Final Report

Impact Evaluation

"Assessing the performance, success and impact of the SAFETAG audits implemented under the Greater Internet Freedom (GIF) project"

July 2023

Table of Contents

List of Acronyms

CSO	Civil Society Organization
GIF	Greater Internet Freedom
HRD	Human Rights Defender
IF	Internet Freedom
INGO	International Non-Governmental Organization
LATAM	Latin America
LGBTQI+	Lesbian, Gay, Bisexual, Transgender, Queer, & Intersex +
MEL	Monitoring, Evaluation, and Learning
MENA	Middle East and North Africa
RP	Regional Partner(s)
CP or LP	Country Partner(s) or Local Partner(s)
RRP	Risk Reduction Plans
SAFETAG	Security Auditing Framework and Evaluation Template for Advocacy Groups
VPN	Virtual Private Network

1. Executive summary

This report summarizes the findings and recommendations emerging from the Evaluation of "**the performance, success and impact of the SAFETAG audits implemented under the Greater Internet Freedom (GIF) project"** which was carried out from May to July 2023 by Purpose+Motion in close collaboration with GIF's Monitoring, Evaluation and Learning (MEL) team.

The report first provides a background (section 2) about the GIF project and SAFETAG, as well as the goals (3), methodology (4), data collection (5) and analysis (6) used for this Impact Evaluation. The main part of the report (section 7) then explores the findings towards answering the evaluation questions. Recommendations for SAFETAG and for the GIF team are presented in section 8.

The key highlights of the Impact Evaluation are:

- In most cases, **SAFETAG audits increase the security of organizations** and lead to changes in attitude and behavior of management and staff.
- However, **Audits must be part of larger strategy of and for CSO's security**: An audit alone usually is awareness raiser/ confidence builder/ quick win implementer; to have deep impact, must be done regularly, have funds for follow up + equipment, integrate other aspects of security/ wellbeing (e.g. mental-health, trauma, marginalized communities).
- **Skills + competencies of Auditor are crucial:** The competencies of the auditor (inter-personal, training, context awareness, dedication as well as technical know-how) are crucial to audit being impactful.
- **Negative impacts of audits** must also be recognized. Some examples of these include the possibility of increased fear and concern amongst audited staff; slowing down the work; or more work for staff.
- **Audits as a relationship creator**: The positive impact of auditors simply being "available"/ "friends" giving confidence and sense of solidarity to CSOs/ audited organizations.
- **Who asks for audit and Management involvement are key**: it is essential that the CSO and in particular Management own the process, ideally asking for the audit in the first place and then participating fully, and following up or implementing recommendations.

2. Background

2.1 GIF project

The Greater Internet Freedom Initiative (GIF) was designed as a three-year, consortium-based, global program that centers regional and local organizations at the forefront of the fight to preserve an open, interoperable, reliable and secure Internet. By extension this would protect the citizens, civic actors, journalists, and human rights defenders who rely on the internet to realize fundamental freedoms.

GIF aims to advance Internet freedom (IF) in the countries in which it works by ensuring that digital security capacities, data awareness, and activism on behalf of an open, interoperable, reliable, and secure Internet are available, adaptive and integrated into the operation of independent media and civil society. Internews' deep commitment to trust and local capacity building formed the core of their technical approach and informed every aspect of project implementation and management.

GIF aims to achieve this by focusing on two objectives:

> **Objective 1: Enhanced Digital Security for Civil Society and Media**
> **Objective 2: Increased Citizen Engagement in Internet Governance**

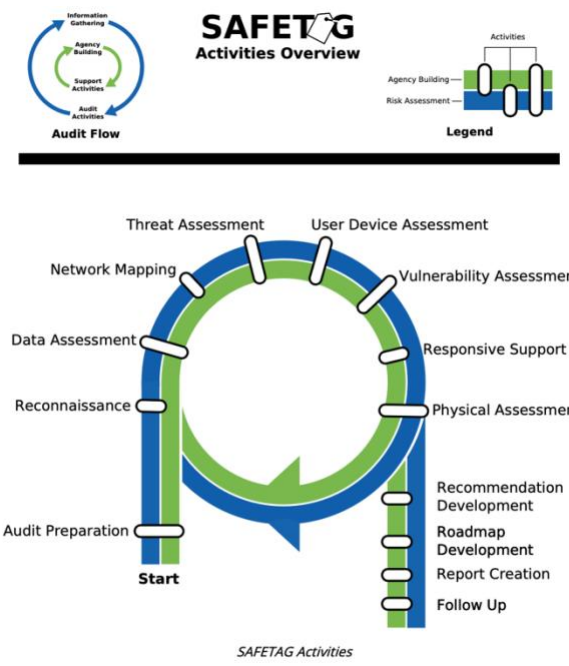
Under this Objective 1, the SAFETAG methodology is an important activity that support the following intermediary results:

> **IR 1.1.1 INCREASED CAPACITY: Increased capacity of CSOs, media outlets, and individuals in both preventative and responsive digital security approaches**
>
> **IR 1.1.2 INCREASED CAPACITY: Increased number of local digital security experts able to advance digital security capabilities of civil society, media organizations and vulnerable communities**

2.2 SAFETAG context

The Security Auditing Framework and Evaluation Template for Advocacy Groups (SAFETAG) is a professional audit framework that adapts traditional penetration testing and risk assessment methodologies to be relevant to small, non-profit, human rights organizations based or operating in the developing world.

SAFETAG is based upon a set of principles, activities, and best practices to allow digital security auditors to best support at-risk organizations by working with them to identify the



SAFETAG Activities

risks they face, the next steps they need to take to address them, and guidance on how to seek out support in the future.

SAFETAG audits are targeted at serving small scale civil society organizations or independent media houses who have strong digital security concerns but do not have the funds to afford a traditional digital security audit. The traditional security-audit framework is based upon the assumption that an organization has the time, money, and capacity to aim for as close to perfect security as possible. Low-income at-risk groups have none of these luxuries. These audits are both far too expensive, and produce output that is too complex for these organizations to act upon.

The SAFETAG audit consists of multiple information gathering and confirmations steps as well as research and capacity-building exercises with staff organized in a collection of objectives, each of which supports the core goals of SAFETAG, creating a risk assessment while also building the capacity of the organization.

2.2 Evaluators: Purpose+Motion

Purpose+Motion is a Berlin-based transformation agency which works with NGOs, social businesses and individuals to co-create a regenerative future. Purpose+Motion does this by supporting Gamechangers leading these organisations to develop their purposes and strategies, define and monitor the impact they are having, and integrate this as learnings within their organisations.

Purpose+Motion has been working with Internews since 2022, facilitating the GIF team and consortium members to work well together, learn from their work and grow the impact of the GIF project. In April 2023, Purpose+Motion was selected to carry out the Impact Evaluation requested by the GIF team.

Further information can be found on their website: purposeandmotion.com

3. Evaluation purpose and questions

The **purpose** of the Impact Evaluation is that the GIF team be able to answer the question: ***What have been the performance, successes, and impact of the SAFETAG audits conducted under the GIF project?***

The **evaluation questions** in the Scope of Work were:

- Are audits increasing digital security of beneficiaries?
- What methods and topic areas are being covered by the auditors?
- What activities are not conducted and why? (exploring if there are activities/methods that are difficult to learn or apply (especially more technical ones))
- What different ways are auditors carrying out audits (duration, scope of activities) and what skills do auditors need to increase the effectiveness of audits?
- What are best practices from the audits?
- How significant are audits to the organizations and to what extent is management involved?
- Are Risk Reduction Plans (RRP) relevant, pertinent and timely for the organizations?
- What is the most useful formats of audit recommendation delivery?
- What is (if any) is the optimal number of recommendations?
- What are the most pressing issues that audits reveal (if possible disaggregated by region)?
- To what extent is a follow up after an audit necessary for the effectiveness of the process (and if so, what type of follow up is effective)?
- What are the ways in which organizations are following up on recommendations?

4. Methodological approach

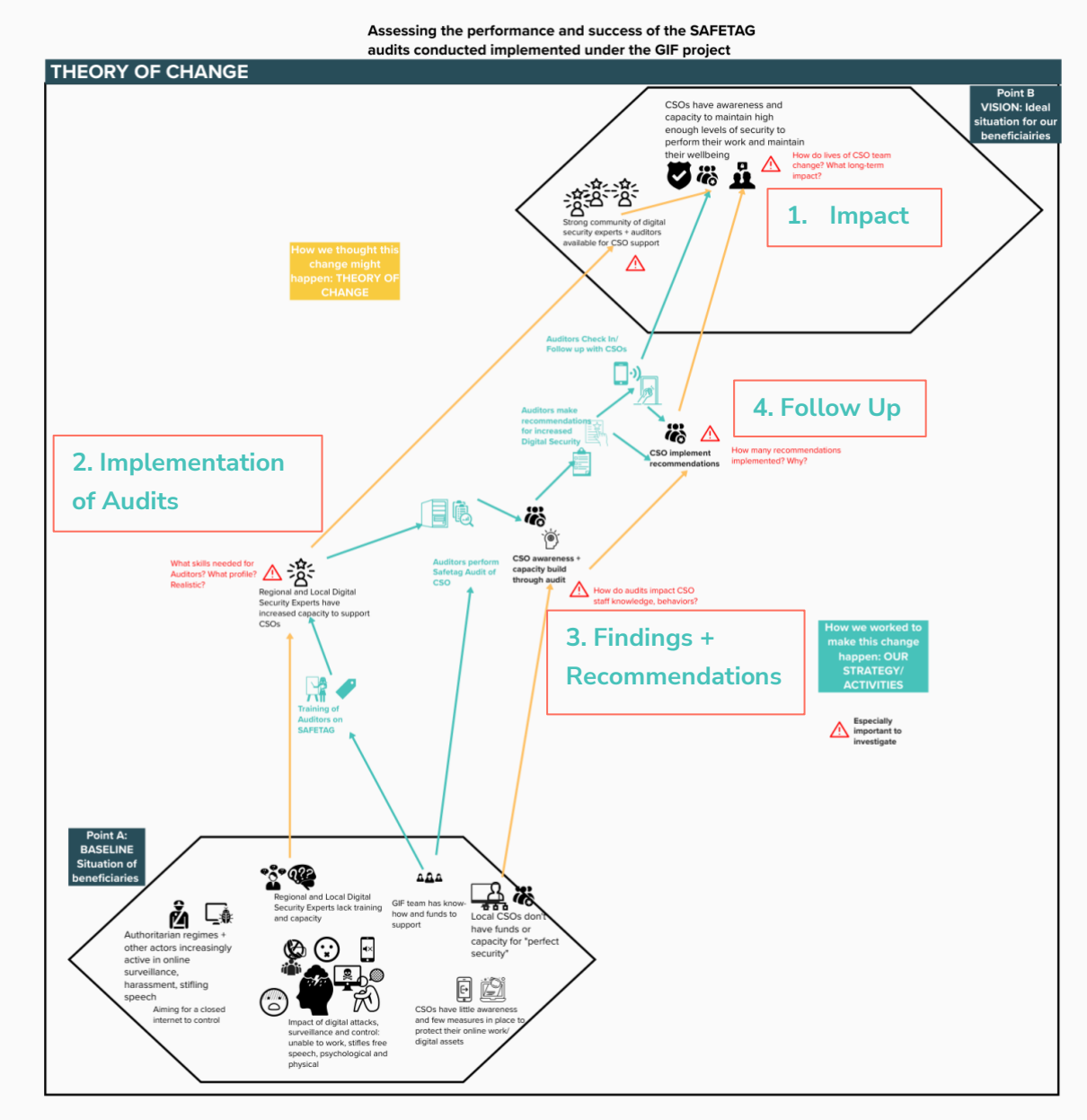
4.1 Design and methodology

As it was not a traditional **OECD criteria evaluation** (evaluating efficiency, effectiveness, sustainability, etc.) but **an "Impact Evaluation"**, we designed the methodology as follows:

- Focusing on exploring the impact of SAFETAG on audited organisations and auditors – both positive and negative, intended and unintended
- Focusing on gathering data and evidence useful to the SAFETAG community to improve the SAFETAG approach, as well as the larger strategies within which the SAFETAG audit is one element
- Triangulating qualitative findings (esp. interviews) with quantitative research (esp. survey, audit reports)
- Developing a nuanced and complex narrative of the impact of SAFETAG
- Aiming to build GIF team Impact Assessment capacities (esp. MEL team)

4.2 Theory of Change

A Theory of Change for the SAFETAG approach was developed, enabling the evaluation questions to be reorganised under 4 areas of focus:



Based on this Theory of Change and in coordination with the MEL team, the evaluation questions were reorganised as follows. In particular, the 2 further questions (in blue) were added to explore the impact of SAFETAG:

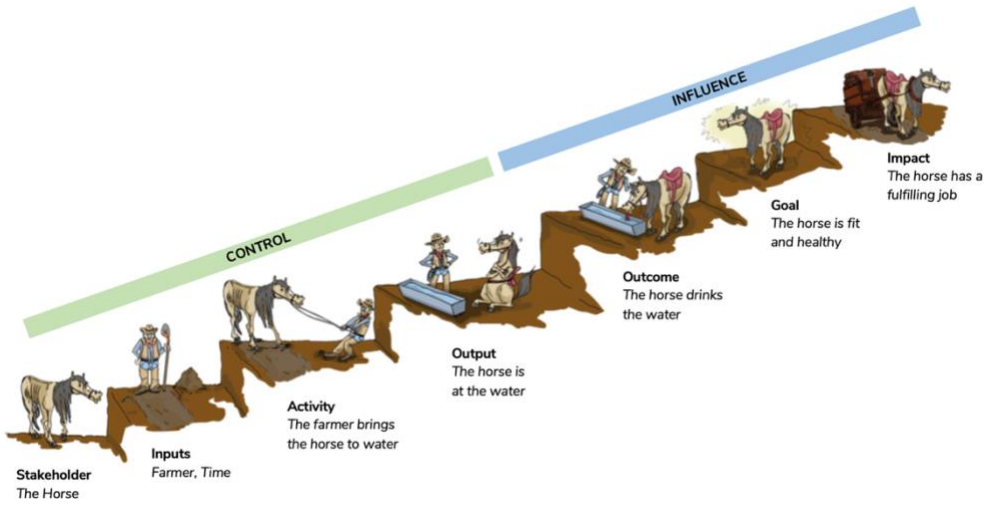
1. **IMPACT**
    - Are audits increasing digital security of beneficiaries?
    - What has changed in the lives of CSO staff due to the audit? What NEGATIVE consequences have audits had?

- How has the audit affected the ability of CSOs to carry out their work? What do/ can they do differently?

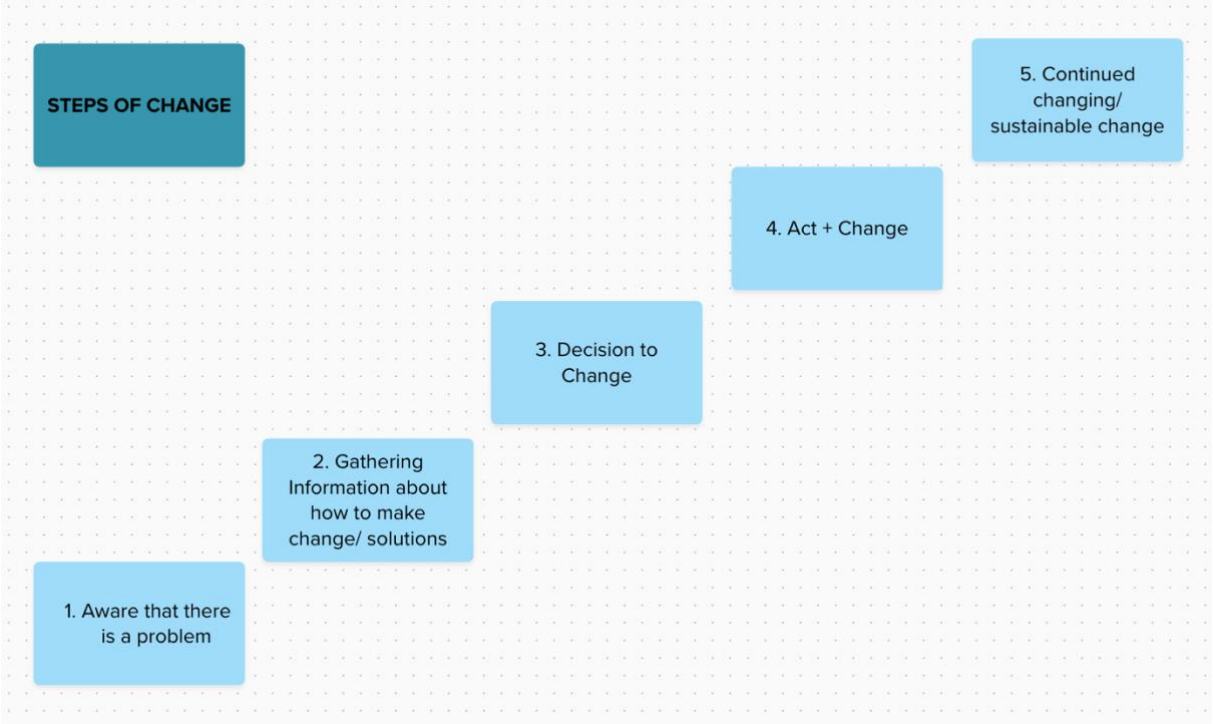
2. **IMPLEMENTATION**
    - What methods and topic areas are being covered by the auditors?
    - What activities are not conducted and why? (exploring if there are activities/methods are difficult to learn or apply (especially more technical ones))
    - In what different ways are auditors carrying out audits (duration, scope of activities) and what skills do auditors need?
    - What are best practices from the audits?
    - How significant are audits to the organizations and to what extent is management involved?
3. **FINDINGS + RECOMMENDATIONS**
    - Are risk mediation plans relevant, pertinent and timely for the organizations?
    - What are the most useful formats of audit recommendation delivery?
    - What is (if any) the optimal number of recommendations?
    - What are the most pressing issues that audits reveal (if possible disaggregated by region)?
4. **FOLLOW UP**
    - To what extent is follow up after audits necessary for the effectiveness of the process?
    - What are the ways in which organizations are following up on recommendations?

4.3 Definition of Impact

As this is an Impact Evaluation, it is important to clarify what we mean by "impact". The usual definition of **"impact"** is the **longer-term social or environmental changes (positive or negative) occurring because of a set of activities, project or strategy**. As shown by the graphic below, this can be understood in the "logical framework" often used for project management and MEL as beyond the project goal which the project activities are aiming to contribute to.



However, this very linear way of understanding the causal links between activities and impact is not always the best reflection of reality. We have found a useful refinement of this definition is to recognize that any long-term social or environmental changes require **sustainable or continued changes in PEOPLE's realities: beliefs, values, attitudes, knowledge, behaviors, situation** (i.e., step 5 in the steps of change below).



This means that we consider such sustainable change in people's realities as an impact, rather than simply an outcome of an activity. For example, changes in digital security behaviors of members of an organization audited using SAFETAG, when they are sustained over time, are considered an impact of the SAFETAG methodology.

4.4 Data protection

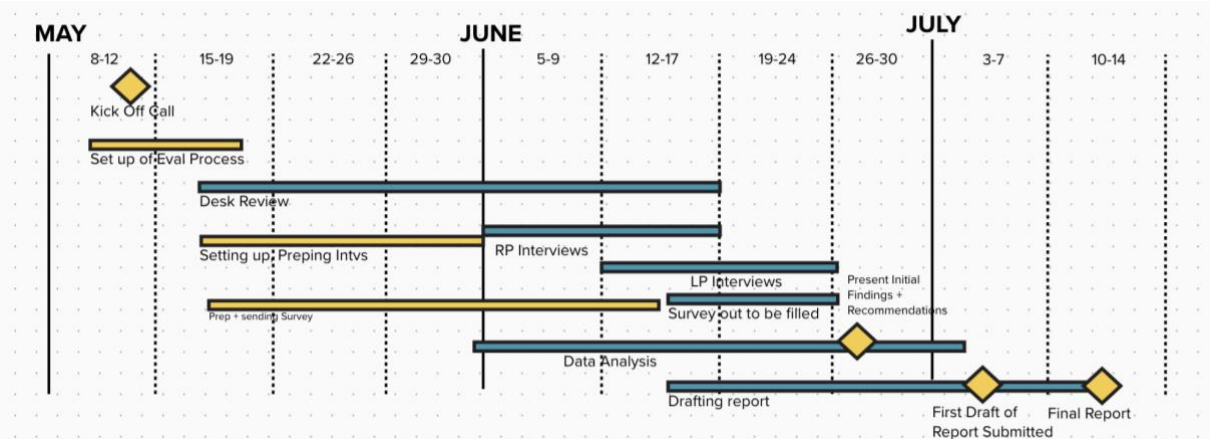
1. Protection of personal data is essential in any evaluation to respect the dignity of all participants and to ensure security, especially in the project context where the risk of data misuse is high. For all stakeholders (key informants), while their names and titles (function/role in an organization) were recorded by the evaluation team for analysis of any trends related to the information / data collected, their names or details were not connected to quotes or data received, preserving the anonymity and confidentiality of information.
2. Specific security measures have been implemented for database access and face-to-face communications to protect data, including using encrypted communications applications for participant contact.
3. We are aware of the obligation not to publish or otherwise disclose information about communities / beneficiaries to third parties, through whatever medium. In communications

with communities and all stakeholders, we have explained these obligations and procedures in a transparent manner so that participants understand the privacy protocol and can decide on that basis whether or not to participate in the evaluation.

4. All data gathered by P+M will be deleted from our servers after the submission of the final report, in order to protect the privacy and data security of those who participated in the evaluation.

4.5 Timeline of Evaluation

The evaluation was carried out from 1 May until 15 July 2023. The following timeline shows the order in which the evaluation activities were carried out:



4.6 Limitations and challenges

1) The **short timeframe of the evaluation (2,5 months)** meant that the usual process of doing the Desk Review to prepare the data gathering tools (survey and interviews) before gathering the data and then analyzing this could not be linear but had to be in parallel. There was also no time to iterate data gathering, going back to stakeholders for further information. It also made it challenging to ensure responses from and book interviews with stakeholders. Finally, it led to a very short time between having gathered all the data and needing to have analyzed it into findings and recommendations. This likely led to some insights and information not having emerged from the data.
2) There was an **unequal amount of data from different regions**, with a bias towards Central Asia, Eastern Europe and Sub-Saharan Africa, as partners there reacted quickly to requests for information and contacts. Also, the coverage of audits under the project was not homogeneous (no audits were done in South and Southeast Asia and Latin America (LATAM) has fewer audits than Eastern Europe or Sub-Saharan Africa for instance), and for some regions, security measures were taken to protect the data of auditors and beneficiaries, meaning the detailed audit reports could not be included in the evaluation.
3) **Most of the data received was self-reported by auditors and audited organisations,** with little "empirical" or "observed data" (no field visits, observation

of organisation's realities) to triangulate what is reported with what is actually changing on the ground.

4) A lot of the **responses, especially from auditors, were generalisations and estimates about sometimes dozens of audits**, making the precision of answers limited.
5) The choice of technical solutions for coding (DeDoose) was very user-unfriendly, and ended up wasting more time than saving. Purpose+Motion recommends using another application for any future Impact Evaluations by the MEL team. Also, delays in acquiring access to pro versions of tools (Descript, DeepL) led to delays in the evaluation process and timeline.
6) The fact that the evaluation team was able to run interviews in English and Spanish meant that stakeholders speaking other languages (Portuguese, Russian) required interpretation (for interviews) and translation (for surveys). This means there is likely a bias towards anglophone (and to some extent Spanish-speaking) respondents.
7) The sensitive nature of the subjects and conversations means that certain respondents likely did not share openly or fully. For example, in some interviews (done online), a more positive perspective about the situation and dangers might have been shared than if the stakeholder could be sure what they were saying couldn't end up with local authorities.
8) The fact that some of the interviews were carried out by two members of the GIF MEL team may have led to some bias. The concerns were that it could have been that the interlocutors were not as transparent / objective/ critical with the members of the project team versus external evaluators. This was mitigated by ensuring that any "sensitive" (where respondents might already be under pressure, or feel pressure not to be critical of the project to not lose funding) interviews were done by Purpose+Motion's team. Following the completion of interviews there were no (externally observable) signs that this limitation affected the results, but evaluators cannot discount the possibility of this bias.

5. Data collection methods

The impact evaluation used 3 data gathering methods: A **desk review** of documents provided by the GIF team; a series of **interviews** and **surveys** of auditors and audited CSOs.

Type of Research	Number of Sources
Desk review	41 Audit reports GIF Project Proposal, Workplan, MEL plan + Success stories 5 GIF Quarterly Reports 3 Reports from other Internews Projects

Interviews (22 people invited; 19 interviews with 22 people)	2 Internews Staff 1 External Consultant evaluating SAFETAG 13 Auditors (2 Spanish, 11 English) 6 Audited Orgs (2 English, 4 Russian)
Survey (sent to 33; received from 22)	12 Auditors (1 Portuguese, 1 Russian, 10 English) 10 Audited Orgs (3 Russian, 7 English)

5.1 Desk Review

The desk review included the above listed documents, reviewing and coding them for relevant information related to the evaluation questions. Qualitative information was gathered from the GIF reporting, the Audit reports and evaluations of other projects. Quantitative information was gathered from the Audit reports.

5.2 Primary data collection

Survey

The high response rates of 75% for auditors and 52% for audited CSOs means a very high level of engagement, and enables the evaluation to have a relatively high level of representativity (with the limitations explained above).

- Mode: Fully structured closed-ended online questionnaire with some open text responses.
- Sample: The total number of people the survey was sent to was 35.
- Duration: 13 minutes.
- Languages: The survey was available in English, Spanish, Portuguese and Russian.

Key Informant Interviews (KIIs)

19 Key Informant Interviews were conducted with a total of 22 stakeholders (some interviews were carried out with 2 or 3 people) connected to SAFETAG – key Internews staff working on SAFETAG, a consultant evaluating another Internews projects which uses SAFETAG, auditors and organisations audited using SAFETAG. These interviews were set up in this way:

- Mode: Semi-structured interview template.
- Sample size: 22 interviewees reached out to and 19 interviews carried out with 22 participants, from a relatively representative balance of different stakeholders (biased towards Central Asia, Eastern Europe, Sub-Saharan Africa).
- Method: MS Teams or Zoom, with informed consent.
- Duration: 60 minutes.
- Languages: Interviews were carried out in English, Spanish and Russian (with interpretation).

6. Data analysis

Quantitative and qualitative data and analysis was used for the purposes of answering the research questions, with narrative analysis applied as appropriate. DeDoose was the main tool used for gathering, coding and analyzing the data.

6.1 Quantitative data analysis

The quantitative data gathered from the Desk Review and Surveys were collated and analyzed together. A number of the research questions mainly required quantitative analysis (what were the optimal number of recommendations; which methods are most used and which least; etc.).

6.2 Qualitative data analysis

The qualitative data came from Audit reports, GIF reports, Interviews with stakeholders and the validation conversation with the GIF team. The qualitative elements include trends, recommendations, and specific examples giving evidence or nuance to findings. These were coded using DeDoose and included in the report as much as relevant.

6.3 Triangulation of Data

As much as possible and relevant, data was triangulated – from primary and secondary sources, quantitative and qualitative sources – in order to ensure as solid an evidentiary backing for the findings and conclusions reached.

7. Findings

From the data collected from the sample population, the following findings were found regarding the evaluation questions.

7.1 Impact

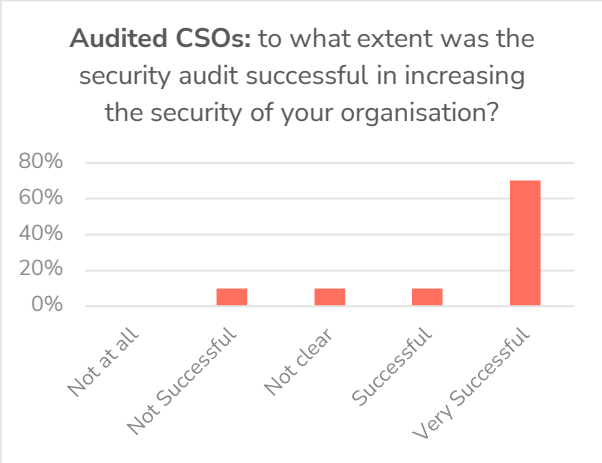
Guiding Research Questions:

- *Are audits increasing digital security of beneficiaries?*
- *What has changed in the lives of CSO staff due to the audit? What NEGATIVE consequences have audits had?*
- *How has the audit affected the ability of CSOs to carry out their work? What do / can they do differently?*

Findings:

1) **Most organisations audited using SAFETAG improve their digital security**, including through greater awareness of the risks, of security behaviours, and implementing recommendations which ensued.

Of the 12 auditors surveyed 75% said SAFETAG was successful and 17% said it was very successful at increasing the digital security of organisations. Of the 10 organisations surveyed, 80% stated the audit was either successful or very successful.



As one auditor explained: *"I would say that the SAFETAG audit methodology is a very good instrument, especially for civil society groups, as it actually solves a lot of things: it solves incidents, it solves risk, it solves attacks, and [it] has really been something that has increased the safety of organizations. [It] has given us resources definitely, and even given us more ability to be able to defend civil society rights and to be able to know where to get support."*

Interestingly, the organisation which rated the audit as "not successful", is also the only one where management was not involved in the audit. As will be explored below, this has been found to be a major factor in the success of audits.

2) In particular, IT staff changed their behaviours and saw their situations change after audits.

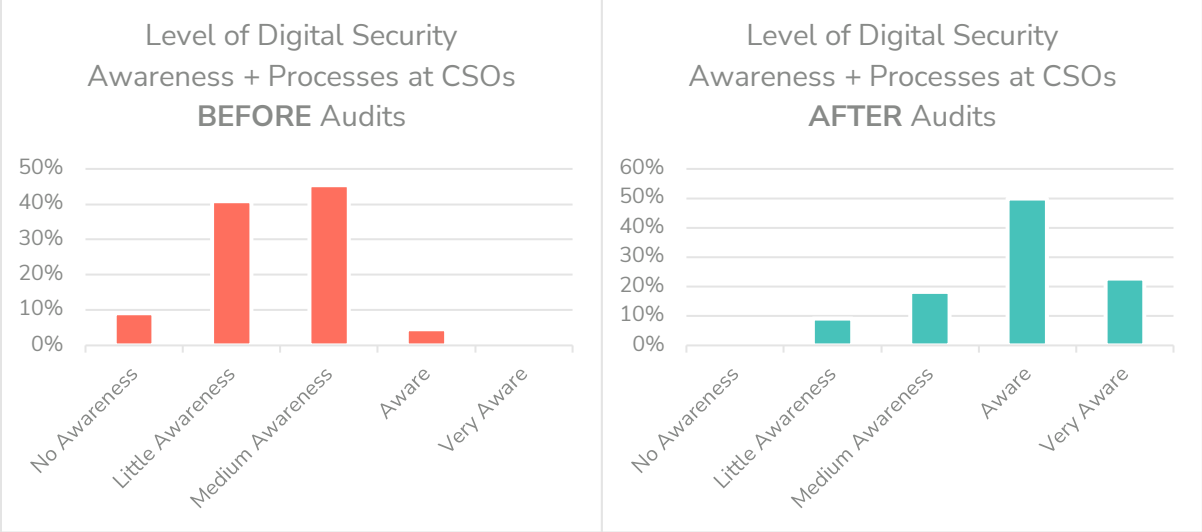
For example, a number of interviewees mentioned feeling motivated by the learnings and capacity building they got from the audit, searching for further capacity building.

As one IT staff member mentioned: *"And all of a sudden, after the audit, [my colleagues felt] 'we can trust the IT guys. Actually, they can help us identify these people who are listening to our conversation'. So I would say most of them, they are now [more] relaxed, as they know they found a solution."*

Others said they had their "position" or legitimacy within the organisation strengthened by the audit, as it showed the real risk and thus the importance of their role. For example, one member of an IT team explained: *"I'm so glad that this [auditor] team came because I have been passionate about security as well. And this audit triggered me and gave me great enthusiasm to go deeper into security and [follow a training] course, to get the knowledge that I'm really lacking in this area so that I can reach an expert level. These hackers keep changing their methods of attacking our organization, so I've developed a desire to learn more of whatever is out there, to see how best I can secure the organization."*

3) Staff in most audited organisations changed their Digital Security awareness, behaviours and processes.

Auditors and Audited organisations agreed that, on average, CSOs had a level of digital security awareness and processes ranging from “no awareness” to “medium awareness” before the audit. After the audit, 91% state the CSOs were between “Medium Awareness” and “Very Aware”.



Interviewees stated that most staff have a more confident, safer approach to their work after the audit. “*I can see that [my staff] are not scared anymore with the threats that are coming in, especially when there is a new incoming threat,*” mentioned the director of one organisation audited. An auditor explained: *“In many situations,* the *organization just became more relaxed, because they saw that they don't have such high risks or they do have high risks, but they are prepared for them.”*

Also, organisations implemented new policies which increased security: *“Now we've got a social media policy, you can post things on our social media platforms, but with the help of the social media policy. It is like a guide, including the dos and don'ts, i.e. you're not supposed to use a personal flash [drive] to put anything on an institutional computer.”*

It was especially appreciated that the methodology focuses on “empowering“ people to take ownership of their risks and actually learning how to handle them rather than seeing digital security as something too abstract or not “handle-able”, as it seemed before the audit. This was especially the case when the auditors then trained the team and gave information on what and why things are the way they are.

As one Auditor explains: “*Before we used to do audits, the most common [format of support for CSOs] was digital security training and this was awful because training does not resolve and answer a lot of problems, especially for the management of the organization, around what they need to do to decrease their risks but also for other staff. [Trainings were just about] studying, building knowledge or awareness raising, but not about the particular steps they need to do. Whereas during the audit, we are able to dive into the internal processes of the organization, we can talk with a lot of the staff, team and management, and we can find some solutions to the problems they are facing”.*

The director of one audited CSO explained "*I can mention that [my staff are] more confident in their work. What has changed in the way the team is doing their work is, in the past they responded by looking for an expert when they noticed that there was a problem. I've noticed now that my staff are trying to independently learn how to use these [digital security] tools and to be able to solve these problems so that they don't need these technical experts all the time.*"

Some staff also spread their knowledge outside of the organisation to other organisations or in their private lives.

In some cases, the audit recommendations also supported these changes in behaviour to be more sustainable. For example, one member of an audited CSO explained: "*We have a policy on the passwords where the server prompts users if the password stays the same for too many days. So, on the passwords, it's not actually [relying on] the users [alone to] do that.*"

4) However, in most cases, **the audit alone is not enough**.

Useful elements additional to the audit are:

1. **Awareness raising/ basic digital security training efforts before or after the audit;**

An auditor highlighted: "*In many instances, we have recommended trainings for staff. Most organizations have not thought about training staff as a group about digital security or raising some of the issues around security. So these trainings go a long way in making staff aware of some of the issues that they face and and it improves a lot how they change their behavior.*"

2. **Combination of "technical" audit with mental and physical-health assessments;**

For example, one auditor mentioned that they do "*a technical audit on the one hand, using SAFETAG and another audit based on mental health issues. Then we intertwine these two reports. We presented a technical report and another psycho-social report, and we look for a way to remedy issues from those two perspectives. We found that a lot of times somebody may be very good on the technical side, saying 'we're going to use these tools, have these policies.' But because social organizations find themselves working in a risky situation, working with people who are also at risk, you can understand a high stress level that can generate digital security risks.*"

3. **Upgrades of software and hardware and implementation of new policies;**

For example, an auditor mentioned: "*our philosophy here is we do SAFETAG audits, and then, because of our experience and what we have seen in the field, we see that it's always important to provide some level of fix up support. So fix up support would be things like, buying backup hard disks, which is not that big of a cost, but goes a long way in making sure that this organization has continuity, in case something happens to their computers or data*"

4. **Follow up/ check-in audits after the first one**

One audited organisation stated "*The audit was done two times. This is very important that this audit should not only be done once but done every few years.*"

5. **On-demand IT support**

This same organisation stated: "*We need to stay in contact with the auditor. Maybe for technical support, maybe just advice or recommendations during the 'burning' [crisis] situations.*" Another organisation explained: "*Our auditors, they are really open people, who*

answer my every question. They are really open for every favour I need. I don't know so many people in this digital security sphere."

5) Some **negative impacts of the Audits** were mentioned, though usually outweighed by the positive impacts.

In some cases, **staff felt worried and concerned by what audits finds**. For example, when spyware is found on personal devices, or that people were listening to their calls, it can create fear, insecurity and anxiety in staff.

One auditor mentioned, "*there were a few cases of increased fear, but we've since learned from those experiences. It stemmed mostly from how we presented findings. So, to be honest, when people are told their real situation and their vulnerabilities, [whether they become anxious or not] is about how you tell them*".

In other cases, **recommendations made after an audit have overwhelmed the organisation or are not adapted to the skills or capacity of the organisation, so hamper the work of the organisation**. As the IT expert from one audited organisation explained: *"The auditors helped us install anti-viruses on all our computers. These are very old computers, so now the computers are very slow. This has been limiting my colleagues' ability to do their work."*

Others pointed out how, **after the audit, the team and especially the management felt they had a lot more work**. As one director mentioned: "*This of course has increased my workload as a manager, but it's good*". The additional work for management, IT and also regular staff due to the new security policies, procedures and awareness, can slow down the work of the organisation, and it sometimes causes staff to go back to former (less secure) habits after some time.

A number of **audited organisations also stated that the recommendations report and presentation from the auditors took weeks or months to be delivered**, which left them in a bit of a limbo and also meant the openness and willingness of colleagues to make changes which was high right after the audit, go down considerably. One organisation mentioned that their audit happened in October 2022 and they received the audit recommendations in May 2023.

Some auditors pointed to **the risk that, during an audit, if something is done wrong on a technical level it can cause permanent or serious damage to the organisation's networks, devices or online presence** (website, social media). There were no concrete examples of where this had happened, but the risk is there, according to auditors.

6) The **skills and approach of the auditor** is seen by many audited CSOs as nearly more fundamental than the methodology used.

A high level of **technical skills** is appreciated. However, the **capacity building skills, understanding of the context and inter-personal skills needed to build and maintain**

relationships before and after the audit, and translate the technical to the non-technical stakeholders were seen as just as key.

"[You want] someone who is technically knowledgeable, he knows what he's talking about, he's been in this field, and then he's also providing solutions to those threats.", mentioned one interviewee.

Another member of an audited organisation mentioned that *"it is very important for the auditor to understand the depth, and the work of the organization, and even to be able to help us classify what we are doing from 'highest risk' to 'lowest' because they really understand our kind of work".*

The **ability to build trust is seen as crucial**. As one Auditor explained: *"If you have this confidence [and trust] with them then you will have better answers later."* A number of auditors mentioned that if the audited team trusts the auditor they are more comfortable sharing their devices to be audited, meaning the audit is more complete and hence increases the impact, whereas otherwise they might hide laptops or phones as they are too afraid to show it to the auditor (e.g. if they feel their "mistakes" will be shown to the management or the team - so having negative consequences).

Other skills outside of the technical repertoire needed for SAFETAG have also been highlighted by some auditors as important, such as the example of the **combination of "psycho-social assessments" with the "technical"** SAFETAG audit.

Some auditors mentioned they **usually don't call what they are doing an "audit" as this word scares people off** – often being associated with "financial audits" or "investigations for mistakes". Auditors use words such as "assessment framework", "security review" or "exploration".

As one auditor explains: *"This person immediately became super defensive when we indicated that we were there to do an audit. [He] felt like we're there to check on his work. Which was not true. We were an ally, but he already saw us as the enemy because we were going to call out his [mistakes] if there were any. Or that's at least what he thought."*

In some cases it seems that **poor levels of inter-personal, communication skills or attitude from auditors toward organisations led to audits being resisted by organisations**. Using sentences in the audit reports such as "Having *** is a disaster waiting to happen" or coming across as condescending or too "audit/ inquisitive-like" with the teams of audited organizations meant certain teams actively worked against the audits.

The fact that **finding individuals with this mix of skills and competencies, willing to do this kind of work in often difficult conditions, is a real challenge for the expansion of SAFETAG audits**.

Some auditors address this by **working in teams of complementary auditors** – some with technical knowledge, others more knowledgeable about the topic and field of work or with greater inter-personal skills. Though this of course requires enough resources for audits with larger teams.

Another option was for **those with part of this skill set to work on building the other skills**. However, until now, the SAFETAG training and materials mainly includes support on the technical elements of the audits, and the audit process itself, but very little about the more inter-personal, communication or psycho-social competencies also much appreciated by audited organizations.

Internews colleagues working on the SAFETAG approach explained that there were some elements of this in the e-learning course for SAFETAG onboarding and other training curricula, but that it is still an area where improvement could be needed.

7) Numerous organisations stated that **the "friendship" or "loyalty" of the auditor** to the organisation (especially when these work on "controversial" topics such as LGBTQ+ issues, etc.), including following up afterwards or being on call for technical issues, is one of the most impactful elements brought by the audit.

One audited CSO mentioned: "*It's a very big thing for us, for me: Our meeting with them was helpful that we make a friendship because we work with LGBT people in our country and it's really difficult to [find people to work with us] who really support us, who are really aligned. Because when we start to work with them, it's really like dangerous to talk openly. That's why I think it's important for us to have friends in that sphere [of Digital Security].*"

Another explained *"[The Auditor] is a very close partner to us now, and we need to have constant access to him for support. Maybe technical, maybe just advice or recommendations during the 'burning' [crisis] situations, because this always helps us when we are in 'hot spots'".*

8) Especially key is also that auditors are locally based, and have both local context (socio-political-security) but also knowledge of the CSOs and how they work.

For example, one audited organisation stated that, whilst the audit wasn't so impactful for their organisation, because they were quite advanced already, thanks to the support on their digital security from an international NGO, what was really supportive was that "*[the auditors] are the first people who I work together with who are based here, because [the INGO] is based somewhere in Europe and I can see them only once if they come [here]. That's why I think it's important for me and for our organization to have them here: we can easily, openly talk and ask for help or favours.*"

9) **Who asks for audit is key** to the engagement and ownership, and ultimately the success of the audit in increasing the security of the audited organisation.

Three different formats of request for audits were found in the data, usually (but not always) leading to different levels of ownership and success. These scenarios include situations mentioned by auditors from outside of the GIF:

1) **The organisation reaches out to the auditor for support**. This also includes situations where the organisation simply asks for help without knowing about an audit, and the auditor proposes the audit as a response to the needs they hear of. In

this situation, the ownership is often the highest, especially if this occurs after a crisis or serious incident – what one auditor labeled "social proof" (i.e. proof that there is a real risk for them.)

2) **The organisation is asked by a donor for a digital security policy or to have the results of an audit to receive funds**. In this situation, ownership of the process and the impact it has is usually minimal. Some auditors state they refuse these requests from CSOs.

3) **An intermediary organisation (such as Internews) identifies organisations which could use support in building their digital security, and offer an audit as one part of a wider toolbox / set of offers**. In this situation, it is really crucial for the intermediary organisation to ensure that the organisation owns the process, at the risk of wasting money and time.

As one auditor mentioned "*It's a big difference [who is asking for the audit]. I like it when the organization asks, but not a donor because if a donor asks, the ownership of the process is on the donor but not on the management. They are not interested. What really makes a difference though, is when there has been some sort of security incident and after that we start an audit. Unfortunately, this is when the audit has the highest impact.*"

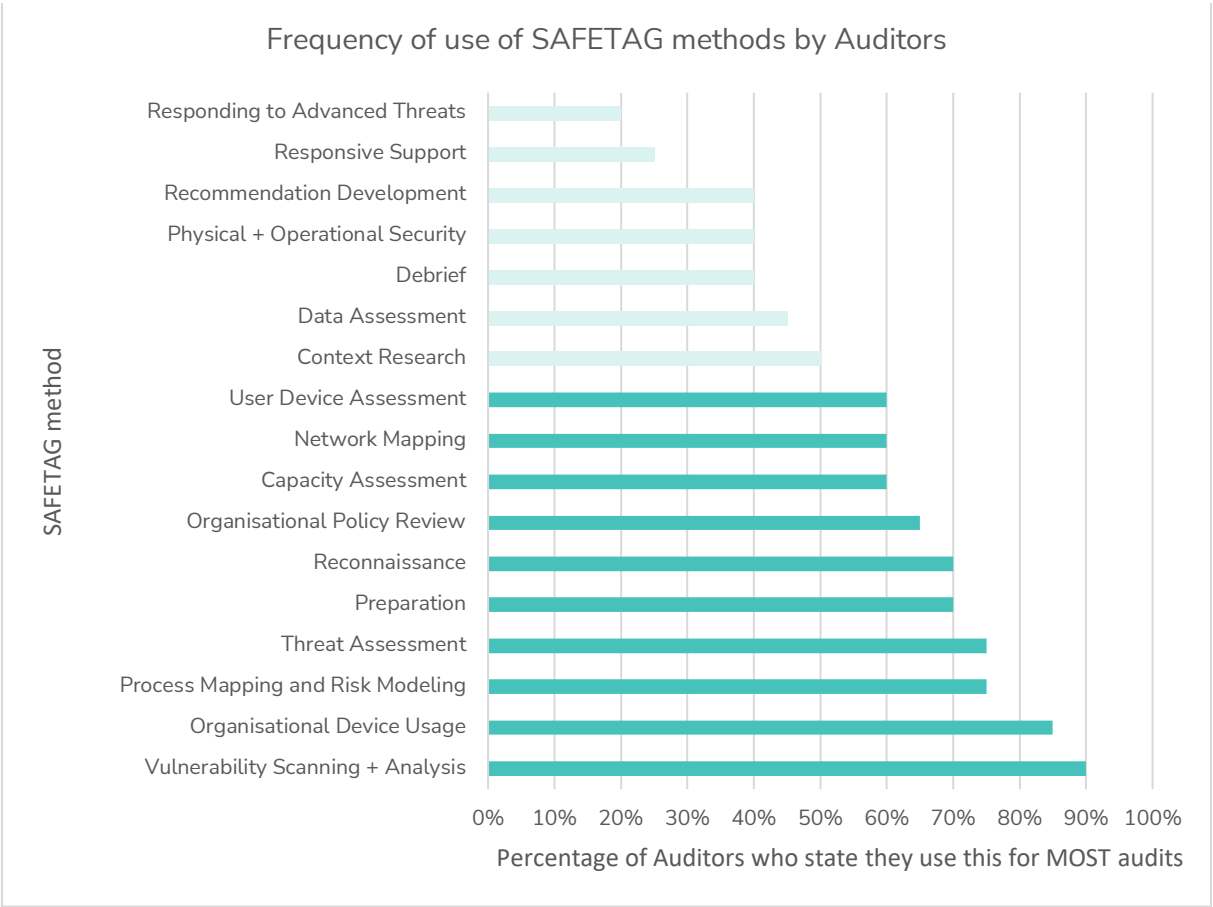
7.2 Implementation

Guiding Research Questions:

- *What methods and topic areas are being covered by the auditors?*
- *What activities are not conducted and why? (exploring if there are activities / methods are difficult to learn or apply (especially more technical ones))*
- *What different ways are auditors carrying out audits (duration, scope of activities) and what skills do auditors need?*
- *What are best practices from the audits?*
- *How significant are audits to the organizations and to what extent is management involved?*

Findings:

1) Each of the following 10 methods are used in MOST of the SafeTag audits carried out by at least 50% of the auditors surveyed:
    1. Vulnerability Scanning + Analysis
    2. Organisational Device Usage
    3. Process Mapping + Threat Modelling
    4. Threat Assessment
    5. Preparation
    6. Reconnaissance
    7. Organisational Policy Review
    8. Capacity Assessment
    9. Network Mapping
    10. User Device Usage Assessment;



	Total	Percentage	LATAM	SS Africa	Europe	Asia
Vulnerability Scanning + Analysis	18	90%	5	5	5	3
Organisational Device Usage	17	85%	6	5	4	2
Process Mapping and Threat Modelling	15	75%	4	4	5	2
Threat Assessment	15	75%	4	7	2	2
Preparation	14	70%	5	4	2	3
Reconnaissance	14	70%	5	5	2	2
Organisational Policy Review	13	65%	3	6	1	0
Capacity Assessment	12	60%	5	3	2	2
Network Mapping	12	60%	4	4	2	2
User Device Assessment	12	60%	3	3	4	2
Context Research	10	50%	4	2	1	0
Data Assessment	9	45%	2	4	0	1
Debrief	8	40%	2	2	0	2
Physical + Operational Security	8	40%	1	3	0	2
Recommendation Development	8	40%	2	3	2	1
Responsive Support	5	25%	1	1	1	1
Responding to Advanced Threats	4	20%	0	1	0	1

These trends seem to be reflected across all regions, though again, the limitation of an imbalance in information from each region is to be kept in mind.

2) At least 4 of the SafeTag activities are only rarely implemented: more than 25% of auditors surveyed never use them.

Which Methods do you NOT use?	Total	Percentage of auditors who NEVER use	LATAM	SS Africa	Europe	Asia
Physical + Operational Security	5	42%	4	0	0	1
Responsive Support	5	42%	2	1	1	1
Reconnaissance	3	25%	1	0	0	2
Responding to Advanced Threats	3	25%	2	0	0	1
Organisational Policy Review	2	17%	1	0	1	0
User Device Assessment	2	17%	1	0	0	1
Data Assessment	2	17%	2	0	0	0
Process Mapping and Threat Modelling	2	17%	1	0	0	1
Context Research	1	8%	0	0	1	0
Network Mapping	1	8%	0	0	0	1
Threat Assessment	1	8%	1	0	0	0
Debrief	1	8%	0	0	0	1
Preparation	0	0%	0	0	0	0
Capacity Assessment	0	0%	0	0	0	0
Organisational Device Usage	0	0%	0	0	0	0
Vulnerability Scanning + Analysis	0	0%	0	0	0	0
Report Creation + Recommendation Development	0	0%	0	0	0	0

Interestingly, one of the methods which is most often NOT used by a large number of auditors (25%) is also one of the most used: Reconnaissance, with 70% of auditors they use this for MOST audits (see findings 1)).

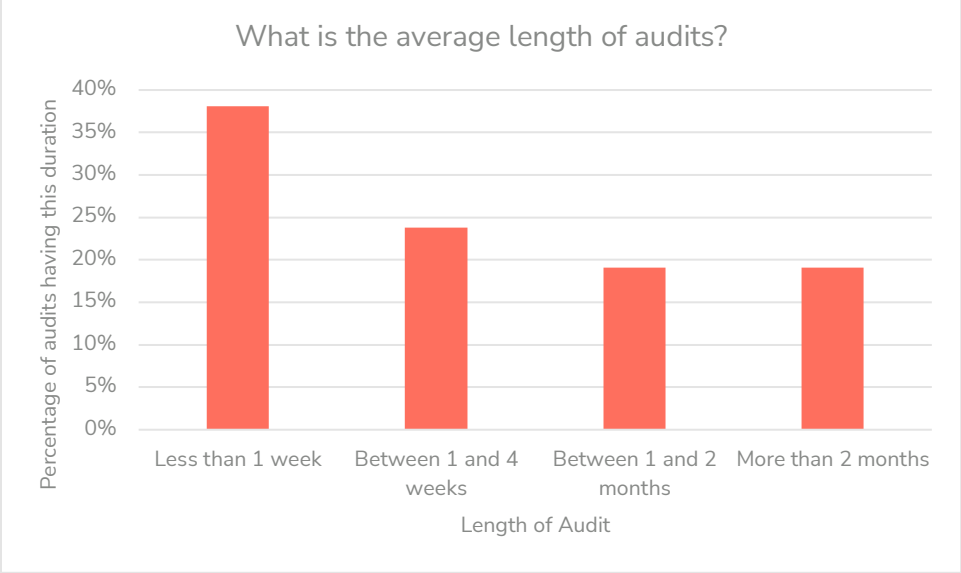
Again, this shows how varied and different the implementations of SAFETAG audits are in different contexts, and how broad the toolkit of SAFETAG is. Indeed, one auditor states (maybe somewhat exaggerating), *"in our work we are using maybe 5% of all of the SafeTag framework"*.

The main reason for these methods not being used are:

- The capacity of the Auditors to carry them out ("*I lack capacity to properly address those issues and topics I don't use*" or "*these are not our areas of expertise*").
- The lack of time available for the audit ("*time limitation for the audit, which required focusing on immediate security vulnerabilities and risks rather than extensive research*").
- Inability of the Organisations to adapt to the results of these activities ("*the organizations are small or without focus on digital communications*" and "*adapting to the context of the organisation*").

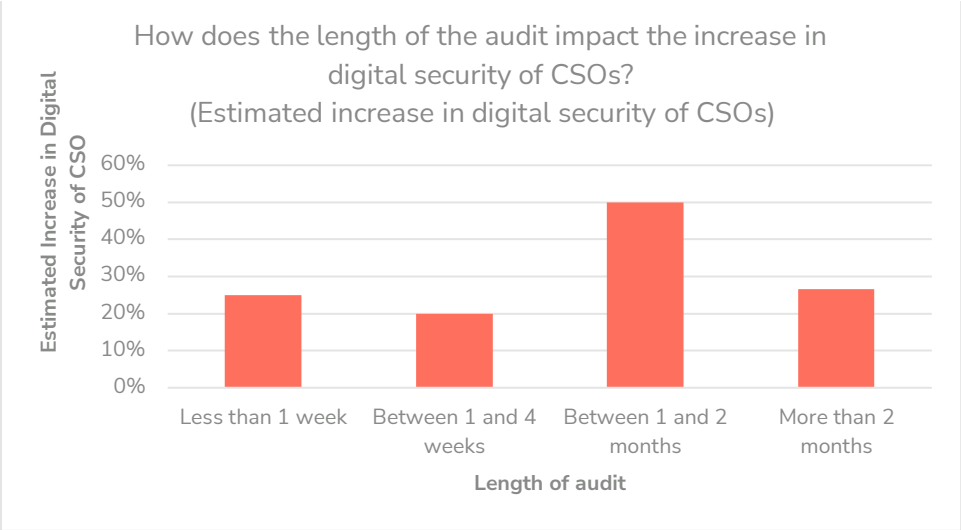
3) There are a wide range of ways that SafeTag audits are being implemented.

According to the data received, more than 60% of audits are less than a month long, and more than 35% are less than 1 week long.



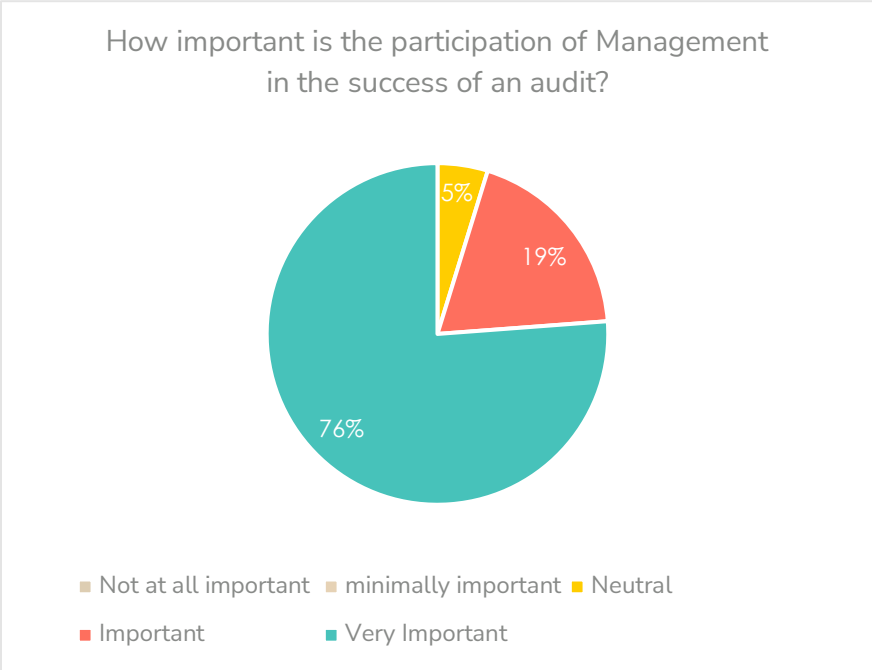
These are some different "modalities" of audits described by organisations and auditors:

A) **Short 2-3 hour conversation by phone with management;** main "quick win" recommendations; 1-2 page report with "status quo" and "risks + recommendations".
B) **1 week "speed-audit"** including in person visit to location, assessment of devices, etc. with the aim to get key recommendations implemented fast with the momentum built; short report focused on quick-wins.
C) **1-2 week audits** with interviews of all staff, visits to location, device analysis and work with management and teams. Long (10-15 page) report with recommendations.
D) **3 weeks to 2 months in depth audit**, interviews with most staff and management, awareness trainings, device analysis, visits to the offices, workshops. Long (20+ page) report with findings, recommendations and technical background.



Interestingly, from the sample population of auditors and with the limitations of self-reporting and generalization, there seems to be significantly greater impact when audits are between 1 and 2 months.

4) There is widespread agreement that audits without management involvement and buy in are ineffective.



As can be seen in this pie-chart, **95% of auditors and audited organisations feel that the participation of management are either "important" or "very important" in the success of an audit**.

Indeed, some auditors refuse to run an audit which doesn't include management. One Auditor stated: *"What we do is we only do our communication directly with the directors because, without them, then nothing is successful, especially in our country. Even if the staff see that there is a need for this. Audits without the management being involved would be just negative."*

Another mentioned: "*We choose [which organisation we work with] using a range of criteria: level of leadership ownership, the quality of participation, the level of commitment, who is involved to participate in an audit. Those four criteria, they make all the difference.*"

IT staff also explained why they saw particular benefit in management being involved: *"At times, management will question [what we say], they kind of don't understand. But the fact that management was involved [in the audit] and was there, at least it confirms our story. They see how much is involved for an organization to be highly secured. They get to know or hear it from someone else besides me. Cause some of these things we propose, and for some reason, obviously they'll hesitate. But then when they see that there are threats actually out there, so then they're like 'okay, I think it's time to consider this.' So for me that's a huge difference."*

As mentioned above, through the surveys, one of the rare cases where members of an organisation audited felt the audit was not effective, that the level of security awareness and processes didn't change, and that 0-20% of the recommendations were implemented, is also the only one which stated that Management was not involved in the audit. In this case, the member of the organisation stated that it would have been "very important" to have management involved. They also mentioned that the mediation plan, with between 6-10 recommendations was quite relevant to them, even if very few of the recommendations were implemented. It would be interesting to have this sort of feedback more systematically from organisations, to be able to follow up and understand the reasons for the lack of change.

5) The general consensus is that Management needs to be involved at specific points of the audit.

Most auditors agree that, at best, management should be present

- at the beginning of the process, for the initial meetings with the whole organisation and, for example, risk modeling exercises;
- in the middle, for example for their device assessments; and
- at the end whilst discussing recommendations and next steps.

7.3 Findings + Recommendations from Audits

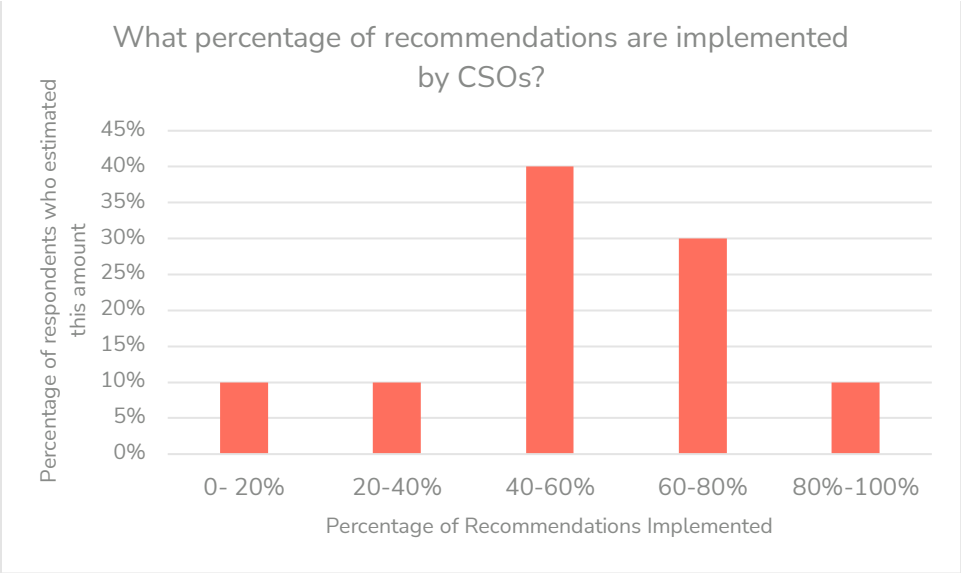
Guiding Research Questions:

- *Are risk mediation plans relevant, pertinent and timely for the organizations?*
- *What is the most useful formats of audit recommendation delivery?*
- *What is (if any) optimal number of recommendations?*
- *What are the most pressing issues that audits reveal (if possible desegregate by region)?*

Findings:

1) Overall, data shows that organisations implemented between 40-60% of the recommendations they received.

As the below table shows, 40% of respondents estimated that CSOs implemented more than 60% of the recommendations received, with the average amount of total recommendations implemented being between 40-60%.



However, 10% of respondents estimated that CSOs implemented none to very few (under 20%) of the recommendations.

An interesting issue which arose, around the resistance or failure to implement recommendations or improve security measures, was what **some respondents felt was a strategy by some actors to use security incidents against them as publicity**: "*Sometimes there is inaction because of what [stakeholders] hope will actually happen so that their profile gets bigger. They'll not do anything to fix it ahead of time because they want it to happen so that their funding increases, their profile increases, and their cause is more heard about. To say, 'look what they're doing to us'. And yet they could have done something about it.*"

2) A number of audited CSOs and auditors stated that, the likelihood of CSOs increasing their security has less to do with the mediation plans and recommendations being relevant, pertinent and timely, than **how these recommendations are formulated, delivered and followed up on**.

In some cases, auditors state that "*recommendations are developed jointly with the organisation*". For example, one auditor explained "*we have developed our own methodology that is quite participatory. After presenting the reports, together with the organisation, we create digital security policies based on the report. Then we follow up for two or three months to start implementing the policies. And that's where you start to notice a change in practical things, not as a simple thing from the way they manage their passwords. Then it's demonstrated through practical activities in their day-to-day life.*"

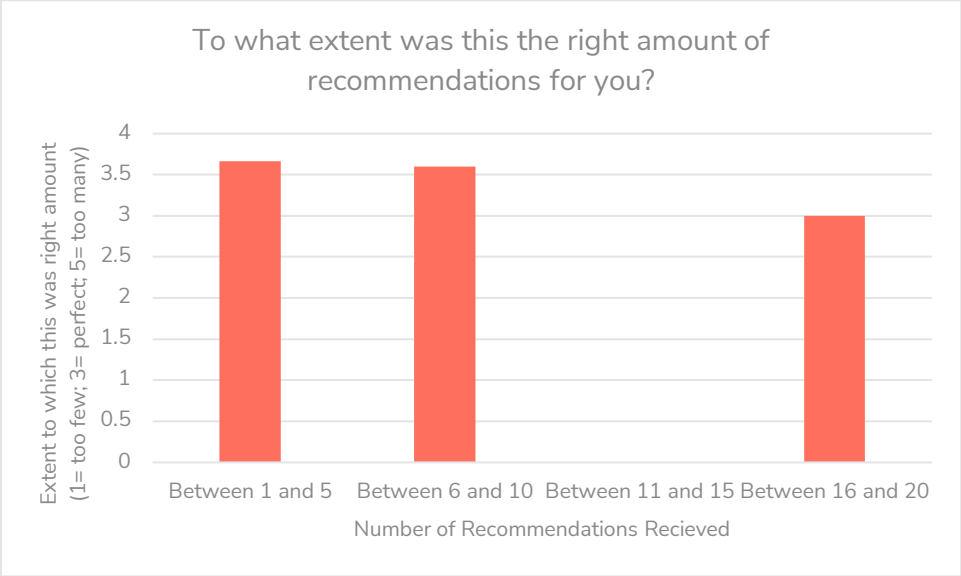
3) Organisations stated they appreciated having a written document summarising the recommendations and next steps; however, it was the final briefings, basic digital security trainings and implementation of the "quick win" measures by the auditors which was seen as most valuable.

As one auditor explained "*we still have a written report, but for them to incorporate or to absorb the knowledge from that report, we have to have a meeting and unpack it for them.*

Others are perfectly happy with just receiving a PDF that tells them that we found this problem and we think these are the fixes and you need to do XYZ to fix it."

4) There did not seem to be a clear pattern of a "perfect" number of recommendations for a report to have.

Indeed, and rather curiously, those organisations who received the least recommendations (between 1 and 5) felt it was too many, compared to those who received the most (16-20), feeling it was the perfect amount.



As one auditor highlights: "*[the number and type of recommendations] depends and the right formats are determined by the beneficiary [and whether or not they are comfortable reading longer documents]. Some organizations just want you to give them the highlights to say 'look, whatever you found, but how you tell it to us is you have this problem, is this bad? That's all we want.' Then some will not specify what they want, but you see from their circumstances that they have a high level of comprehension.*"

One director of an NGO, when receiving a 30-40 page audit report, exclaimed*: "I just don't have time to read this whole report, neither will I understand it. But what I need from you is a summary and some kind of a scale to say 'you have this problem and on a scale of one to 10, it is this bad'. That's, that's what's going to be useful to me."*

5) The **audits most often highlight the following 6 vulnerabilities**:

- Lack of Digital Security policies + procedures
- Issues with password strength, management and communication
- Unprotected Devices
- Unprotected Sensitive Files
- Lack of Digital Security understanding + awareness
- Phishing attacks

The following table shows the total prevalence of these in the documents reviewed, as well as the regional breakdown. This shows that in these regions, within the audits carried out and for which data was available, these issues and vulnerabilities are most prevalent.

	Total	MENA	Eastern Europe	Global	LATAM	Asia	North America	SS Africa	Western Europe
Lack of DS policies	26	0	0	0	0	5	0	21	0
Password Issues	26	0	0	0	1	9	0	16	0
Unprotected devices	16	0	0	0	0	3	0	13	0
Unprotected Sensitive Files	14	0	1	0	1	7	0	5	0
Lack of DS understanding	13	0	1	0	0	8	0	4	0
Phishing attacks	11	0	0	0	0	2	0	9	0
Lack of Physical Security	8	0	0	0	0	1	0	7	0
Lack of updates (software, web)	8	0	0	0	0	4	0	4	0
Virus contamination	8	0	0	0	0	0	0	8	0
Lack of backups	7	0	1	0	0	3	0	3	0
Unencrypted Information	7	0	0	0	0	1	0	6	0
Antivirus issues (unlicensed, out of date, Russian, etc.)	6	0	0	0	0	2	0	4	0
Network issues	6	0	0	0	0	4	0	2	0
Social Media issues	6	0	0	0	0	5	0	1	0
Lack of File Storage	4	0	0	0	0	2	0	2	0
Use of vulnerable Cloud based tools	3	0	0	0	0	3	0	0	0
Surveillance	2	0	0	0	0	1	0	1	0
Hosting Issues	1	0	0	0	0	1	0	0	0
Ownership of Domain	1	0	0	0	0	1	0	0	0

7.4 Follow up

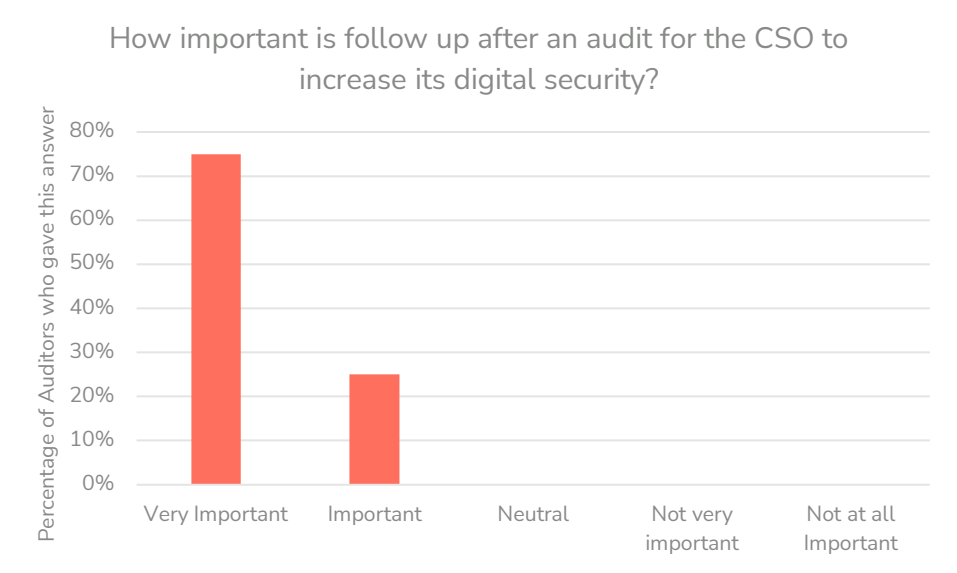
Guiding Research Questions:

- *To what extent is follow up after audits necessary for the effectiveness of the process?*
- *What are the ways in which organizations are following up on recommendations?*

Findings:

1) Follow up is a crucial factor in ensuring the organisation actually implements the recommendations, and improve their digital security.

While SAFETAG experts made it clear that, technically, follow up is not part of the "SAFETAG methodology" as it actually only includes the audit, the evidence of the importance of follow up on the success of audits in improving the digital security of CSOs makes it worth investigating.



Indeed, from the survey results, it is clear that 100% of auditors felt follow up was either important or very important.

Interestingly, despite the overwhelming evidence of the importance of follow up, interviews and evaluations of other programs describe how many projects have struggled to effectively provide reliable follow up to audits.

In some cases, only the audits themselves are funded as part of the project, with no attached follow up funds. Whilst some auditors stated that this ensured that follow up was "owned" by the organisation, and those who were motivated would make it happen, others felt this put them in an awkward situation, leaving organisations hanging with some pretty serious vulnerabilities unaddressed.

As an auditor said, "*Initially, we would just be given money or scope enough to do the audit. That's it [...]. We tell an organization, look, you have this problem and that problem, and we're trying to build relationships with these organizations, some of them have trusted us enough to be vulnerable with us to say 'sure, look at our systems, look at our servers.' And then you just say, 'you have this problem and that problem. That's it. And we we're not addressing the problems[...]' Then when something really hectic happens in an organization, they contact you again, you show up there to do first aid and then you find no one is using any of the tools you taught them.*"

Some auditors mentioned that they also felt uncomfortable as the message organisations got from them was, "*we can do this audit for free, but the follow up you have to pay for*", which felt more like the audit being a sales pitch, rather than real support for the organisation.

In other project set ups, funding was attached to every audit, but the administration of that funding was so heavy that at times it took months (and in one case a year) for the organisation to receive the funding for software and hardware upgrades, further training or other support they needed. In some of these cases, organisations said it made it nearly counterproductive to get the funding, as they could have organized themselves faster without it.

2) Most organisations implemented a small amount of the recommendations directly after the audit (or even as part of the debrief); however, implementation of the rest remained highly dependent on whether follow up support was available.

„*We believe that, once an audit is done, some of the low hanging fruits that you go on fixing here and there, like setting up passwords or turning on encryption, keep on protecting these people even long after you have gone. So I believe, it's really impactful for the security of organizations,*" said one auditor.

Some auditors explained that they see the difference in this level of implementation when they are doing an audit as part of a longer-term "accompaniment": "*If you're doing an accompaniment and you've estimated with the organization that we need to be with them for four months, that we estimate we'll finish all the fixes during that time. Then, there is definitely an observable amount of attitude and behavior change because they're interested in what you're doing. You are there, you are sort of keeping them accountable because you keep showing up, right?*"

8. Recommendations

Recommendations regarding SAFETAG

The following recommendations regarding improvements to SAFETAG as a framework or methodology and its implementation within projects emanate from respondents as well as from Purpose+Motion's analysis.

1) Have the **SAFETAG methodology, website and documents in other languages** (esp. Spanish). A number of respondents mentioned that the expansion of the SAFETAG methodology in their region was held back mainly by language, so people turn to other methods available in their language.
2) Explore how **SAFETAG can be mixed with / collaborate with other complementary methodologies**. In particular the inclusion of psycho-social assessments, trauma-informed and intersectional methodologies, ecological/ environmental risk and sustainability analyses, and facilitation methodologies could strengthen the impact of SAFETAG.
3) Build out and strengthen the **modules and training for auditors on inter-personal, communication and coaching competencies** and elements of the audit.
4) Develop larger digital security strategies with CSOs, including "upgraded" audits , where necessary, in the following ways:
    - **Identifying one or several "champions"** within the audited organisation who takes responsibility and accountability for following up on the recommendations and processes.
    - Enough **funds for multidisciplinary teams** to perform audits – either to implement different elements of SAFETAG, or intertwining SAFETAG audits and other complementary methodologies (see point 2) above).
    - **Funding for upgrades** of software, hardware and even physical security in buildings / spaces.
    - **Follow up audits every 12-24 months** – to ensure that the latest threats are identified, addressed and further upgrades are made.
    - **Monitoring of implementation of recommendations** by audited CSOs, which could bring valuable feedback to the effectiveness of different applications of SAFETAG, different approaches by auditors, etc.
    - Formalizing **training on digital security awareness and techniques for CSO staff** before or after the audit. The connection with the audit being a crucial part in making the training relevant to their daily life and work.
    - A **certificate for the audited organization** / IT teams participating in the audit.
5) Clearer **guidance on reporting to CSOs the findings and recommendations of SAFETAG audits**.
    - Template for different types of organisations (with IT department; only to management; as capacity building for all staff).
    - Examples of different ways to provide the recommendations (report; trainings or workshops with staff; etc.).

- Incorporate activities into the framework to help auditors develop recommendations in a collaborative way with the organizations.
- Encouraging auditors to have recommendations and debriefs with organisations shortly (within days to a week) after the audit.

6) More **meetings and joint trainings of auditors across regions**, to exchange experiences, tools and provide mutual support.
    - These might include other practitioners conducting similar kinds of activities, like incident responders, trainers, etc.

Recommendations to GIF team on future Impact Assessment

As this was the first Impact Evaluation run by the GIF MEL team, it was also a pilot to learn what else the MEL team needs to more regularly and easily monitor and report on the impact of the GIF project on key stakeholders. Below are listed some recommendations from Purpose+Motion's side in this direction:

1) Brainstorm with GIF team and consortium, as well as donors or other Internews teams about **further impact topics to explore** and questions to answer.
2) Increasingly **integrate questions relevant to these impact topics in monitoring tools** and reporting requests from project partners.
3) Explore **what other methods and opportunities can be created or used to gather continuous impact related data** – be it interviews with or surveys for partner or beneficiary organisations before and after sets of activities from the GIF project; more in-depth conversations with a range of project stakeholders on a regular basis (to note the changes over time); etc.
4) Consider creating **a tool to maintain an overview of the Impact of SAFETAG audits carried out throughout the GIF project** including: when was the initial audit, what were main vulnerabilities and recommendations identified; what follow up was done; what was "baseline" of the organisation vs. changes in processes, behaviours and DS overall. This would require regular check-ins with each organisation (either by auditors or GIF team) – see above recommendation of regular check-ins.
5) Ensure increased **alignment between reporting, MEL and communications functions within the GIF team**, to ensure a smooth user experience for project partners and to avoid duplication or triplication of efforts by team members.

Annexes

Annex A: KII Template (Auditors)

Specific Questions

Thank you for taking the time to talk with me today.

If needed, introduce yourself.

Internews is working on the Greater Internet Freedom (GIF) project with which you have interacted. I want to speak with you today about the experience of the SafeTag approach you have been involved in. There are no wrong answers to any of the questions, and our focus is to learn what impact the GIF and SafeTag activities and approach are having on the groups using them.

MUST READ VERBATIM: Your responses will be kept confidential, so you can be honest and direct. Only our research team will see them; other members of the GIF consortium will only see the full results of our analysis. No information or quotes we use will be attributable to the person or organization who said them, without us first checking for your explicit consent. You also do not need to respond to any questions that you feel would risk the security of the organizations with which you worked or which you feel unsafe or uncomfortable about answering.

We estimate the following questions to take about 45-60 minutes. Is that ok? Do you have any questions before we get started?

If yes and no questions, continue.

Administrative Information

1. Date and time of interview:
2. Info about person/ people:
    - Name of respondent:
    - Position within organisation:
    - Name of organisation:
    - How many audits using Safetag/ including safetag methods?
    - What countries do you work in?
    - What type of work do you do?
    - When was your audit using Safetag carried out?
3. Info about organisation
    - Name of organisation
    - How many auditors in your organisation?
    - How many auditors are male/ female/ other?
    - When org established?
    - How many employees?

Research Questions

RQ 1: Are audits increasing digital security of beneficiaries?

1.1. **MUST:** Do you believe the auditing model is successful to increase the security of Civil Society organizations? Why/how?

1.1.1. **Nice to have:** Did Audits help surfacing vulnerabilities organizations didn't know about?

1.1.2. **Nice to have:** Are there other factors that makes audits more or less successful to increase the security of the beneficiary organizations?

RQ 2: What has changed in the lives of CSO staff due to the audit?

1.1. MUST: How have you noticed members of CSOs act differently with the knowledge and results of the audits?

1.2. MUST: What negative consequences have you seen from audits? (greater fear? More awareness of vulnerability?

1.2.1. Nice to have: Has it changed anything in how their feelings of security/ mental wellbeing/ stress?

RQ 3: How has the audited affected their ability to carry out their work? What do/ can they do differently?

1.1. MUST: After the audit, in what ways did organizations change their attitude towards security process and policies?

1.2. MUST: Where does the request from for the audits? (the org, the auditor, the RP, donors, etc) What difference does it make on the success of the audit/ increase in the security of the CSO, where the request comes from?

1.2.1. Nice to have: How did it affect their ability to carry out their work?

1.2.2. Nice to have: What changes were you hoping to see and didn't?

RQ 6: Exploration of different ways auditors are carrying out audits (duration, scope of activities)?

1.1. MUST: What different ways have you implemented audits? (duration, infrastructure, etc) What influence does different implementations have on success?

1.1.1. Nice to have: What difference does the infrastructure, type of organisation, etc. make?

RQ 7: What are best practices from the audits?

1.1. MUST: What would you say are the best ways to use Safetag? What best practices can you share?

1.1.1. Nice to have: Do you have specific processes (not documented on SAFETAG) that you always follow for most or all your audits?

RQ 8: How significant are audits to the organizations and to what extent is management involved?

1.1. MUST: What is the difference in success when management/ directors are involved/ on board with the audit vs. When they are not? Why?

RQ 10: What is the most useful formats of audit recommendation delivery?

1.1. MUST: What have you found are the most effective/ useful formats to deliver the reccommendations to the beneficiary org (report document, presentation, workshop)?

1.1.1. Nice to have: How is the report sent to the partners (given that it is sensitive document)?

RQ 12: What are the most pressing issues that audits reveal (if possible desegregate by region) ?

1.1. MUST: Are there recurring vulnerabilities that appear every time on audits?

1.1.1. Nice to have: Are they technical (like related to servers, devices, etc.) or more related to processes (like related to policies, agreements, habits, etc)?

RQ 13: To what extent is follow up after audits necessary for the effectiveness of the process?

1.1. MUST: To what extent is follow up after audits necessary for the effectiveness of the process?

RQ 14: What are the ways in which organizations are following up on recommendations?

1.1. MUST: How are organisations you audited following up on the recommendations?

1.1.1. Nice to have: Which are the main limitations from the organization to implement the recommendations from audits?

What else is relevant to share with us for this evaluation? What recommendations do you have to improve the impact of the SafeTag approach?

Annex B: KII Template (Audited CSOs)

Specific Questions

Thank you for taking the time to talk with me today.

If needed, introduce yourself.

Internews is working on the Greater Internet Freedom (GIF) project with which you have interacted. I want to speak with you today about the experience of the SafeTag approach you have been involved in. There are no wrong answers to any of the questions, and our focus is to learn what impact the GIF and SafeTag activities and approach are having on the groups using them.

MUST READ VERBATIM: Your responses will be kept confidential, so you can be honest and direct. Only our research team will see them; other members of the GIF consortium will only see the full results of our analysis. No information or quotes we use will be attributable to the person or organization who said them, without us first checking for your explicit consent. You also do not need to respond to any questions that you feel would risk the security of the organizations with which you worked or which you feel unsafe or uncomfortable about answering.

We estimate the following questions to take about 45-60 minutes. Is that ok? Do you have any questions before we get started?

If yes and no questions, continue.

Administrative Information

1. Date and time of interview:
2. Info about person/ people:
    - Name of respondent:
    - Position within organisation:
    - Name of organisation:
    - What countries do you work in?
    - What type of work do you do?
    - When was your audit using Safetag carried out?
3. Info about organisation
    - Name of organisation
    - When org established?
    - How many employees?

Research Questions

RQ 1: Are audits increasing digital security of beneficiaries?

1.1. **MUST:** Was the auditing model successful to increase the security of your organizations? Why/how?

1.1.1. **Nice to have:** Did the Audit help surfacing vulnerabilities your organization didn't know about?

RQ 2: What has changed in the lives of CSO staff due to the audit?

1.1. MUST: How do team members act differently with the knowledge and results of the audits?

1.2. MUST: What negative consequences have you seen from audits? (greater fear? More awareness of vulnerability?)

1.2.1. Nice to have: Has it changed anything in how their feelings of security/ mental wellbeing/ stress?

RQ 3: How has the audited affected their ability to carry out their work? What do/ can they do differently?

1.1. MUST: Where did the request for the audit come from? (the org, the auditor, the RP, donors, etc) What difference does it make to the success of the audit/ increase in the security of the CSO, where the request comes from?

1.2. MUST: After the audit, in what ways did your organization change its attitude towards security process and policies?

1.2.1. Nice to have: How did it affect your ability to carry out your work?

1.2.2. Nice to have: What changes were you hoping to see and didn't?

RQ 4: What methods and topic areas are being covered by the auditors?

1.1. MUST: Which methods and topics covered in the audit were particularly useful for you? Why?

RQ 7: What are best practices from the audits?

1.1. MUST: To what extent have you been sharing with other organisations the tools and processes of safetag?

RQ 8: How significant are audits to the organizations and to what extent is management involved?

1.1. Was management in your organisation involved in the audit? What difference did this make/ would this have made?

RQ 9: Are risk mediation plans relevant, pertinent and timely for the organizations?

1.1. MUST: How relevant, pertinent and timely was the mediation plan/ recommendations?

RQ 10: What is the most useful formats of audit recommendation delivery?

1.1. MUST: How were the audit recommendations delivered? How useful was this and what could have been better?

RQ 12: What are the most pressing issues that audits reveal (if possible desegregate by region) ?

1.1. MUST: Are there recurring vulnerabilities that appear every time on audits?

1.1.1. Nice to have: Are they technical (like related to servers, devices, etc.) or more related to processes (like related to policies, agreements, habits, etc)?

What else is relevant to share?

Annex C: Survey questions (Auditors)

First name
Last name
Email
Company
Consent and confidentiality Your responses will be kept confidential, so you can be honest and direct. Only our research team will see them; other members of the GIF consortium will only see the full results of our analysis. No information or quotes we use will be attributable to the person or organization who said them, without us first checking for your explicit consent. You also do not need to respond to any questions that you feel would risk the security of the organizations with which you worked or which you feel unsafe or uncomfortable about answering. Are these terms clear and do you accept them? I accept I do not Accept

Thank you. And are you an Auditor who uses SafeTag methodologies or a member of an organisation which was audited?
Thank you. Now a bit more information about you. How many Security audits have your performed?
And what countries have you performed these audits in?
Great. Now let's get into the real content of our research! In your experience, to what extent is the SafeTag auditing model successful to increase the security of civil society organizations?
On average, what level of security awareness and processes do the CSOs you audited have *BEFORE* the audit?
On average, what level of security awareness and processes do the CSOs you audited have *AFTER* the audit?
Which of the SafeTag Methods do you use for MOST audits?
Preparation
Context Research
Capacity Assessment
Reconnaissance
Organisational Policy Review
Network Mapping
Organisational Device Usage
User Device Assessment
Vulnerability Scanning + Analysis
Data Assessment
Physical + Operational Security
Process Mapping and Threat Modelling
Responding to Advanced Threats
Threat Assessment
Responsive Support
Debrief
Follow Up
Report Creation + Recommendation Development
Which of the SafeTag Methods do you NOT use?
Preparation
Context Research

Capacity Assessment
Reconnaissance
Organisational Policy Review
Network Mapping
Organisational Device Usage
User Device Assessment
Vulnerability Scanning + Analysis
Data Assessment
Physical + Operational Security
Process Mapping and Threat Modelling
Responding to Advanced Threats
Threat Assessment
Responsive Support
Debrief
Follow Up
Report Creation + Recommendation Development
How long, on average, do the audits take?
How often is management involved in the audits?
How important is it that management be involved in the audits?
How often have recommendations you made not been feasible for the organisations?
Rank in order of frequency used the different formats to deliver the audit recommendations?
How important is follow up after an audit?
On average, what percentage of recommendations would you say are implemented by audited organisations?
What else do you feel is relevant to share about the impact of SafeTag methodologies?

Annex D: Survey questions (Audited CSOs)

First name
Thank you. Now a bit more information about you and your organisation. What role do you hold in your organisation?
Which countries does your organisation work on?
How many people work for your organisation?
Great. Now let's get into the real content of our research! In what year was the sercurity (SafeTag) audit of your organisation performed?
And to what extent was the security audit successful in increasing the security of your organisation?
What level of security awareness and processes did your organisation have **BEFORE** the audit?
What level of security awareness and processes did your organisation have **AFTER** the audit?
Which of the SafeTag Methods were most useful for your organisation?
Preparation
Context Research
Capacity Assessment
Reconnaissance

Organisational Policy Review
Network Mapping
Organisational Device Usage
User Device Assessment
Vulnerability Scanning + Analysis
Data Assessment
Physical + Operational Security
Process Mapping and Threat Modelling
Responding to Advanced Threats
Threat Assessment
Responsive Support
Debrief
Follow Up
Report Creation + Recommendation Development
How long did the audit take?
Was the management of your organisation involved in the audit?
In your experience, how important was management's participation in the audit for the audit to be successful?
In your perspective, how important would it have been for management to have participated in the audit for the audit to be more successful?
How relevant was the mediation plan and recommendations you received from the auditor?

How many recommendations did you receive?
To what extent was this the right amount of recommendations for you?
Have you had any follow up with the auditor since the audit happened?
In what format did this follow up happen?
What percentage of recommendations received during the audit would you say your organisation has implemented?
What else do you feel is relevant to share about the impact of SafeTag methodologies?

Annex E: Picture of ToC (attached as separate file)