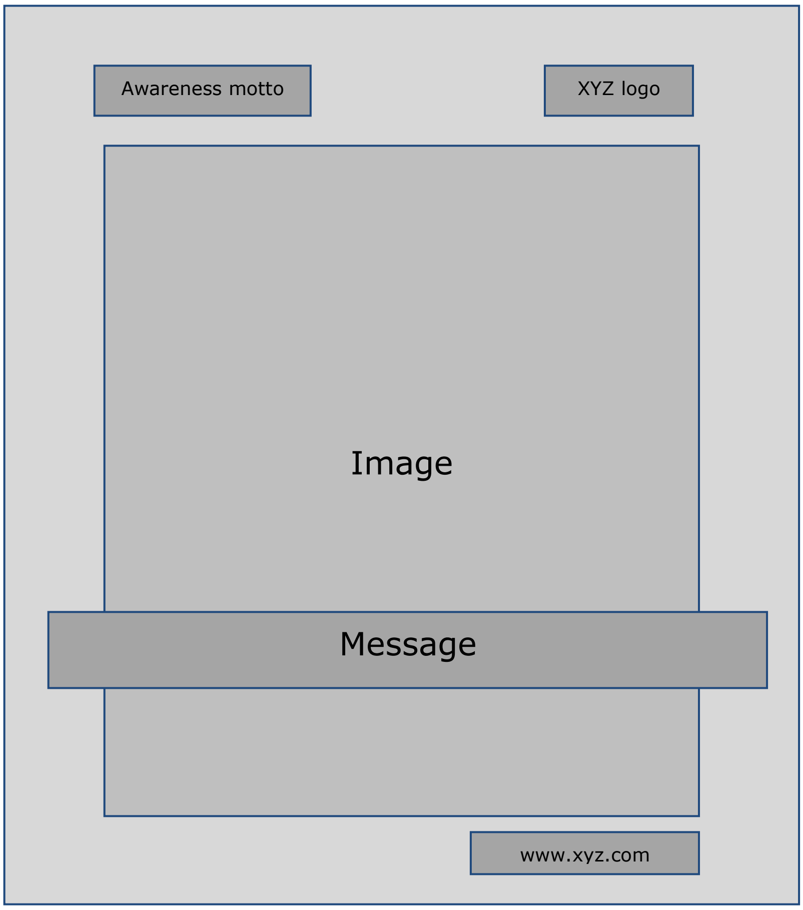
Activities	Target activity start date	Target activity completion date	Outputs
List each activity and provide a brief description of the activity and any sub-activities (main purpose, etc.)			For each activity listed, indicate what will be produced.
I. Plan, assess and design			
- Establish initial programme team	April 2010	April 2010	- team identified
- Take change management approach	April 2010	April 2010	- programme principles identified
- Obtain appropriate management support and funding	April 2010	June 2010	- explicit management support and budget approval
- Identify personnel and material needed for programme	May 2010	May 2010	- shortlist of personnel and materials
- Evaluate potential solutions	May 2010	June 2010	- 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 2010	July 2010	- signed contract
- Prepare work plan	June 2010	June 2010	- work plan
- Define goals and objectives	June 2010	July 2010	- programme goals and objectives formalised and agreed
- Define target groups	June 2010	July 2010	- target groups identified and needs documented
- Define the programme and checklist of tasks	June 2010	July 2010	- programme developed
- Develop communications concept	June 2010	July 2010	- 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 2010	July 2010	- evaluation metrics
- Establish baseline for evaluation	June 2010	July 2010	- assessment of present situation
- Document lessons learned	July 2010	July 2010	- lessons learned recorded

II. Execute and Manage			
- Confirm programme team	August 2010	August 2010	- team confirmed
- Review work plan	August 2010	August 2010	- final work plan
- Launch and implement programme	October 2010	January 2007	
- Deliver communications	October 2010	January 2010	- communications plan implemented
- Document lessons learned	January 2011	January 2011	- lessons learned recorded
III. Evaluate and Adjust			
- Conduct evaluations	February 2011	March 2011	- survey results
- Incorporate communications feedback	February 2011	March 2011	- communications feedback
- Review programme objectives	February 2011	March 2011	-programme objectives
- Implement lessons learned	March 2011	April 2011	- updated lessons
- Adjust programme as appropriate	March 2011	April 2011	-updated work plan
- Re-launch the programme	May 2011		

Appendix V — Roles to topic mapping example

Role	**Topic**											
	Information security policies and procedures	*Workstation security*	*Website policies*	*E-mail security*	*Social engineering*	*Third-party and partner security*	*Identity verification*	*Technical security mechanisms*	*Information classification and controls*	*Incident response*	*Asset management (e.g. USB flash drives, printing devices, etc.)*	……
R*n*	X				X		X		X			X
R*n*+1	X			X		X				X		
R*n*+2		X				X			X	X		
R*n*+3			X	X			X		X			X
R*n*+4					X	X		X		X	X	X
R*n*+*n*	X		X	X	X	X		X	X	X		X

Appendix VI — Poster sample



Appendix VII — Information security awareness inventory worksheet template

INFORMATION SECURITY AWARENESS INVENTORY WORKSHEET					
Organisation name:					
Programme name:					
Goals and objectives	Topic description		Target group	Executive support? Y/N	Baseline measurement? Y/N
Programme been given? Y/N	Date	Next delivery date	Frequency	Group size	Local, national, international?
Delivery methods	Language		Notes		

Appendix VIII — Information security awareness baseline worksheet template

INFORMATION SECURITY AWARENESS OFFERING BASELINE WORKSHEET		
Name reviewer:		
Date:		
Awareness programme name:		
Trainer name:		
Delivery method:		Language:
Management support:		Communications sent out:
List scheduled and past activities related to this programme:		
List goals and objectives completed:		
Strengths:		
Weaknesses:		
Participation:	n. of attendees/total n. of users invited to date	Reasons for discrepancies:
	n. of users still have to attend/ total n. of users should participate	
Evaluation forms:	n. of evaluation forms collected/total n. of evaluation forms distributed	Main comments/suggestions gathered:

Appendix IX — Awareness questionnaire sample — for use by a public authority

AWARENESS QUESTIONNAIRE

[*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 do 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 apply)?
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 apply:
a. _____Viruses and worms
b. _____Spam and other unsolicited e-mails
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 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 back-up 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 to 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) ____

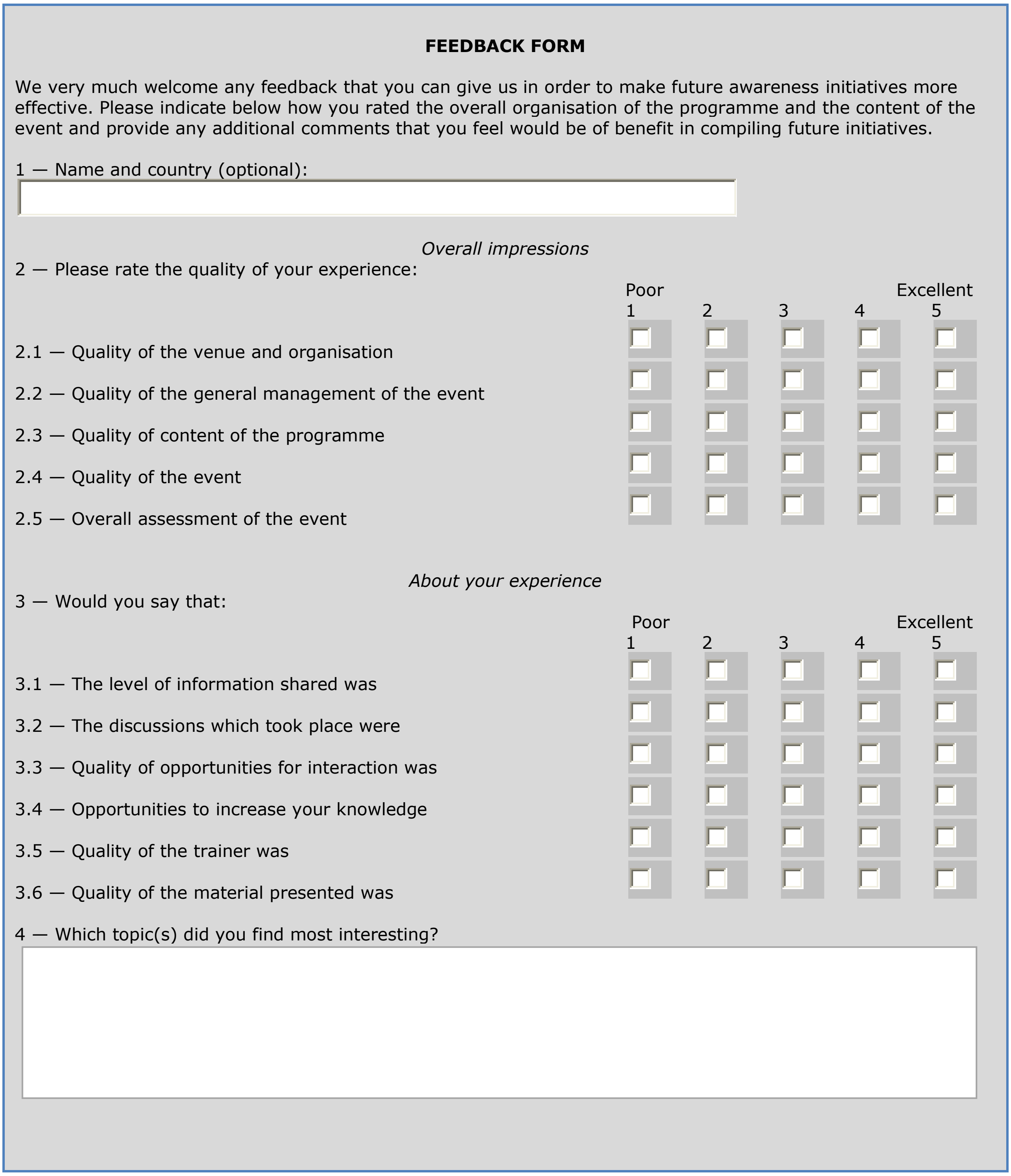
Thank you for participating in this survey. We plan to use your answers to help us develop information in order to raise awareness of the importance of information security.

Please check here if you would like to receive additional information on information security.
o Yes
o No

Appendix X — Lessons learned capture form template

LESSONS LEARNED			File No	Page of
			Category (primary/alternate):	
Title/subject:			Keywords:	
Event description:				
Lessons learned:				
Recommendations:				
Attachments:		References:		
Submitted by:	Project/office:	Org./company:	Location:	Date of occurrence:
Telephone:	E-mail:	Specialisation:	Building/room:	Date submitted:

Appendix XI — Feedback form sample



FEEDBACK FORM

We very much welcome any feedback that you can give us in order to make future awareness initiatives more effective. Please indicate below how you rated the overall organisation of the programme and the content of the event and provide any additional comments that you feel would be of benefit in compiling future initiatives.

1 — Name and country (optional):

Overall impressions

2 — Please rate the quality of your experience:

	Poor 1	2	3	4	Excellent 5
2.1 — Quality of the venue and organisation	□	□	□	□	□
2.2 — Quality of the general management of the event	□	□	□	□	□
2.3 — Quality of content of the programme	□	□	□	□	□
2.4 — Quality of the event	□	□	□	□	□
2.5 — Overall assessment of the event	□	□	□	□	□

About your experience

3 — Would you say that:

	Poor 1	2	3	4	Excellent 5
3.1 — The level of information shared was	□	□	□	□	□
3.2 — The discussions which took place were	□	□	□	□	□
3.3 — Quality of opportunities for interaction was	□	□	□	□	□
3.4 — Opportunities to increase your knowledge	□	□	□	□	□
3.5 — Quality of the trainer was	□	□	□	□	□
3.6 — Quality of the material presented was	□	□	□	□	□

4 — Which topic(s) did you find most interesting?

5 — What aspects of the event did you find most valuable?

6 — Would you welcome the organisation of a similar initiative in the future? Yes □ No □

7 — Are there any topics or activities that you would like to see included in a future event?
Please give suggestions below:

Additional comments

8 — Please provide below any other comments that you wish to make:

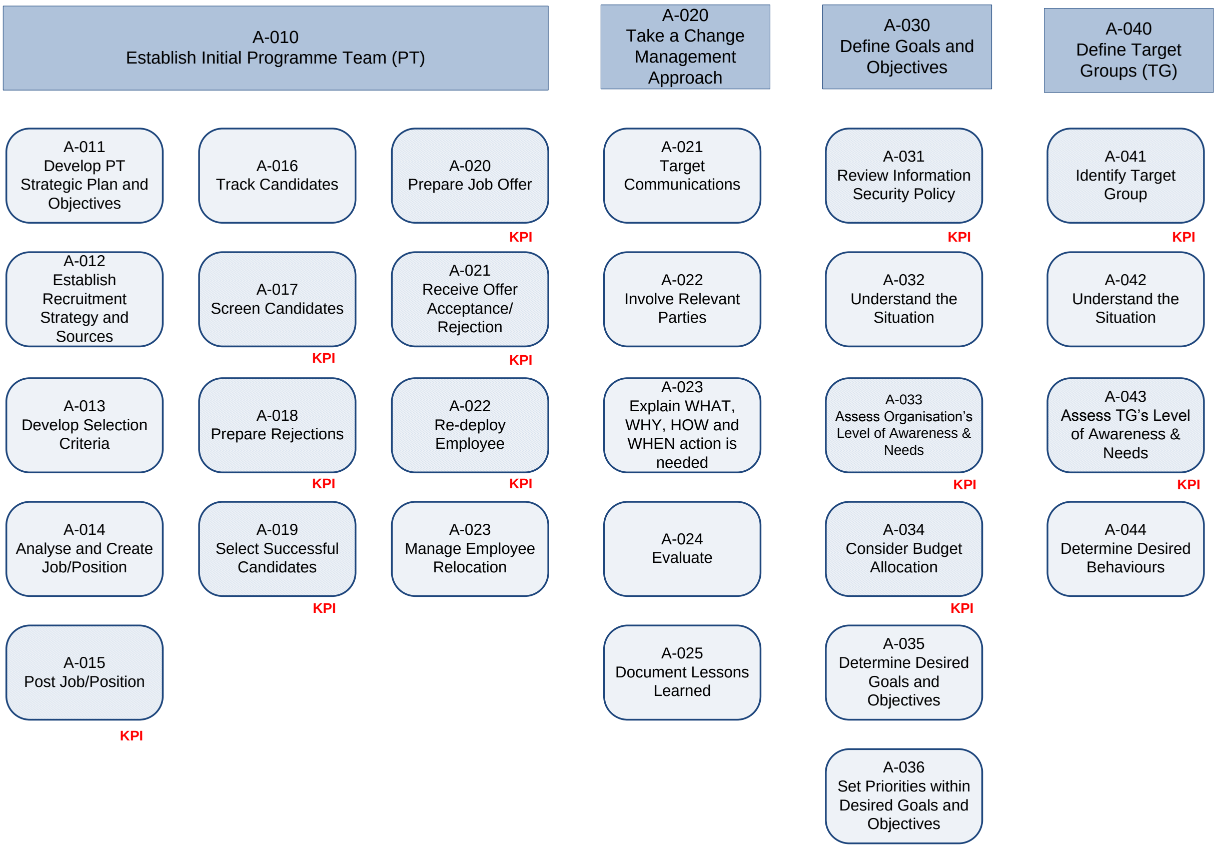
THANK YOU FOR YOUR FEEDBACK. PLEASE HAND THIS EVALUATION FORM TO A MEMBER OF THE ORGANISATION COMMITTEE OR LEAVE IT ON YOUR SEAT FOR COLLECTION.

Appendix XII — Incident report sample

INCIDENT REPORT	
Name:	E-mail:
Department:	Phone:
Description of unusual or suspicious event:	
Date:	
Location:	

Process mapping

Appendix XIII — Plan, assess and design



A-010
Establish Initial Programme Team (PT)

- A-011 Develop PT Strategic Plan and Objectives
- A-012 Establish Recruitment Strategy and Sources
- A-013 Develop Selection Criteria
- A-014 Analyse and Create Job/Position
- A-015 Post Job/Position — KPI
- A-016 Track Candidates
- A-017 Screen Candidates — KPI
- A-018 Prepare Rejections — KPI
- A-019 Select Successful Candidates — KPI
- A-020 Prepare Job Offer — KPI
- A-021 Receive Offer Acceptance/ Rejection — KPI
- A-022 Re-deploy Employee — KPI
- A-023 Manage Employee Relocation

A-020
Take a Change Management Approach

- A-021 Target Communications
- A-022 Involve Relevant Parties
- A-023 Explain WHAT, WHY, HOW and WHEN action is needed
- A-024 Evaluate
- A-025 Document Lessons Learned

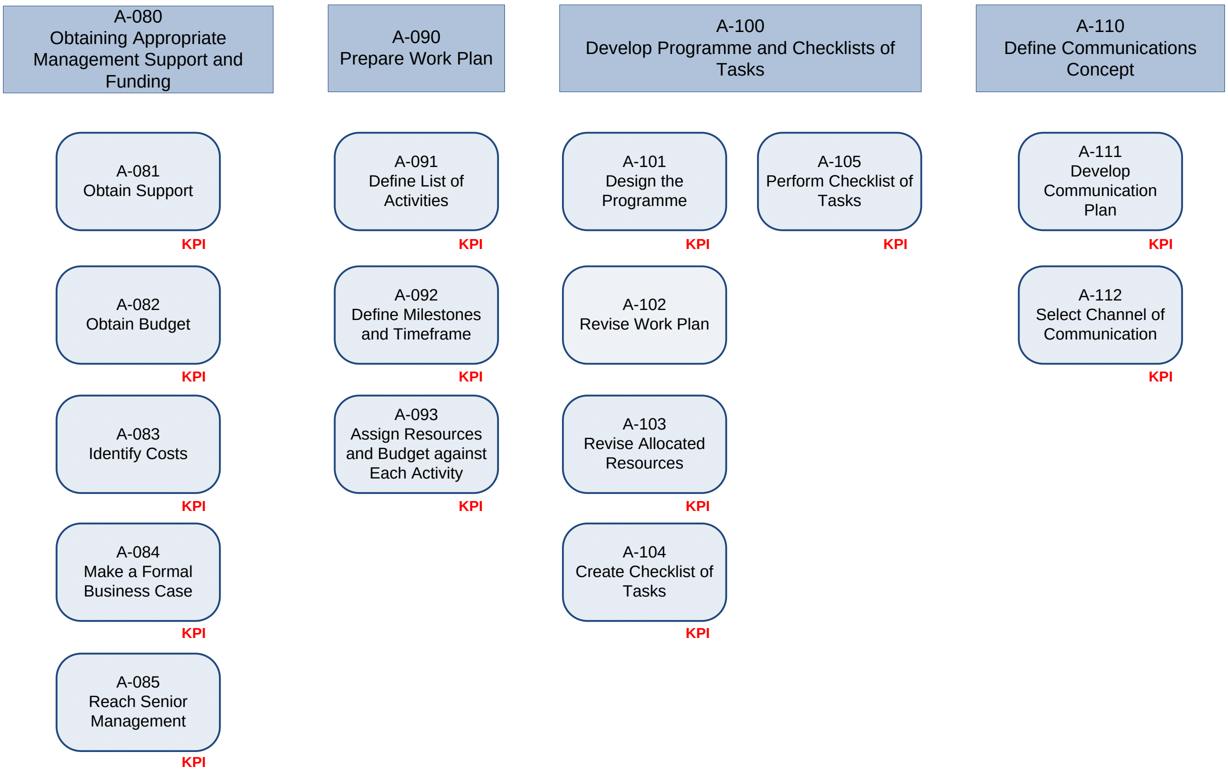
A-030
Define Goals and Objectives

- A-031 Review Information Security Policy — KPI
- A-032 Understand the Situation
- A-033 Assess Organisation's Level of Awareness & Needs — KPI
- A-034 Consider Budget Allocation — KPI
- A-035 Determine Desired Goals and Objectives
- A-036 Set Priorities within Desired Goals and Objectives

A-040
Define Target Groups (TG)

- A-041 Identify Target Group — KPI
- A-042 Understand the Situation
- A-043 Assess TG's Level of Awareness & Needs — KPI
- A-044 Determine Desired Behaviours

A-050 Identify Personnel and Material for Programme				A-060 Evaluate Potential Solutions	A-070 Select Solution and Procedure
A-050-5 Develop PT Strategic Plan and Objectives	A-053 Analyse and Create Job/Position	A-055-5 Select Successful Candidates KPI	A-058 Identify Material KPI	A-061 Define Organisation's Strategy	A-071 Review Possible Solutions KPI
A-051 Establish Recruitment Strategy and Sources	A-053-5 Post Job/Position KPI	A-056 Prepare Job Offer KPI	A-058-5 Produce/Prepare Material KPI	A-062 Outsource Strategy KPI	A-072 Request Clarification on Budget, Terms, Timeframe KPI
A-051-5 Develop Benefits, Rewards and Recognition	A-054 Track Candidates	A-056-5 Receive Offer Acceptance/ Rejection KPI	A-059 Review Material and Select Relevant KPI	A-063 Keep in-House Strategy KPI	A-073 Identify Benefits KPI
A-052 Define Programme Operational Budget	A-054-5 Screen Candidates KPI	A-057 Re-deploy Employee KPI	A-059-5 Document Lessons Learned		A-074 Select Solution KPI
A-052-5 Develop Selection Criteria	A-055 Prepare Rejections KPI	A-057-5 Manage Employee Relocation			



A-080
Obtaining Appropriate Management Support and Funding

A-081
Obtain Support
KPI

A-082
Obtain Budget
KPI

A-083
Identify Costs
KPI

A-084
Make a Formal Business Case
KPI

A-085
Reach Senior Management
KPI

A-090
Prepare Work Plan

A-091
Define List of Activities
KPI

A-092
Define Milestones and Timeframe
KPI

A-093
Assign Resources and Budget against Each Activity
KPI

A-100
Develop Programme and Checklists of Tasks

A-101
Design the Programme
KPI

A-102
Revise Work Plan

A-103
Revise Allocated Resources
KPI

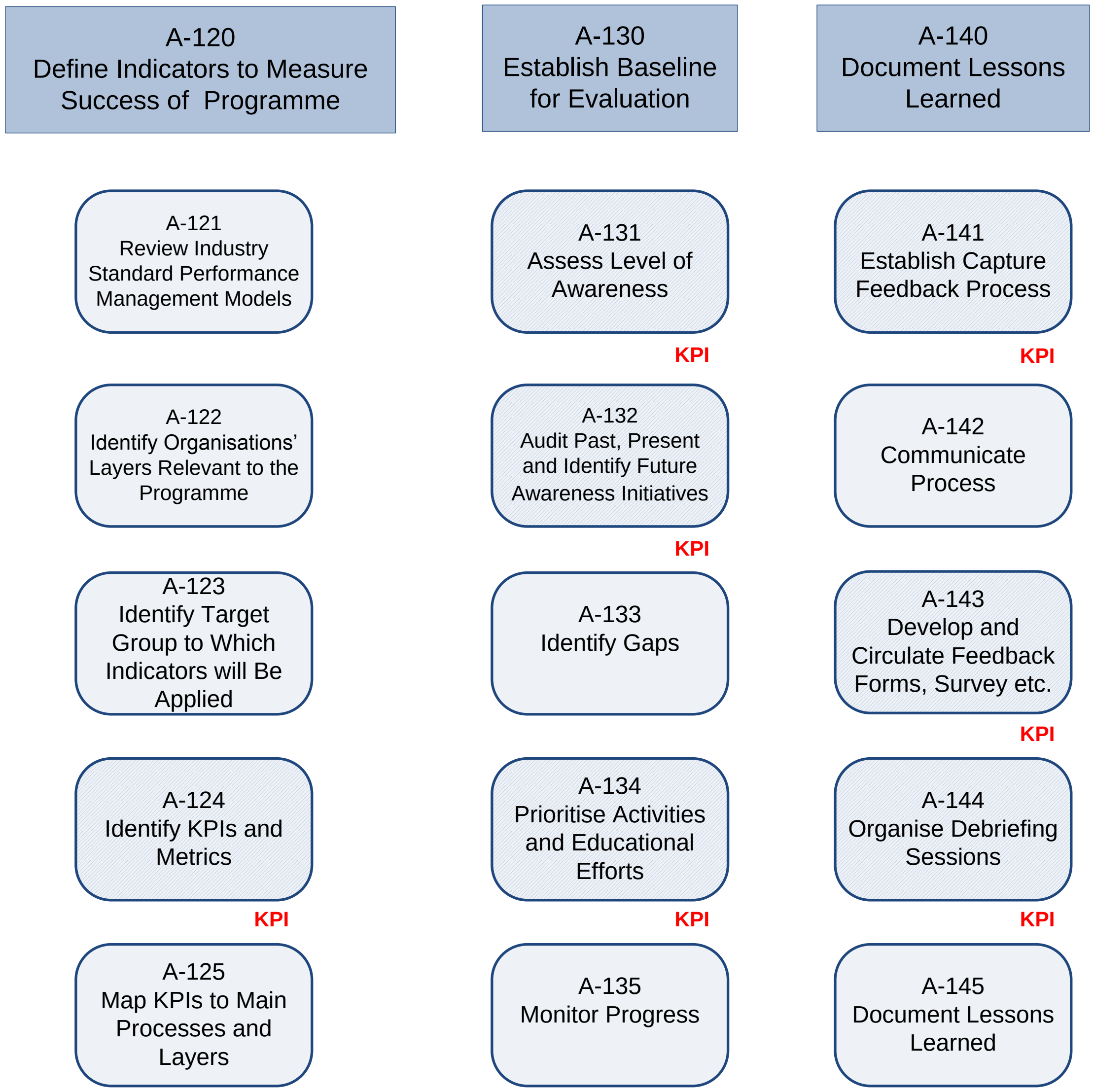
A-104
Create Checklist of Tasks
KPI

A-105
Perform Checklist of Tasks
KPI

A-110
Define Communications Concept

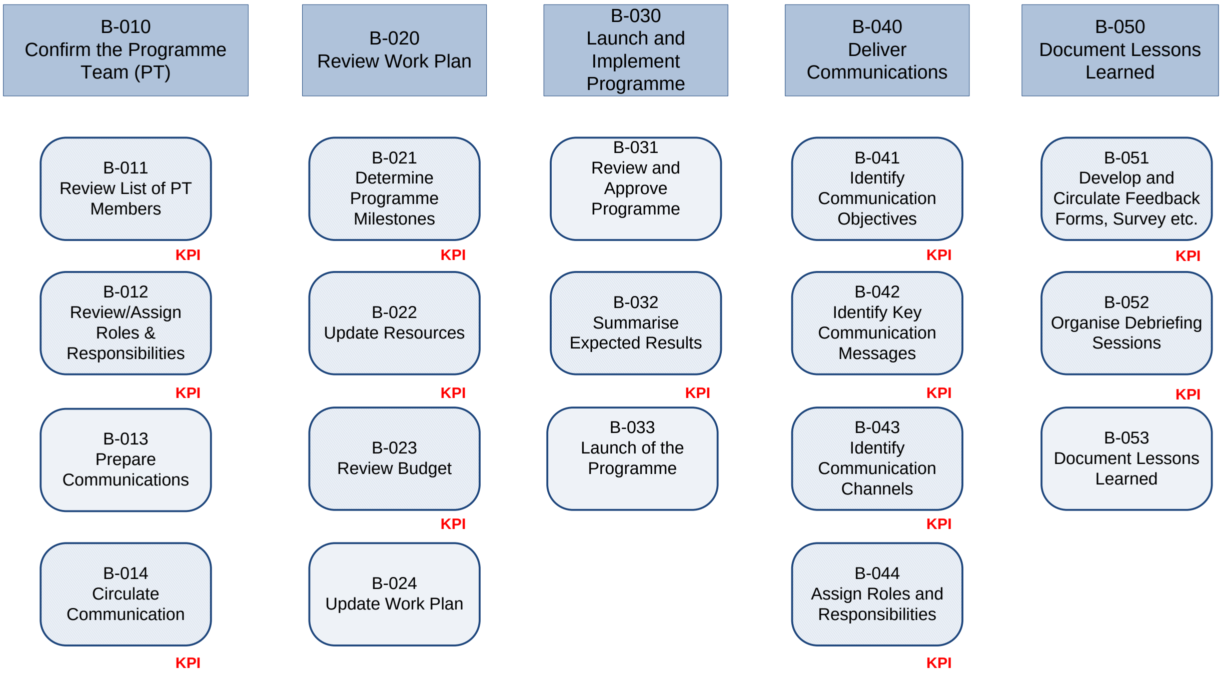
A-111
Develop Communication Plan
KPI

A-112
Select Channel of Communication
KPI



A-120 Define Indicators to Measure Success of Programme	A-130 Establish Baseline for Evaluation	A-140 Document Lessons Learned
A-121 Review Industry Standard Performance Management Models	A-131 Assess Level of Awareness KPI	A-141 Establish Capture Feedback Process KPI
A-122 Identify Organisations' Layers Relevant to the Programme	A-132 Audit Past, Present and Identify Future Awareness Initiatives KPI	A-142 Communicate Process
A-123 Identify Target Group to Which Indicators will Be Applied	A-133 Identify Gaps	A-143 Develop and Circulate Feedback Forms, Survey etc. KPI
A-124 Identify KPIs and Metrics KPI	A-134 Prioritise Activities and Educational Efforts KPI	A-144 Organise Debriefing Sessions KPI
A-125 Map KPIs to Main Processes and Layers	A-135 Monitor Progress	A-145 Document Lessons Learned

Appendix XIV — Execute and manage



B-010
Confirm the Programme Team (PT)

B-011
Review List of PT Members
KPI

B-012
Review/Assign Roles & Responsibilities
KPI

B-013
Prepare Communications

B-014
Circulate Communication
KPI

B-020
Review Work Plan

B-021
Determine Programme Milestones
KPI

B-022
Update Resources
KPI

B-023
Review Budget
KPI

B-024
Update Work Plan

B-030
Launch and Implement Programme

B-031
Review and Approve Programme

B-032
Summarise Expected Results
KPI

B-033
Launch of the Programme

B-040
Deliver Communications

B-041
Identify Communication Objectives
KPI

B-042
Identify Key Communication Messages
KPI

B-043
Identify Communication Channels
KPI

B-044
Assign Roles and Responsibilities
KPI

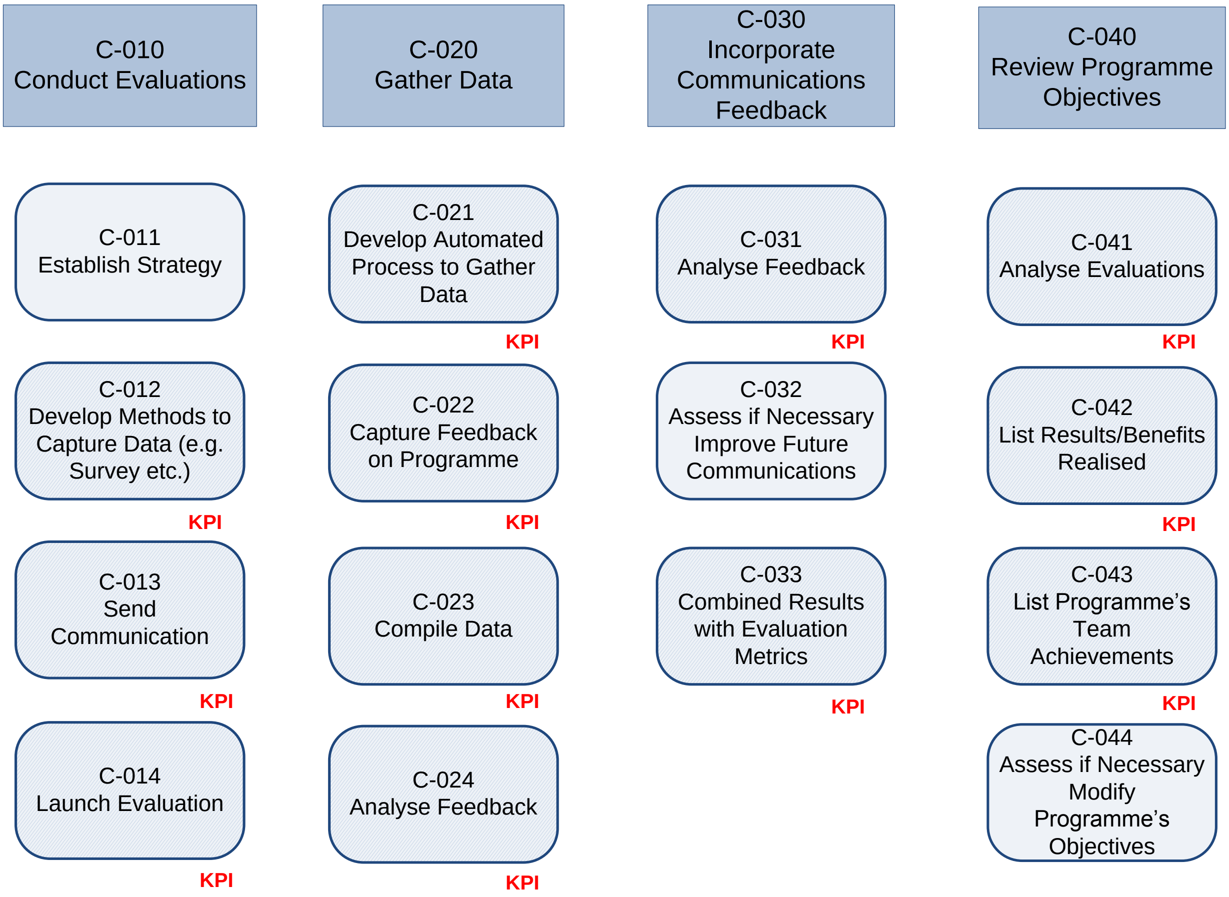
B-050
Document Lessons Learned

B-051
Develop and Circulate Feedback Forms, Survey etc.
KPI

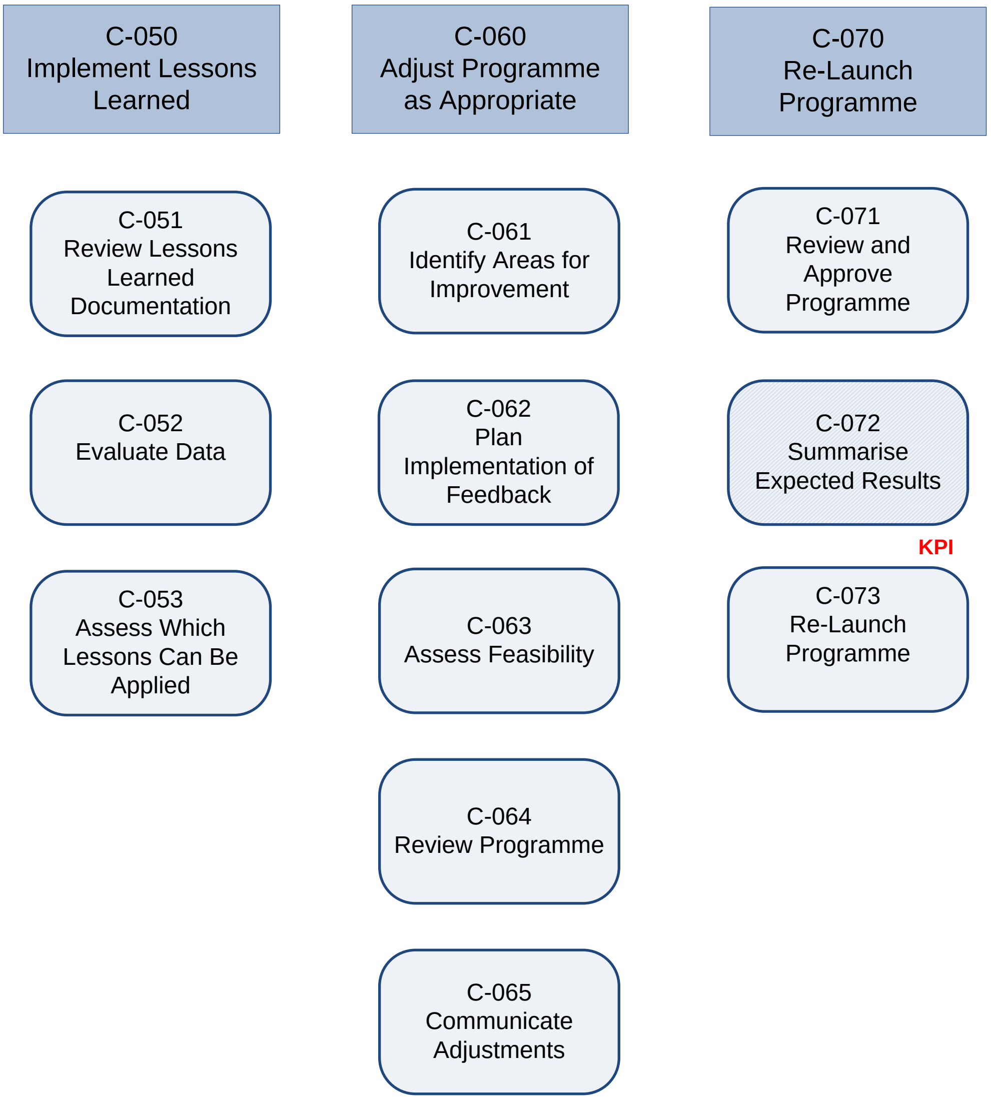
B-052
Organise Debriefing Sessions
KPI

B-053
Document Lessons Learned

Appendix XV — Evaluate and adjust



C-010 Conduct Evaluations	C-020 Gather Data	C-030 Incorporate Communications Feedback	C-040 Review Programme Objectives
C-011 Establish Strategy	C-021 Develop Automated Process to Gather Data KPI	C-031 Analyse Feedback KPI	C-041 Analyse Evaluations KPI
C-012 Develop Methods to Capture Data (e.g. Survey etc.) KPI	C-022 Capture Feedback on Programme KPI	C-032 Assess if Necessary Improve Future Communications	C-042 List Results/Benefits Realised KPI
C-013 Send Communication KPI	C-023 Compile Data KPI	C-033 Combined Results with Evaluation Metrics KPI	C-043 List Programme's Team Achievements KPI
C-014 Launch Evaluation KPI	C-024 Analyse Feedback KPI		C-044 Assess if Necessary Modify Programme's Objectives



C-050
Implement Lessons Learned

C-051
Review Lessons Learned Documentation

C-052
Evaluate Data

C-053
Assess Which Lessons Can Be Applied

C-060
Adjust Programme as Appropriate

C-061
Identify Areas for Improvement

C-062
Plan Implementation of Feedback

C-063
Assess Feasibility

C-064
Review Programme

C-065
Communicate Adjustments

C-070
Re-Launch Programme

C-071
Review and Approve Programme

C-072
Summarise Expected Results

KPI

C-073
Re-Launch Programme

Index

The new users’ guide: How to raise information security awareness

ISBN-13 978-92-9204-006-2

doi: 10.2824/19110

Catalogue number: TP-30-10-582-EN-C

TP-30-10-582-EN-C

enisa
European Network
and Information
Security Agency

ISBN-13 978-92-9204-049-9

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu