THE NATIONAL CYBERSECURITY AWARENESS RAISING GUIDE

2021 - 2025

BEST PRACTICE TO CONDUCT AN AWARENESS RAISING ON CYBERSECURITY NATIONWIDE

Partners

The Gambia National Commission For UNESCO(NATCOM)

www.moici.gov.gm | info@moici.gov.gm

Table of Contents

INTRODUCTION

The Ministry of Information and Communication Infrastructure (MOICI) formulated a project proposal in 2019 to raise awareness on Cybersecurity and Cybercrime, nationwide. MOICI, through The Gambia National Commission for UNESCO (NATCOM) sought funding from the United Nations Educational, Scientific and Cultural Organization (UNESCO) to implement the project.

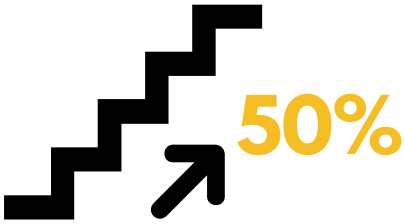
After securing funding from UNESCO in 2021, MOICI in collaboration with relevant stakeholders proceeded with the implementation. The project consists of 7 activities as follows:

- Activity 1: Develop a National Cybersecurity Awareness Guide.
- Activity 2: Validate the Cybersecurity Awareness Guide
- Activity 3: Seminar on Awareness Raising Cybersecurity and Cybercrime for Law Enforcement Agencies
- Activity 4: National Cybersecurity Awareness Raising for Students/Youth
- Activity 5: Cybersecurity Awareness raising campaign for parliamentarians, Judiciary (seminar), and the general public (through the media).
- Activity 6: National Cybersecurity Day Commemoration.
- Activity 7: Monitoring and Evaluation

This Awareness Raising Guide which is a result of Activity 1 of the project, is to advise and assist entities with better understanding of awareness raising to help propagate a responsive use of Information and Communication Technologies, with a secured resilient cyberspace for The Gambia.

OBJECTIVES OF THE GUIDE

1. Increase the level of awareness by 50% on Cybersecurity and Cybercrime issues in the Gambia by 2025.



2. Ensure a secured and resilient cyberspace for The Gambia by 2025.

SCOPE

- This Guide will serve as a reference document for entities to use during planning, organizing or implementing Cybersecurity and Cybercrime awareness raising initiatives.
- The Guide is not legally binding however; it serves as best practices for entities.
- To ensure that best practices are followed for the development and design of Cybersecurity awareness programs; which would increase the level of awareness

IDENTIFICATION OF A CHAMPION

Identifying a Champion is an essential first step in ensuring that the agenda of the initiative is adopted, prioritized and fully supported at all levels. In this regard, it is imperative to highlight some of the qualities of a champion. This will help in the identification of the right people.

What constitutes a champion?

- Someone/entity who has authority
- Someone/entity who can influence decision-making
- Someone or entity who is pragmatic and action-oriented
- Someone/entity who has resources
- Someone/entity with the ability to adapt to change.
- Someone/entity who is a winner
- Someone/entity who is passionate about the cause ready to commit resources.
- Someone/entity who is a good Listener

How to engage a Champion?

- Consistency in the initiative
- Ensure involvement of Champion in relevant activities.
- Activity Reporting or sharing information
- Maintain confidentiality, professionalism and trust.

How to bring a champion on board?

- Planning the whole process. e.g. approach, clarity of message, viability of initiative,
- Ensure access to the Champion
- Apply persuasive approaches when needed.
- Promote Agenda of the initiative with a brief and precise presentation to the Champion.
- Being confident and eloquent when making your case.
- Use all means (that are legal) necessary to reach the Champion

PLANNING

Planning is so important in any initiative and must be done at the very beginning. It ensure error are minimized and a sequence of flow of activities takes place with an informed budget. There are several factors to consider when planning and they include:

1 Understating your environment.

There are various factors that require consideration. These include roles and responsibilities, external stakeholders, existing policies, legal and regulatory frameworks, cybersecurity culture, business case, timelines, etc.

2 Constitute a Team

A team must be assembled to initiate the planning of Cybersecurity awareness raising initiative. The mandate of the team should include planning, organizing the initiative and executing the plan of activities.

3 Adopt a change management Approach

To bridge the gap between the issues and human responses to the issues, the use of a change management approach to an awareness initiative is vital.

4 Explore Solutions

While exploring solutions, a key questions would be whether the awareness program will be kept in-house or be outsourced. Over time, the use of outsourcing as a strategic decision has increased. Organizations and institutions should evaluate areas of operation where do well against those that can be effectively conducted by external partners.

5 Finalize the solutions to adopt and procedure to follow

After exploring and weighing your choices, the solution and procedure need to be finalized.

6 Develop a Work Plan

Formulate a work plan incorporating all planned activities with attainable timelines.

PLANNING

1 Set Goals and Objectives

Define what the initiative is aiming to achieve and the end. The results. Set SMART objectives to help in achieving the Goals.

2 Describe your Target Audience

At this stage you need to understand your target audience. Categorize them early and later elaborate before implementation.

Formulate the fully blown project proposal with a detailed Plan of Action. Also develop a Checklists to activities or tasks.

3 Develop a Communication Plan as an Annex to the proposal.

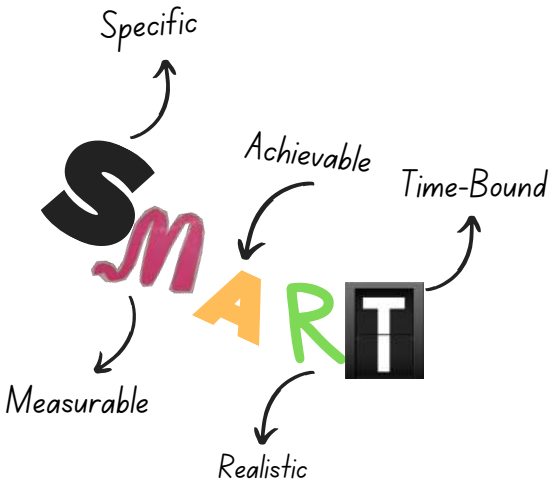
The Plan should include when to communicate to each and every stakeholder and roles and responsibilities of team members in executing that task.

4 Set up Indicators to measure the success of the initiative.

Ensure a Baseline is established for Evaluations.

The SMART Approach should be adopted to ensure objectives are met and impact is measurable. The acronym is known to be used for best practice.

"S" means "Specific" – This involves the subject matter of the objective of the initiative. "M" means "Measurable" is the objective of the initiative. "A" means Achievable". "R" means "Realistic" and "T" means "Time-bound."

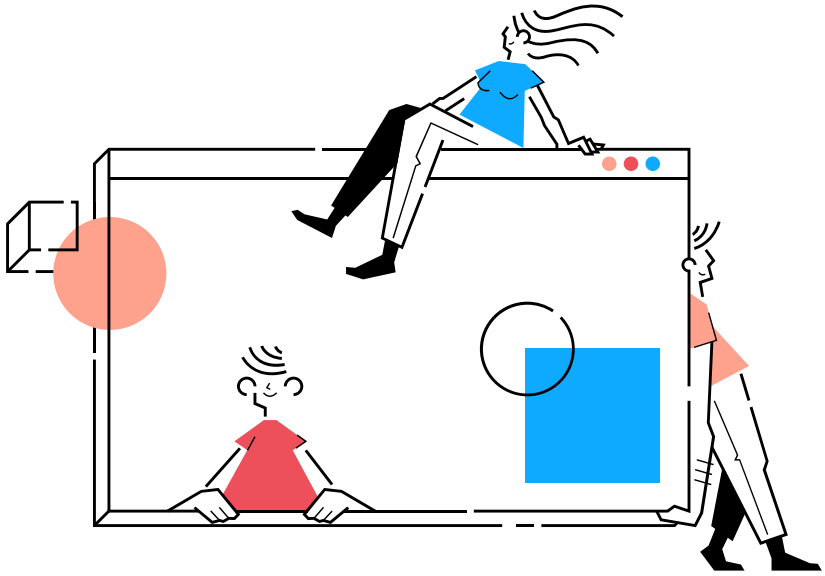


DESIGN

When designing, it is important to consider whether it supports the business needs of the organization, also whether it complements the organizational culture and IT infrastructure.

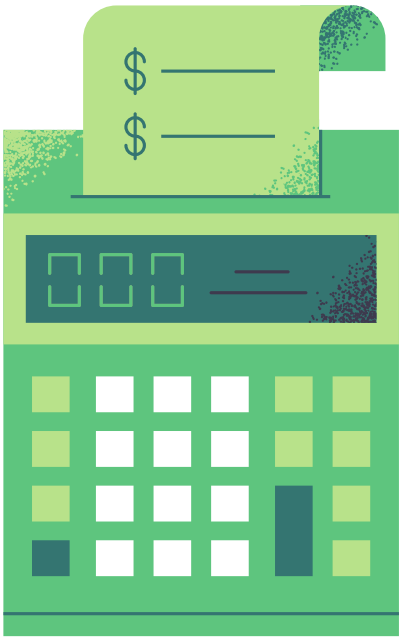
1. Where applicable the logical or physical design (s) needs to prepared and elaborate.

2. A flowchart need to prepare depicting alternative routes to achieve the objective of the initiative.



BUDGETING

A proper budget is the life blood of your initiatives. You need it to acquire funds. Without it, it would be difficult to convince donors or even internal funding authorities to provide you funds. Budget require detailing. The following is best practice guidelines:



- Budget at the beginning of every initiative. Understanding funding, and available resources at the beginning of any 1.awareness program/campaign is paramount.
- Obtaining appropriate support from management and funding, if available.
- Scoping the program and determining how many activities and at what level it would be offered. There are challenges in budgeting but important to ensure the scope and success of the initiative.

GETTING APPROVAL

Without formal approval initiates will not go far. In fact it may contradict or breach organizational guidelines and procedures. For cybersecurity awareness initiatives to be successful, formal approval would be required.

Why is approval needed?

- To obtain formal recognition for the initiative.
- To ensure organizational buy-in and commitment.
- To ensure trust when engaging stakeholders.
- To ensure smooth and effective implementation of the initiative.

How to seek approval?

- Initiative must be formally written to management seeking approval.
- The purpose should be clearly communicated, convincing and justifiable.

The Plan and Budget should be communicated in a transparent manner.
Ensure a professional approach.

When to seek approval?

From the time of project concept
When creating a timeframe to achieve the goal. At the planning stage – this includes preparing terms of references, cost benefit justification.

- When preparing budgets
- During implementation at every other stage.
- Before Monitoring and Evaluation (M&E).
- When submitting the final report.

Where to seek approval?

- Management
- Executive body
- Authorities
- Boards/Councils
- Committee/Commission

RESOURCE MOBILIZATION

Before identifying or mobilizing resources for the initiative, it is important to first determine what is needed in terms of personnel and materials. An ideal approach is to begin looking within the organization for the right resources. Personnel within Information Technology (IT), Human Resource (HR), Communication, Training and Development units would probably have the requisite experience that is suitable for an awareness raising program.

What constitutes a resource?

It is equally important to understand what constitutes a resource. Resources are divided into two components namely;

- Material Resource: This includes funds, logistics, equipment etc.
- Human Resource: This includes experts, relevant personnel that are **useful for the initiative etc.**

When to seek resources?

It is also important to comprehend the right time to seek for resources. The following steps need to be taken into account;

- Resources should be sought after planning and budgeting i.e on condition of an approved budget.
- Resources should be sought before the implementation of the initiative.

Where to get resources?

Resources can be acquired from various entities. Some are internal and others external. They are categorized as follows;

- For material resources, we can acquire resources from organizational, external grants, donations, etc.
- For human resources we can receive support from internal or external experts, consultants, resource persons, advisers, panelists, rapporteurs, etc.

How to seek resources?

Coordination is of paramount importance. In doing so, the following steps should be observed:

- Writing bankable project proposals.
- Identifying network and communication channels to reach donors.
- Projects that are submitted to donors must be justified, achievable, realistic, and time-bound.
- Projects must be properly pitched or presented.
- Professionalism, commitment and determination must be shown.
- Vivacious, charismatic, lobbyists need to be identified to lead the presentation of project concepts to donors.

IDENTIFICATION AND INVOLVEMENT OF RELEVANT STAKEHOLDERS

Before identifying and involving stakeholders, it is crucial to consider the relevancy of the stakeholders' participation. Critical questions that need to be addressed are as follows:

What is a Stakeholder?

A stakeholder is a person or organization that has a legitimate interest in a specific project/initiative or policy decision and whose support is required in order for an institution to be successful.

Who are the relevant Stakeholders?

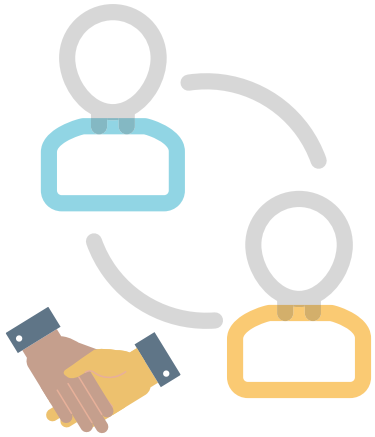
The relevant stakeholders can be identified from various entities with common interest and support for the initiative. They are categorized as follows;

1. The Public Sector
2. The Private Sector
3. The Civil Society Sector, NGOs, Community Based Organizations (CBOs)
4. The Academia
5. The Media
6. Religious Groups
7. Donors
8. Bi-Lateral and multilateral

How to involve them?

It is important to ensure stakeholder involvement or consultation at every stage of the initiative. This can be accomplished through:

1. Establishing effective communication channels via appropriate authorities. These channels include:
   - Written(Physical or electronic formats)
   - Verbal (for complimentary follow-ups)
2. Inviting them to participate in activities, such as launching and concluding programs.
3. Inviting them during evaluations.



IDENTIFICATION OF TOPICS OF DISCUSSION

Prior to identification of topics of discussion, it is important to consider the following:

1. Relevancy of topics as per current time e.g., prevailing issues that affect the society, the context of the country, etc.

2. Topics should be informed by Reports of preceding year (s); Especially cybercrime reports.

IDENTIFICATION OF TARGET AUDIENCE

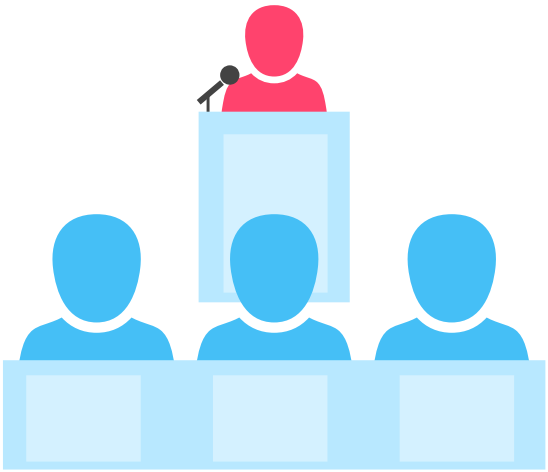
1. **Level 1 – General Users**
   - Users without formal ICT education

2. Level 2 – General Users – IT Literates
   - Users with formal ICT education

3. **Level 3 – IT Technicians**
   - Users with technical background in administering computer systems, applications or networks.
   - User with a relative practical understanding of the theoretical principle of a computer system and application.

4. **Level 4 – Lawmakers and Law Enforcers**
   - Parliamentarians who enact laws
   - Security institutions and other sectors responsible for enforcing the laws such Police, Judiciary (responsible of interpretation of Laws and adjudication)
   - People responsible for formulation of laws e.g. Draftsperson.

5. **Level 5 – Policymakers and the Executive**
   - Government, public institutions and other relevant stakeholders.



IDENTIFICATION OF TOOLS/RESOURCES TO USE

Tools or resources are essential and critical enablers in ensuring the successful implementation of a cybersecurity awareness raising initiative. To start with, you must identify the tools that are useful for the initiative. The following questions need to be addressed:

How to identify tools/resources to use?

- The usefulness of the tool/resource must be assessed first and must be up-to-date as per the initiative.
- Availability of the tool/resource must be explored
- Is the tool/resource cost-effective?
- Effectiveness of the tool/resource must be assessed.

When to identify tools/resources?

The timing of identifying tools and resources is crucial because failure to acquire them on time may delay or negatively affect the implementation of the initiative. Therefore the timeframe should be informed during:

- The planning stage
- Evaluation

Where to identify tools/resources?

Tools/resources can be identified through various markets or institutions. These outlets can be domestic, international or online.

What are some of the tools/resources?

List of generic tools/resources:

- Funds: organizational funds, external grants, donations, etc.
- Logistics: Transportation (vehicles, motorbikes, bicycles), accommodation, publications (eNewsletters, newspapers, social media platforms, websites, banners, posters, flyers/booklets, badges etc), stationary materials (pens, exercise books, etc...), food and refreshments.
- Equipment: Laptops, Tablets, Projectors, Flip Charts, Internet connection devices and other communication devices (Phone, Radio, TV, SMS, Public Announcement Systems), printers, scanners.
- Human: Experts (consultants, resource persons, advisers, panelists, rapporteurs), and relevant personnel (facilitators, support staff, stakeholder representatives, donor representatives, Civil Society Organizations, NGOs).

ASSUMPTIONS AND RISKS

It is essential to assess and highlight the potential risks associated with the awareness raising initiative. It is mandatory to perform comprehensive risk assessment for the organization/institute and with a conclude Risk list/matrix. After making your risk assessment, there is a need to make some assumptions. These assumptions can be categorized as beneficial and detrimental. It is ideal to first highlight the negative assumptions.

What are the factors that can affect launching your initiative?

- Lack of funding
- Poor planning
- Poor publicity
- Low turnout
- Low expertise
- Cultural, environmental, other natural factors
- Epidemic/Pandemic outbreaks
- Flooding, windstorms
- Fire outbreaks
- Conservative communities
- Difficulty in finding a Champion for the initiative.
- Lack of Political Will.
- Lack of persuasive techniques
- Sabotage
- Conflict of interest
- Corruption

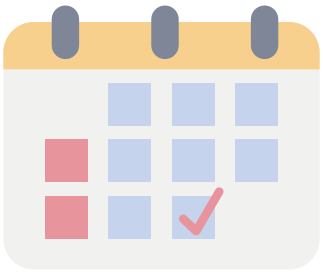
What are the possible success factors for your initiative?

The following are key success factors of awareness raising initiatives. They can be considered positive assumptions:

- Understanding of the subject matter and its positive impact on beneficiaries at the end of the initiative.
- Securing funding
- Proper/good planning
- Good publicity
- Great turnout
- High expertise
- Favorable cultural, environmental, other natural conditions.
- Getting a good Champion on board for the initiative.
- Demonstration of Political Will.
- Great persuasive techniques
- Supporters
- No Conflict of interest
- Honesty
- Positive stakeholder feedback
- Securing partnership with donors, public, private entities.

IMPLEMENTATION OF PLANS OF ACTION

Implementation must always follow the approved plan and budget. Therefore, it is imperative that the following steps are observed:



1. Revert to program plan of action
2. Confirm the personnel that will be working on the initiative.
3. Review and update the work plan
   Prior to starting the initiative. This is to ensure the initiative's milestones are ascertained. It will also assure compliance with objectives of the initiative as well as budgetary requirements.
4. Execute the initiative as guided in the work plan. It is obvious that the process may seem bureaucratic and time consuming. However, after embarking on these steps in sequential order, the implementation will go on smoothly and more effectively. After completing this stage, the confirmed personnel, or team may come in and play their roles as defined in the Plan, thereby achieving the overall objective of the initiative.
5. 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.
6. Communicate stakeholders at early and at the right time.

MONITORING AND EVALUATION

1. **Conduct Evaluation from project initiation to conclusion.**

2. **Document every lesson learned from the start of the project to conclusion. This is important because it will help you when the initiative is relaunched. The mistakes, shortcomings or failures that occurred during implementation will be improved in the next cycle. This will serve as a learning curve, especially when comparing success rates as per previous initiatives.**

3. **Roll-out of questionnaires to participants in order to capture feedback. The results obtained from feedback must be assessed and used to improve and track progress in subsequent cybersecurity awareness raising initiatives.**

4. **Measuring the Impact: At the beginning of the planning stage a monitoring and evaluation framework or form must be developed, which will be used to assess the effectiveness of the initiative over a long period and the effect it has brought to a larger community.**

5. Adjusting program/initiative on the fly: This step is vital in accommodating flexibility during implementation of activities. However, this flexibility must be limited based on the lessons learned 1.during execution of previous sub-activities and tasks of the initiative.

6. Preparing a Final Report and submitting a report to all stakeholders. It is important that the report reflects the input views of stakeholders. It should also include the lessons learned and success rates of the initiative.

COMMON MISTAKES TO AVOID

There are common mistakes that occur when launching such initiatives. It is equally imperative to identify these common mistakes and become alert or watchful during implementation of activities. This will ensure mistakes are mitigated. The two key question are as follows:

What are the common mistakes?

- **Lack of proper planning**
- **Implementing the initiative without an appropriate budget for all activities.**
- **Less clarity about the importance of the initiative to stakeholders.**
- **Failure to abide by organizational principles and guidelines of both the initiative and its dependent processes.**
- **Failure to follow-up on activities.**
- **Too much information about the topic that is beyond scope of the initiative.**
- **Inadequate communication to stakeholders.**
- **Lack of proper organizational awareness and inconsistent procedures and strategies when communicating to stakeholders.**

How to avoid them?

There are several ways to avoid common mistakes highlighted above. Some of them include:

- Proper planning
- Get the budget of the initiative approved and secure funding.
- There must be clarity about the initiative to targeted audiences.
- Establish good and timely communication channels.
- Commit fully to organizational principles and guidelines and its dependencies.
- Proper organization of the entire initiative must be established and maintained.
- Ensure consistent follow-up and periodic reviews.
- Stay within scope of topics of discussions.

REVIEW CHECKLIST

It is critical to go over every step of your planning before executing the initiative to ensure the recommendations of this Guide are followed and the initiative is successfully accomplished. The same process applies during implementation. Therefore, it is recommended to have a checklist at every sub-stage of the Cybersecurity Awareness Raising Framework in figure 1.

The Checklist is divided into 8 stages for planning and initial engagement.

1. **Champion identified and brought on board**
2. **Plan and Budget prepared**
3. **Approval obtained**
4. **Resources Mobilized including tools**
5. **Stakeholders identified and engaged**
6. **Relevant Topics identified**
7. **Target Audience identified**
8. **Risks identified and assumptions made**

The second Checklist is divided into 2 stages

1. All activities Implemented
2. Monitoring and evaluation
    - Evaluation forms rolled out
    - Feedback collected
    - Lesson learned documented
    - Final Report prepared and communicated to stakeholders

CYBERSECURITY AWARENESS RAISING FRAMEWORK

The below diagram illustrates the framework of the National Cybersecurity Awareness Raising Guide.

Reference: ENISA Cybersecurity Awareness Raising Guide

THE NATIONAL CYBERSECURITY AWARENESS RAISING GUIDE

@moici_gambia | @moici

www.moici.gov.gm | info@moici.gov.gm