Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of the
Environment, Transport, Energy and Communications DETEC

Federal Office of Civil Aviation FOCA

Security Culture

Guidance on the development and expansion of security culture and a possible awareness-raising campaign

Federal Office of Civil Aviation FOCA I Security Section SISE I 20.11.2020

Contents:

Glossary:

AVSEC	Aviation security
FOCA	Federal Office of Civil Aviation
DNA	Genetic information stored in the cell nucleus
ICAO	International Civil Aviation Organisation (United Nations civil aviation organisation)
OECD	Organisation for Economic Cooperation and Development
SeMS	Security Management System
SISE	FOCA Security Section

I Security culture – Basics

"Culture cannot just be bought in or imposed from above; it permeates all processes in an organisation. Often culture means dealing more with the HOW than with the WHAT."

Bernd Schmid, German economist

1. What "security culture" means

a. Introduction

The introductory quotation suggests that culture cannot be simply decreed, determined or purchased. Rather it follows a pattern of development and must be lived. In the following explanations, an attempt is made to present the basics and positively influence a broader understanding of the topic of "security culture".

How can corporate culture or security culture be (further) developed? In this context the following essential questions must be clarified:

- What is culture;
- How is it created; and
- How can we influence it.

The aim of this paper is on the one hand to create a basic understanding of the mechanisms which give rise to culture. On the other hand, it aims to indicate how an active, effective and sustainable security culture can be designed and implemented. It does not provide a ready-made training programme or pre-defined control elements. Rather, it is intended to encourage those responsible in the entities to individually and creatively design and implement the appropriate solutions themselves.

b. Understanding "culture"

In order to better understand the terms and contexts, a brief excursion into the basics of social and cultural science is helpful.

What is "culture"? The term "culture" is generally understood as the set of shared attitudes, values and methods of an institution or organisation. Semantically, the word "culture" stands for "*the habits, traditions, and beliefs of a country or group of people*[1]". Cultural knowledge is learned or acquired by the individual over time. The Latin origin of the word is also worth mentioning: *cultura* stands for "processing", "care" or "cultivation".

To a certain extent, "culture" is part of our individual inherited DNA. The more essential part, however, is learned over time. This happens from childhood on, generally when we interact with other people. In the course of our cognitive development, the individual builds his or her understanding and behaviour on acquired knowledge and experience.

[1] Cambridge Dictionary (Engl.)

It should be stated that individual elements are absorbed (internalised) by people differently. It is generally apparent that those elements which are emotionally related are internalised more deeply. The more emotions a picture or a scheme triggers, the deeper the internalisation and therefore the greater the stimulus to act.

The motivation to internalise something more deeply is controlled by the interest in something. Generally, interest is understood to be attachment or affinity to someone or something. The more someone is affected or touched, the greater the interest. Positive emotions[2] associated with the object of interest additionally promote the bond.

It follows that a new or altered security culture cannot be simply prescribed or instructed. Rather, first and foremost it must be put into practice and taught. By analogy with the Latin origin of the term culture, we cultivate something in spirit and accompany its growth, as in agriculture. It is also important to note that those elements which affect the emotional level of an individual are accepted more readily, so the chances of a positive development are increased.

c. Transfer of “safety culture” elements into "security culture"

The current definition of the International Civil Aviation Organisation (ICAO) is based in principle directly on the scientific definition of “culture”. It also states that it is addressed to each entity and all personnel within an organisation (“security should be everyone's responsibility”) and lists the following favourable elements[3] :

- Recognizing that effective security is critical to business success;
- Establishing an appreciation of positive security practices among employees;
- Aligning security to core business goals; and
- Articulating security as a core value rather than as an obligation or burdensome expense.

The concept of security culture is understood as a behavioural characteristic of a group or an organisation, in relation to dealing with security issues. The related term “safety culture” became widely known in connection with the Chernobyl reactor disaster in 1986.

The Organisation for Economic Co-operation and Development (OECD) stated in this context[4]:

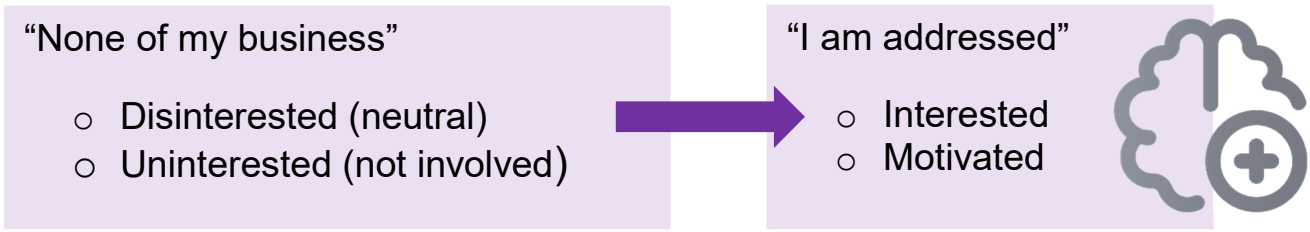
The reactor accident in Chernobyl has shown that *“… when the basic safety values, norms and attitudes of an entire organisation are weak or missing, then one can have procedures ignored operating limits exceeded and safety systems bypassed, no matter how well they have been designed and built (…) Safety culture must permeate all levels of an operating organisation*
(…) At the top of the corporation, management commitment to safety has a profound influence on the safety culture of the entire organisation, and senior management must establish a set of values emphasizing safety and quality, making it clear that workers should not have a conflict in their daily tasks between safety and electrical production goals. The employees will keenly watch whether the senior management’s actions match their words in this regard.”

[2] Examples of positive emotions: satisfaction, solidarity (empathy), pride, caring, enjoyment and gratitude
[3] ICAO toolkit on enhancing security culture, November 2018
[4] OECD, The Role of the Nuclear Regulator in Promoting and Evaluating Safety Culture, 1999

Another example which indicates related or similar systemic weaknesses is the sinking of the Costa Concordia (2012). The ship was excellently equipped with radar systems, echo sounders, satellite navigation and a digital maritime chart system. In the case of the incident, however, central requirements such as reducing speed and maintaining safe distances were neglected by the ship's command. In retrospect it was an aggravating factor that the specified emergency exercises had not been carried out for all passengers. It was also shocking that the majority of the ship's command, including the captain, left the ship after the accident at a time when several hundred people were still on board. The criminal investigation after the accident also showed that such dangerous manoeuvres (very close passing of islands) were part of the common practice of the cruise line company.

The key finding is that even the best equipment and sophisticated processes cannot prevent an incident and can dramatically increase its impact if the persons responsible for implementation deviate from the specifications and standards or act recklessly.

In general it can be said that for a culture change to succeed it is crucial that the various participants develop an active interest in the subject. The following principle applies: security concerns everyone. To this end the individual attitude to the topic which often prevails must be changed:



d) “Just culture” and active reporting

Just culture is a concept which sees the causes of errors which have been made more in a defective process culture or organisational culture and less in individual persons. After an incident people ask what went wrong and do not primarily look for the person at fault (“What went wrong?” versus “Who is responsible for the incident?”)[5]

The concept is to learn from mistakes and to create a climate in which people report their mistakes independently and frankly so that lessons can be learned for the commonality and so that mistakes can be avoided in the future. The concept is established in the field of technical safety in many areas, especially in aviation.

Elements of the concept are also possible in the field of security. It is desirable, for example, to make available an appropriate reporting channel for observations of improper behaviour and suspicious situations. It would be useful to examine the extent to which a reporting system for one's own mistakes would be useful and could be integrated.

[5] Maurizio Catino, “A review of Literature: Individual Blame vs. Organizational Function Logics in Accident Analysis.” Journal of Contingencies and Crisis Management (03. 2018)

Example of self-reporting:

"*I had the task of supervising a number of people in the sensitive security area (monitoring regulation). During this task I was also instructed to pack a flyer for mailing. After completing the additional task I became aware that I had no longer been performing the monitoring task."*

(The example is based on an actual situation; observation by AVSEC inspector).

In a company with an open and positive work culture, it can be assumed that the employee concerned, after realising his own improper behaviour, will address this if a similar situation arises again ("… I cannot perform both tasks at the same time…"). However, if such a culture is not established and if the employee shies away from a possible confrontation or even experiences rejection, disregard or even disadvantages due to the internal reference, it is highly probable that in the future no positive action or report will ensue.

2. How can an active and effective security culture be achieved?

A coordinated approach is necessary to establish an effective and sustainable security culture. This must be led from the top down and must address all levels of a company or organisation. The following elements are central to this:

a. Foundation

A good foundation secures or anchors a superordinate structure and should prevent unintentional fluctuation or distortions of the same. What the building industry does also applies to security culture. The foundation must be authoritative and solid so that the structure can develop in a stable way.

From the outset there should be a declaration of intent by the leadership of an entity or organisation. This can be recorded and communicated in the form of a binding policy. Important: security culture must be a fundamental value of an entity or organisation.

A practical example of how the leadership of an entity or organisation can influence general understanding and behaviour can be found at a Swiss airport:
After the introduction of 100% security checks for staff, there was regularly friction at the one security checkpoint with employees of a particular company. Interventions with the company management did not bring about understanding of, or improvement in, the situation. Only after a change of management in the company following its sale did the problems end. The new company management from Great Britain was used to a high level of security and demonstrated their full support. This quickly rubbed off on the employees.

In a second step, generic claims such as, for example "It [FOCA] promotes open reporting (…)"[6] are to be used to formulate concrete and realistic goals as to how this is to be achieved. The fundamental path to the goal can be implemented in a so-called Security Management System (SeMS) or a comparable concept.

[6] Security policy of the Federal Office of Civil Aviation, Measures

A SeMS or a comparable structure should anchor security culture and focus on performance, results and impact. It should not only reflect relevant processes but in particular underline a commitment on the part of the management. The involvement of the employees of an entity or organisation at all levels of the development and implementation of an SeMS is essential to secure understanding, commitment and ultimately the success of the system.

b. Implementation

Successful implementation begins with the members of the various management levels of an entity or organisation putting values and norms into practice. Exemplary conduct, seriousness and credibility are core. Members of the management team should promote the importance of security culture and effective preventive measures, adhere strictly to the guidelines themselves and maintain an open dialogue with management colleagues and employees.

Implementation should begin with more detailed induction training on the subject in which the background, basic values and objectives are ideally transmitted with reference to practical application. This is how an understanding of the meaningfulness of a measure is gained. Thanks to positive learning content (e.g. practical and concrete rather than abstract; encouraging rather than deterrent), interest and an emotional bond should also be created. This contributes to a deeper internalisation of the elements of security culture.

Furthermore, it is important to create suitable instruments for implementation. These may include, among other things, a reporting and analysis tool as well as information material. An instrument for feedback from employees supports the credibility and effectiveness of the system.

c. Sustainability

In order to achieve sustainable implementation, it must be regularly reviewed. To do this, achievement of the defined goals and evaluation of the results of measures or activities are necessary.

A good security culture can be demonstrated, for example, as follows:

- Awareness and vigilance concerning security risks among all employees;
- Challenging by employees of persons who do not conform; and
- Active use of a reporting tool to report security incidents and/or observations.

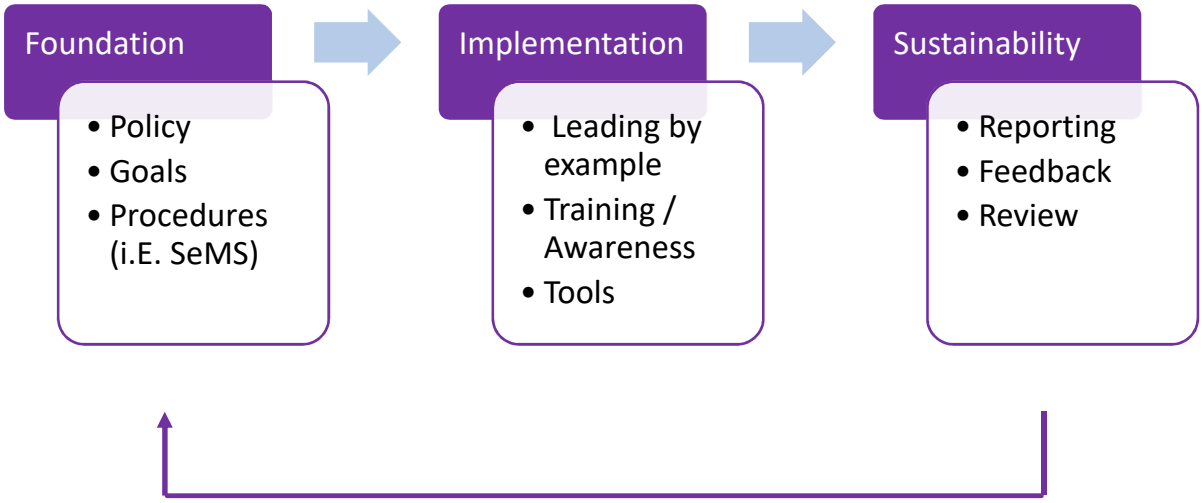
These exemplary elements can be measured: general awareness can, for example, be addressed and deepened within the framework of periodic refresher courses (continuous learning). The state of knowledge can also be determined through questions. Reports can be measured by the number and the quality of their content.

It is crucial that data is not only collected but that the results are returned to employees after analysis. Someone who receives feedback feels that they are being taken seriously and supported. If necessary, the analyses should also result in concrete measures.

Security culture should be addressed regularly. A variety of platforms are conceivable: a 'security day', flyers, electronic information, posters, etc. These actions should be structured and work with objectives (e.g. what do I want to achieve) which in turn enable analysis of the effectiveness of the measure.

Finally, the defined elements of the security culture, such as the goals or measurement parameters, should be periodically reviewed and amended if necessary.

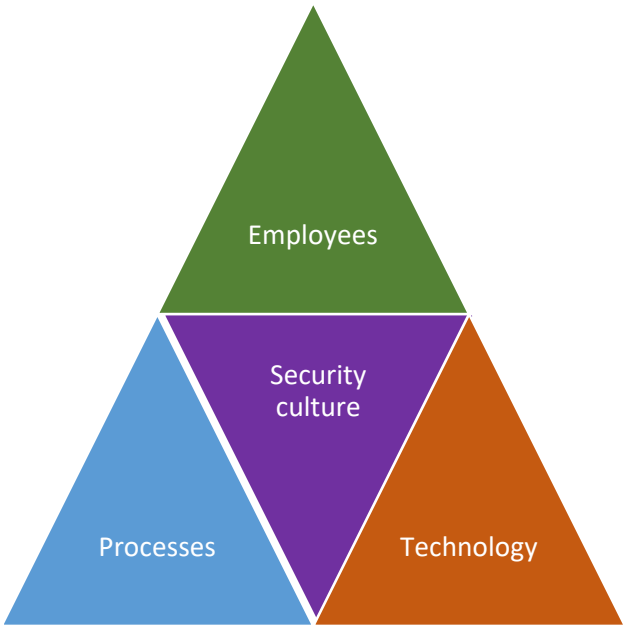
In simplified form, the process can be represented in 3 steps (foundation, implementation and sustainability):



3. Conclusions - short and sweet

- (Security) culture is acquired/learned over time;
- Characteristics/elements of a culture are accepted by people depending on their interest or emotional bond;
- Policy and application/commitment are necessary;
- Leading by example is the key to success;
- Systematic development and implementation are crucial;
- Motivational training, adapted to different levels, is necessary;
- Recording and feedback are essential elements of the system; and
- Security culture concerns everyone.

An actively lived security culture is the crucial link between the key elements of an entity or organisation. It is intended to ensure that the prescribed security measures and goals are implemented by all employees on a continuous basis and in accordance with the rules. In addition, vigilance and personal responsibility will be promoted.



4. Awareness-raising campaign

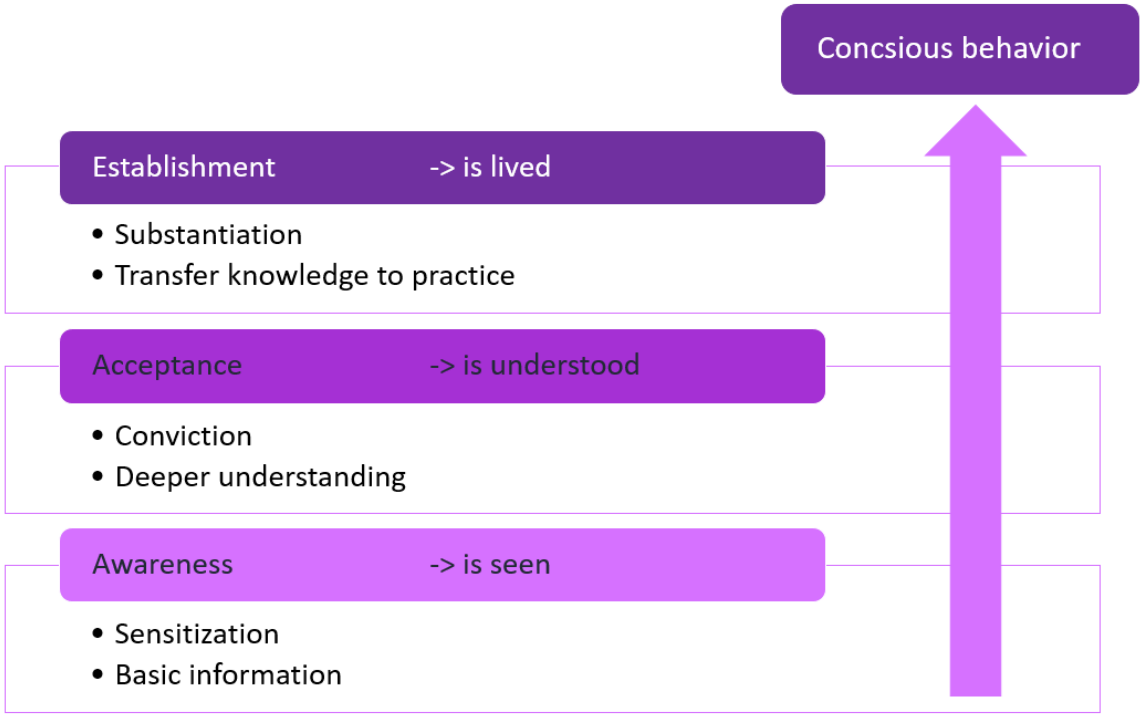
An awareness-raising campaign is one possible means of ensuring security culture or elements of it are known or borne in mind.

For the campaign to be effective, it should be designed specifically, efficiently and in a targeted manner. The campaign must not only communicate threats and risks but also ensure that the persons addressed understand the contents and are motivated to implement the desired objectives.

As stated above, change is only brought about over time. A campaign must therefore aim to cover a longer time scale and should include initial and follow-on components (impetus - basic knowledge - repetition - advanced knowledge).

From the literature, the following “success factors” for campaigns can be identified:

- Orientated to the target group/appropriate to the different levels
- Understanding/acceptance
- Time span (continuous training)
- Building on established guidelines and regulations



Three steps model of developing conscious behaviour over time.

The method of communication is also a relevant factor. Fear-inducing or intimidating communication is often counter-productive, since this is more likely to instil fear in those addressed rather than motivate them. Risks should ideally be presented using internal examples and the information should generally be simple and brief.

The campaign should be supported by suitable accompanying measures. Among other things these may include posters and flyers, e-mailings or special events such as themed or focus meetings[7].

It is also helpful if an emotional bond to the campaign is made. This can be supported by “branding”, for example. Integrating an impressive “brand name” and/or a logo creates positive emotions, motivation and credibility.

[7] Security days at Zurich Airport in 2019: under the banner of “secure together", Zurich Airport AG and various partner companies provided information on the subject of security. An information meeting for all airport employees with information stands, refreshments and a competition.

II Security culture and awareness campaign - Guidance

The following pages are intended to indicate simply, with keywords, the steps necessary for development, publicity and training. As a guide, they are divided into four sections:

Start - basis and foundation;
Preparatory work and preparation of the general conditions

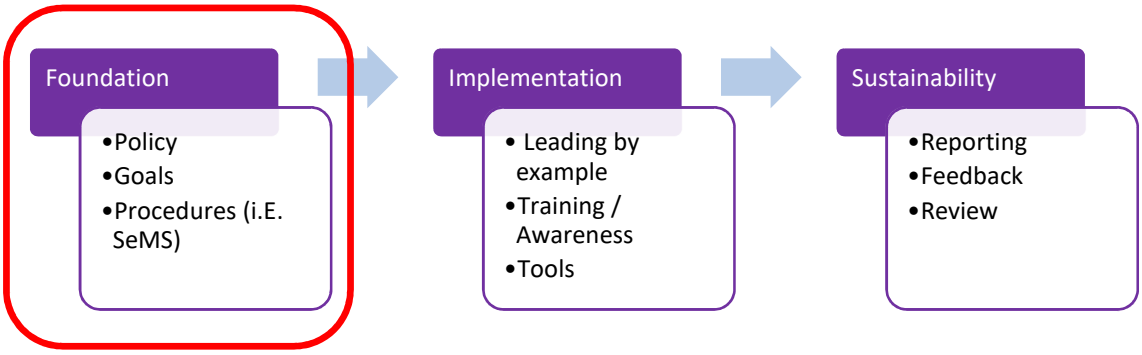
Set-up - input, elaboration;
Creation of processes and documentation

Implementation - rollout and dissemination;
Communication, training and initiation of implementation

Note, observe:
Key elements or issues to observe

5. One, two, three -> Go! Security Culture

We proceed from the well-known scheme (foundation - implementation - sustainability) and break this down into the three individual phases:

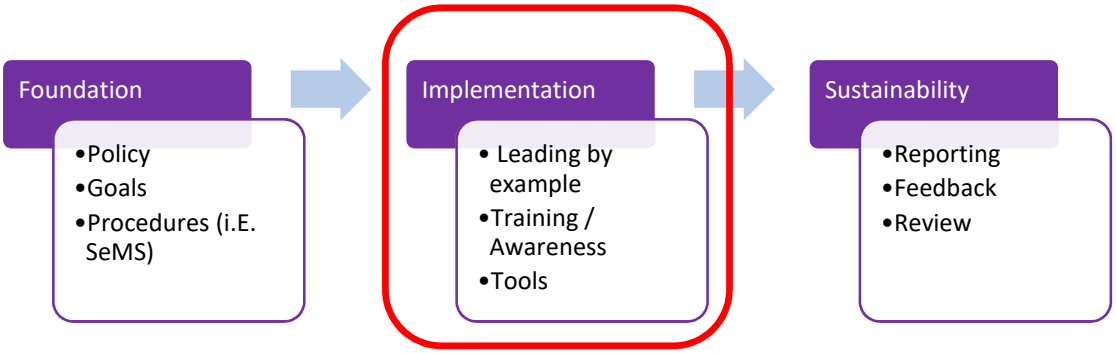


- Declaration of intent concerning security policy and security culture by the management of the entity
- Project initiation and initial communication
- Determine project participants, responsibilities and time scale
- Analysis of the current status in the context of the corporate culture

- Development and anchoring of a mandatory security policy
- Definition of objectives and measurement parameters
  - What do we want to achieve (goals)?
  - How can this be evaluated/measured?
- Review of the elements of a control system, e.g. Security Management Systems (SeMS); which ones should/can be integrated?
- Creation of processes and documentation

- Detailed communication to employees, including policy
- Provide induction training to all employees
- Set up a reporting tool including the creation of reporting and evaluation processes

- A declaration of intent by the management of the entity is key
- Regular and clear information which is appropriate to the various stages
- Define challenging but realistic goals
- Branding: give the project a handy, catchy name, a symbol - > emotional connection

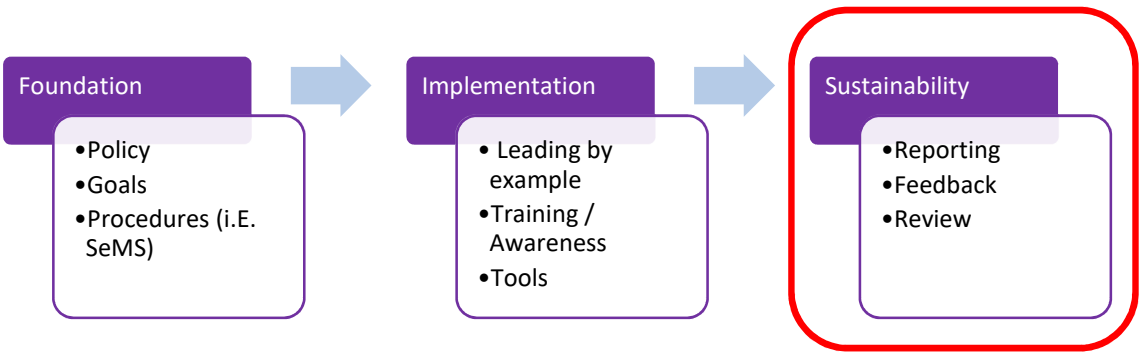


- Living the policy by the management of the entity/organization
- Active support of the implementation phase
- Processes approved/anchored (e.g. in a SeMS)

- Rollout and induction training of the employees
  - Appropriate stages
  - Practical
  - Background, basic values, convey goals
- Launch the reporting tool
- Launch the awareness-raising campaign
  - Alongside the basic training
  - Guarantees visibility of the project
  - Memorability

- Rollout communication
- Initiate feedback and analysis from the reporting tool
- Achieve visibility, e.g. by means of e-mail, flyers, posters, events

- Exemplary function is critical for success!
- Effective promotion of the project by appropriate measures, such as an employee event
- Positive communication and visibility promote emotional connection and acceptance



- Ensure identification with the principles and goals even if there are changes in the management team (corporate principle, anchoring)
- Define options for action in the event of positive developments (e.g. fewer security-relevant incidents) and negative developments

- Regular review and analysis of the data from the reporting tool
  - Analysis of the data
  - Derive measures, if necessary
  - Initiate adaptation of goals, if necessary
- Periodic review of policy, goals, and measurement parameters
- Periodic review of the tools, such as SeMS and reporting tool
  - Are we getting reports?
  - What is the quality of these?
  - Are these reaching the relevant locations?
  - Does the feedback loop work?

- Regular communication
- Feedback on evaluation of the data from the reporting tool or individual reports (individually, or as a whole, if applicable)
- Plan periodic refresher courses

- Ensure ongoing support from management
- Feedback is crucial for motivation
- Review is the basis for advancement
- Maintain visibility and memorability

6. One, two, three -> Go! Awareness-raising campaign

- Based on established standards (e.g. security policy)
- Define target group(s) and resources
- Define content and goals of the campaign
- Plan timeline (rollout, sending of e-mails, flyer/poster campaign, analysis, etc.)

- Design campaign tools (flyers, posters, logo, etc.)
- Create analysis tools
  - E.g. a short questionnaire
  - Measure the change in the number of reports after the beginning of the campaign, etc.
- Green light from the management of the entity

- Clear and purposeful communication
- Positive message
- Create and implement corresponding awareness training
  - Short, precise, consistent

- Timescale: Impact - basic knowledge - repetition - development
- Individual, clear, motivating
- Catchy slogan and/or logo (branding)
- Exploit bandwidth of information channels:
  - E-mail
  - Flyers
  - Poster
  - Event
  - …

7. One, two, three -> Go! Induction training

- Define target group (basically training in security culture for all members of the entity/organization)
- Define training course goals and scope of training
- Select form of instruction (e.g. face-to-face instruction, e-learning etc.)
- Training should be launched/monitored by a member of the management - > demonstrates importance/seriousness

- Produce training documents; these should ideally address the following topics:
  - Background/basis of security culture
  - Security policy of the entity/organization and tools (e.g. SeMS)
  - Insider threat and radicalization
  - Practical examples and goals
- If possible, training should contain interactive and creative elements; this may include:
  - Group work; e.g.
    - What is understood by “security culture”
    - Where we [the entity] are strong; where can we become better?
  - Quiz
  - Design a campaign logo or slogan
- Provide appropriate progress monitoring (not a formal test)

- Provide obligatory training courses for all members of the target group
- Obtain feedback, take up any ideas from training/feedback, evaluate progress monitoring - > if necessary, integrate into review process (sustainability)
- Reporting, e.g. in the company magazine
- Plan and implement refresher training

- Adopt a positive approach to learning content
- Creativity and interaction generate excitement and bonding
- Clear training goals create understanding and simplify progress monitoring
- Communication: “Do good and talk about it”