Monitoring and Evaluation Framework for Organisational Security

June 2020

THE ENGINE ROOM

Internews

Contents

At a glance

What is this guide?

The Engine Room worked with Internews and several practitioners from various backgrounds to design a monitoring and evaluation framework that organisational security (org sec) practitioners can use to measure the impact of their work. The framework is designed to measure changes in organisational knowledge, attitude, behavior and condition, giving a clear and comprehensive picture of the achievements and solutions practitioners enable. This guide supports you in using the framework.

Who is this framework for?

Organisational security practitioners from all backgrounds.

Why should I use this framework?

- To understand what's working, what can be improved and what can be discarded
- To focus on effectiveness in different contexts
- To help organisations see and celebrate improvements while recognising remaining gaps
- To demonstrate impact to funders and donors so they invest in org sec

How does this framework define org sec?

The framework was created with four guiding principles in mind:

1. Org sec involves a holistic approach: physical, psychosocial, digital.
2. The duration of org sec support affects the quality of the impact and the ability to measure that impact.
3. Organisational culture plays a significant role in the success of org sec.
4. Each organisation has unique needs, and org sec must respond to changing contexts.

When should I use this framework?

The full framework is designed to be used to evaluate long-term, holistic support, but we've also included a light version for shorter-term and limited support. Ideally, you would begin using this framework at the start of your support, but if you want to incorporate it into a project that you have already begun, you can do so. Just be sure you can document improvements, showing where an organisation started and the changes they made, in the time remaining.

Which framework is the right one for me?

There are two frameworks available: the full version and the light version.

Use the full version if any of the following apply:

- ❏ You are providing long-term support (a few months to years)
- ❏ You will do a safety audit or assessment, develop a plan and support implementation
- ❏ You have had a little practice with measuring outcomes (even if through the light version)

Use the light version if any of the following apply:

- ❏ You are providing shorter-term support
- ❏ You lack time for a fuller evaluation
- ❏ You have no experience with measuring outcomes

What will I get out of this guide?

Through this guide, you will be able to:

- Understand how this framework was built
- Dive deeper into its guiding principles and imagine how they apply to your work
- Explore the two versions of the framework and learn which one applies to you
- Learn how to use both versions
- Learn how to create additional objectives and outcomes
- Explore ways to collect data for the framework

Introduction

Human rights organisations (HROs) often face attacks that can disrupt their work, cause physical and psychological harm to staff, volunteers and the people they serve, and have long-term consequences for human rights across regions. HROs working in conflict or authoritarian environments face additional barriers to effectively addressing security threats. Powerful states, along with closely tied companies, target poorly resourced organisations that are often working without a support network. Few HROs have dedicated IT staff, necessary equipment and tools, and adequate knowledge of how to identify and mitigate malicious activity.

This is where organisational security practitioners come in. **Organisational security (org sec) is a holistic approach to developing, implementing and monitoring digital, physical and psychosocial security practices and policies across an organisation.** Typically, a long-term org sec engagement will begin with a risk assessment or security audit, resulting in a report and recommendations. In some cases, there is also support to implement recommendations and/or follow-up to check that they have been implemented. Org sec practice, and the character of an engagement between a practitioner and an HRO, varies depending on the needs and context of the organisation, the level of resources available, and the practitioner's availability and capacity to assess holistically and technically.

Although some best practices have been developed in the org sec community, there has been no comprehensive evaluation of org sec methods to determine their effectiveness. It's clear that human rights organisations need support and that org sec must be effective on some level, but there are questions around level of impact and how to increase impact, especially when resources are limited. **The Engine Room worked with Internews and several practitioners from various backgrounds to design a monitoring and evaluation framework that org sec practitioners can use to measure the impact of their work.**

By building a deeper understanding of the impact of their work, practitioners can focus on what works in different contexts, refine approaches to increase impact and convince funders to invest in org sec. Presenting evaluation as an essential part of the support process can help organisations see the value of understanding the ways they are improving and where any gaps remain. **This framework is designed to measure changes in organisational knowledge, attitude, practices and condition, giving a clear and comprehensive picture of the achievements and solutions practitioners enable. It is a blueprint for how change can happen.**

This guide will support you in using the framework. You'll find details on the work and principles that informed the framework, the logic model for the framework (goal, objectives, outcomes), instructions on using and adapting the framework, tips and examples for data collection and analysis, and a lightweight version of the framework for simplified evaluation.

How the framework was developed

Our work on this is informed by multiple phases of research:

- **Desk research**: We searched for examples of monitoring and evaluation frameworks, tools and measurements, and we were unable to find anything comprehensive. We did, however, find analyses on the practices of org sec.
- **Internews regional workshops and surveys**: Practitioners from regions with challenges ranging from conflict to surveillance described their experiences and needs. These practitioners also completed surveys, giving us an overview of their thoughts on impact, including the barriers they face.
- **Interviews**: We conducted follow-up interviews with select workshop participants to better understand how they define and are measuring (or not) org sec impact.

This framework went through several rounds of revision with input from org sec practitioners embedded in a variety of communities. Some practitioners reviewed the framework, while others tested it and then sent their feedback.

Guiding principles

As we put together this framework, we worked with four guiding principles in org sec that were informed by the research phase. These are important to keep in mind as you use the framework.

1. **Organisational security involves a holistic approach.**

Addressing digital, physical and psychosocial security, sometimes alongside legal support, is important for sustaining good security practices. Sometimes practitioners are too overworked or under resourced to provide comprehensive support, but ideally org sec addresses all types of security risk.

🔑 *If you are only able to focus on one type of security, some parts of the framework will not be relevant. That's okay, but it's important to be aware of the many aspects of security.*

2. **The duration of org sec support affects the quality of the impact and the ability to measure that impact.**

Long-term support is necessary to build sustainable practices within an organisation. Taking the time to build trusting relationships—especially if only interacting remotely—encourages positive change within HROs and helps in shifting implementation priorities according to changing contexts. Long-term engagements allow HROs to build greater capacity to recognise digital attacks and collect the evidence needed to diagnose them as well as to identify attack trends internally and potentially among other HROs working in similar contexts.

A Tactical Tech case study revealed that the benefits of org sec may not be fully apparent until long after training, which means outcomes may be difficult to measure without long-term timelines that go beyond training. This is an important point to communicate to funders.

🔑 *You need to be able to see how an organisation has transformed their security practices and their thinking around security. These changes can be identified throughout a long-term process, although following up beyond the support period may be necessary.*

3. Organisational culture plays a significant role in the success of org sec.

An organisation has to be open to change on many levels and trust the process. Buy-in from senior staff is important for successful and lasting implementation of recommendations, and a willingness from all staff and volunteers to build a base level of awareness of security vulnerabilities is critical. Moreover, high staff or volunteer turnover can lead to a loss of internal knowledge. An organisational culture that reflects a commitment to policies, practices and continued training heavily affects the sustainability of impact. A key ingredient is collaboration between the practitioner and the organisation rather than simply giving directions.

🔑 *If an organisation does not or cannot commit to change, your ability to have a positive effect is limited. Keep this in mind as a barrier as you use the framework.*

4. Each organisation has unique needs, and org sec must respond to changing contexts.

A practitioner’s understanding of the context of each organisation they support can affect impact. This may include cultural, political, financial, sectoral and other contexts. This is one reason why it’s important to work with organisations to develop org sec plans collaboratively. Each organisation’s support plan will be different, which means evaluation plans will also vary. Furthermore, contexts, and therefore priorities, can shift rapidly. As organisational needs evolve so should evaluation.

🔑 *You can adapt the framework to suit the needs of each organisation you support by selecting outcomes from a list and even designing your own. Throughout the support period, you may find that you need to tweak or add outcomes due to changing contexts.*

Choosing a framework version

There are two frameworks available: the full version and the light version.

Use the full version if any of the following apply:

- ❏ You are providing long-term support (a few months to years)
- ❏ You will do a safety audit or assessment, develop a plan and support implementation
- ❏ You have had a little practice with measuring outcomes (even if through the light version)

Use the light version if any of the following apply:

- ❏ You are providing shorter-term support
- ❏ You lack time for a fuller evaluation
- ❏ You have no experience with measuring outcomes

Even if you choose the light version, it will be helpful for you to read the details below on the full framework to better understand the light version.

🔑 *You can find the light version on page 16.*

The full version emphasises the collaborative, flexible nature of org sec. It is designed to be adaptable for different contexts and to suit the needs of both the practitioner and the organisation they support. Objectives fall into three categories: service areas (infrastructure, response, culture and knowledge), holistic approach and context.

Logic model (full framework version)

A logic model is an explicit, visual representation of the intended effects of your work. It demonstrates a chain of causes and effects that ultimately lead to your goal. Goals tend to be fairly broad statements, while objectives show the different avenues you will follow to meet your goal. Outcomes are the quantifiable change you will measure to reflect those objectives. They are the steps that lead to overall impact.

Activities: Effective, sustainable organisational security can last anywhere from six months to several years. In that time, practitioners assess problems, develop recommendations, work with the organisation to implement recommendations, follow up on implementation and evaluate progress. Activities may also include building HRO trust, facilitating trainings, identifying resources and connecting HROs to networks of support, especially those sharing and analysing threats.

Goal: To build the capacity of organisations to prevent and mitigate security threats in a way that ensures sustainability.

- 📍 **Objective 1:** Practitioners and organisations work collaboratively.
  - ➢ Outcome 1.1: The practitioner and organisation work collaboratively and communicate ongoing needs effectively.
  - ➢ Outcome 1.2: The practitioner and organisation develop and maintain a workflow suitable for their specific context.

- 📍 **Objective 2:** Organisations develop a culture of security.

- Outcome 2.1: Decision makers in the organisation express commitment to the org sec process.
- Outcome 2.2: Decision makers in the organisation consistently make time for staff to discuss and work through the org sec process.
- Outcome 2.3: Staff and volunteers express support for the org sec process.
- Outcome 2.4: The organisation develops or improves an org sec policy and practices manual that follows a holistic approach.
- Outcome 2.5: The organisation trains staff to understand and use the org sec policy and practices manual and documents trainings.
- Outcome 2.6: The organisation revisits and updates the org sec policy and practices manual as necessary.
- Outcome 2.7: The organisation enforces adherence to the org sec policy and practices manual.
- Outcome 2.8: The organisation supports new staff in understanding and using the policy and practices manual.
- Outcome 2.9: Staff and volunteers talk regularly about security.

📍 **Objective 3:** Organisations successfully address physical and psychosocial security needs.

- Outcome 3.1: Staff and volunteers know how to anticipate and respond to physical threats.
- Outcome 3.2: Staff and volunteers know how to identify psychosocial needs.
- Outcome 3.3: Staff and volunteers have identified ways to cope with psychosocial needs.
- Outcome 3.4: The organisation has developed a process for providing or ensuring access to psychosocial support.
- Outcome 3.5: Staff and volunteers report feeling relatively safe at work and outside of work.

📍 **Objective 4:** Organisations improve their infrastructure and threat response.

➢ Outcome 4.1: The organisation regularly improves its infrastructure, such as hardware, to meet current needs.

➢ Outcome 4.2: The organisation understands what they need from the applications/tools they use when it comes to trust, security and functionality.

➢ Outcome 4.3: The organisation can successfully identify the most common threats they face.

➢ Outcome 4.4: The organisation has access to effective tools for threat mitigation that are relevant to their context.

➢ Outcome 4.5: The organisation can successfully mitigate most threats and access appropriate support for those they cannot address independently.

➢ Outcome 4.6: The organisation has processes and safeguards in place to help prevent the most common malicious attacks.

➢ Outcome 4.7: The organisation has developed and follows an internal threat-reporting process.

➢ Outcome 4.8: The organisation has developed and follows an external threat report-sharing process.

➢ Outcome 4.9: The organisation regularly documents security incidents.

📍 **Objective 5:** Practitioners and organisations work toward sustainability.

➢ Outcome 5.1: The organisation knows where to find information on trends and developments in org sec that are relevant to their context.

➢ Outcome 5.2: The organisation is part of a community of support that can help them continue building org sec skills.

➢ Outcome 5.3: The practitioner feels comfortable leaving org sec work in the hands of the organisation.

How to use the full framework

Select outcomes

1. Read through the logic model to understand how the goal, objectives and indicators fit together.
2. In the logic model tab, identify and highlight the outcomes that are relevant to the organisation you are supporting. In the full or light version tab, delete any indicators you will not be using at this time. You will not need to measure them, and leaving them in will negatively affect the formulas for overall change.
3. You may also create your own outcomes if you need to.
   🔑 *See more information on creating your own objectives and outcomes on page 13.*

4. Alternatively, you can edit indicators to better suit each support plan. First, read the tips on creating objectives and outcomes to be sure your edits create something measurable.

Score and explain

1. **Initial score:** The initial score is the baseline. At the beginning of your support period, give the organisation a score for each of your chosen outcomes. You can choose from 1-5 in the dropdown box for each.
2. **Justification:** In the Justification column, briefly explain why you scored them the way you did. A sentence or two will suffice. Documenting why you chose the scores you did will help you see more clearly any change that takes place. You can add data from the data collection methods you have chosen or pull information from the Notes tab in the framework or from other documentation you have kept during the support period.
   🔑 *See more about data collection methods on page 14.*
3. **Mid-term score:** You may come back to add mid-term scores if you are providing significant, long-term support. Mid-term scores can help you see whether or not the organisation is progressing and give you a good opportunity to reinforce discussions and practices. They can also capture progress that fluctuates. For instance, an organisation might improve on training their staff, have significant staff turnover and then fail to train the new staff. If you document this, you might see a low beginning score, a high midterm score and a low-medium final score.
4. **Final score:** At the end of your support, select final scores and add your justification. As you add mid-term and/or final scores, the percentage change will populate.

In the full framework, the scores range from 1 to 5, with 1 being the lowest and 5 being the highest. The following rough definitions will give you a sense of how to think about these numbers:

1	**Not at all**	The organisation has no experience with this outcome. There is little to no awareness. There is no policy or process in place.
2	**A little**	The organisation shows some understanding and has made some attempt to achieve this outcome. There has not been much success, but there is a little awareness and effort. There may be a policy or process that needs serious revision and enforcement.
3	**Somewhat**	The organisation has made a decent attempt to understand and implement this outcome and is having low to moderate success. There may be a policy without a process, a policy in need of some revision or a process in need of better enforcement. There may be a deep understanding without full implementation yet.
4	**Mostly**	The organisation shows significant understanding and has made a concerted effort to achieve this outcome. While they have been fairly successful, there is still room for improvement. There may be a need for additional training,

		improved policy enforcement, or knowledge documentation for potential staff turnover. It may be that implementation has not gone on long enough to be sure of success or sustainability.
5	**Very much**	The organisation has a deep understanding of this outcome and has successfully implemented it. The organisation has put in the work to make this change sustainable.

🔑 *A note on context: One of the difficulties of org sec is that **success may look different depending on the context**. Each organisation deals with different risks and has varying capacity, so it is important to score for each organisation and not compare one organisation to another.*

On infrastructure, for example, a very small organisation with limited resources might experience a critical change in security by simply upgrading their router, whereas a larger organisation with more resources might have more room to improve their infrastructure, with a router upgrade being one of several changes within the infrastructure outcome. You might give the first organisation a 3 or 4 after a router upgrade, but the second organisation a 2 because they still have a lot more to do. It depends on the audit and recommendations, as well as the level of impact the change has on the organisation. If the router is their biggest problem, this change can have a high impact.

Regularly review

1. Set aside time to review any documentation you are keeping on impact, including scoring.
2. Impact should be shared across teams to ensure that everyone sees the results of their work in terms of the big picture and understands what is working and what is not working.
3. Consider how to feed learnings back into the work. For example, if an approach to change in a certain area does not seem to be effective, think about how you can try a different approach.
4. You may find that your evaluation framework or methods need to be tweaked by, for example, capturing data through a different method, changing the wording in a survey question or editing your chosen outcomes. Measuring impact is a process of constant refinement.

Analyse results

There are a variety of ways to use this form to analyse impact. Use them all or choose what makes the most sense for your purposes.

1. Examine the range of scores from beginning, to mid, to end on each indicator to see how the organisation improved and/or struggled over time. This method works best when the duration of support is at least one year.
2. Compare the beginning score to the final score for each indicator by looking at the scores themselves and/or by noting the percentage change in the Overall change column.

3. Consider the potential reached. In other words, how much the organisation improved compared to the maximum amount (5) they could have improved. What might they need in order to do better?
4. Focus on the average final score for each objective in G21, G28 and G26.
5. Note the overall average score and the overall average change. Compare these results to what you expected or hoped for when you began.

Understand limitations

Because the success of org sec depends on a variety of factors, including forces outside of your (and even the organisation's) control, you may not see as much change as you had hoped to. This does not mean there was no success. In our research, practitioners reported that small successes are vital but often not visible. While a practitioner may see success on several outcomes, there may be many other indicators where there has been no significant change. This can lead to an overall sense of failure, but sometimes impact can be hard to define or document. Remember, true change takes time, and there may be little opportunity to see the change during short periods of engagement.

It’s important to recognise the different ways that org sec can be effective even if not every box is checked. Being realistic about the potential for change in difficult circumstances is also important. Remember, too, that this framework is not for comparing organisations against each other but for tracking progress within an organisation.

You can use the **Notes** tab to expand on your justifications, document unexpected impact, and explain why some outcomes were not reached. This can help you—as well as the organisation, funders or other partners—understand the barriers faced and whether or not they were beyond your control. Remember that this framework is not for comparing organisations against each other but for tracking progress within an organisation.

In our research, we found key barriers that can deeply limit impact no matter how competent and knowledgeable the practitioner is. Some of this has been addressed in the guiding principles section above, but other serious barriers that cannot be solved by org sec include the following:

- **Lack of funding for organisations to fully invest in org sec:** Many organisations cannot afford to hire an IT person or technical support of any sort, purchase necessary hardware and software, or change devices as needed, and funders are rarely supportive of the long-term capacity building org sec requires. Not having a dedicated ‘owner’ of IT security activities impacts organisations significantly.

- **Lack of time for HRO staff to engage:** Human rights workers often face burnout because of the demands of their work. Staff and volunteers are stretched thinly and focused on the urgent needs of their community. Burnout, harassment, physical threats, and funding difficulties can lead to high staff turnover, which can make it impossible to implement processes and enforce policies. This barrier also leads HROs to develop dependency on practitioners instead of making sustainable changes.

Our goal with the framework is to not only build evidence showing that org sec works but also to build evidence reflecting limitations that can be overcome by other tactics, such as funding and advocacy. **By using the framework, you can document these types of problems and contribute to systemic change in how funders and allies support HROs.**

How to create additional objectives and outcomes

Ideally, you will work with the organisation to prepare an evaluation framework that responds to their vision of success. Because each support plan will be unique, a one-size-fits-all approach to evaluating org sec impact has limitations. For this reason, you may need to define additional outcomes to measure. It's likely that any new outcomes can fit into one of the pre-defined objectives, but you can also add a new objective if necessary.

Note that if you add new outcomes, you may need to adjust the formulas to be sure they are included in averages and overall change. If you add objectives and outcomes, you can copy and paste the formulas from one of the current sections. Just check to be sure your formulas contain all the correct outcomes.

Objectives

Objectives are steps toward achieving a goal. As such, they are more specific than goals and are the foundation of outcomes. One goal can have multiple objectives, as in the case of this framework. The logic model, on page 6, shows you how the goal, activities, objectives and outcomes all fit together.

Outcomes

Outcomes are also sometimes known as "indicators." They are quantifiable statements describing how the objective will be met. In other words, outcomes are what you measure, and each objective usually has multiple outcomes.

Outcomes measure a change in the organisation you are supporting. Usually, they reflect a change in knowledge, attitude, behavior or condition. They should be SMART:

- **Specific:** Who will accomplish what?
- **Measurable:** How much change is expected? How will it be measured?
- **Achievable:** Can the expected change happen with available resources and time?
- **Relevant:** Will the indicator have an impact on the goal?
- **Timebound:** When will the impact be achieved?

Because this framework is intended to be used by a wide range of practitioners in different settings, the outcomes do not include all SMART details. You can add individuals or teams that you want to experience change, methods for capturing data on the change, and timeframes for when the change is expected. For instance, you might be able to accomplish some objectives in one month, some in three months and others in six months to a year. Think carefully about what is realistic and be as specific as possible.

You may also want to make the outcomes more specific based on a security audit. Outcomes 1.1, for example, broadly addresses infrastructure, but you may find specific infrastructure needs whose progress you want to measure individually.

🔑 *For more information, see:* [*https://www.betterevaluation.org/en/plan/describe/measures_indicators*](https://www.betterevaluation.org/en/plan/describe/measures_indicators).

Once you've created any new objectives or outcomes add them to the Objectives tab in the spreadsheet so you can see how all the pieces fit together and make sure there is no repetition. Add rows in the Outcomes form as you need to.

How to collect data for the framework

There are many ways of capturing data to evaluate an organisation's progress around org sec. Choose the method(s) you think will work best for the context you're in, keeping in mind your level of familiarity with evaluation, the ability of the organisation you're supporting to share information, and what is needed for you to have a solid understanding of impact. You will likely use different collection methods for different outcomes, as some outcomes are easier to observe whereas others require participant responses.

In each case, you start with a baseline—where the organisation is at the beginning. A security audit is a good way to get baseline data. You will also want to determine timelines for gathering and measuring data. Think about when each outcome can feasibly be accomplished and whether you may need to collect data on a particular outcome once or multiple times (e.g., quarterly).

Observation

Many org sec practitioners may already be capturing change without realising it simply by observing. You conduct a security audit, make recommendations, and then pay attention to what happens with your recommendations. Observation is a legitimate way of gathering information on impact.

Observation works best if you keep regular notes on how an organisation is progressing, what challenges they face along the way, and what strengths pop up throughout the process. If you work in a team, detailed notes on how you came to your conclusions can help colleagues make sense of your work and even pick up where you left off. This preserves the integrity of the evaluation process.

Interviews

If you're supporting an organisation from a distance, especially one that is difficult or impossible to get to, your main interaction with the organisation is likely through conversations with one or a few people. These conversations can be good opportunities to check in on progress in a way that feels informal and non-judgmental. Prepare a few questions for various calls according to your evaluation timeline and try to get clear, specific answers. You can work them into the conversation or schedule dedicated progress calls on a monthly or quarterly basis. If you are supporting a large organisation, you might interview people from different teams.

The benefit of interviews is that you can ask follow-up questions to dig deep and consider impact in context. It's harder to synthesise narrative responses than quantifiable data, however.

Pre- and post-tests

Pre- and post-tests are best used for capturing changes in knowledge resulting from a training or series of trainings. In such cases, you will want to give the pre-test before each training or at the start of a series and follow up with a post-test at the end of the training or series. Develop your test questions around the key indicators of knowledge an organisation needs to get out of the training.

The pre-test gives you baseline data. The post-test will look exactly the same as the pre-test and will allow you to see if participants improved their knowledge of certain areas. You might see people answering "no knowledge" or "little knowledge" regarding an indicator in a pre-test and "significant knowledge" on the same indicator in a post-test. You can count how many people improved on each outcome and use that as the justification for scoring in your framework. Depending on how much information your tests include, you can even capture a percentage reflecting how much people improved.

You can also use pre- and post-tests to measure changes in behaviour, but you will need to cover a longer period than a training. People need time to change their habits. You might give a behaviour pre-test at the beginning of your support period, examining activities like password management, and a post-test after three or six months.

🔑 *See Annex A for an example of a pre- and post-test.*

Surveys

Surveys can be used to measure just about anything. They can be written, digital, verbal or through a show of hands.

Surveys often use a Likert-style scale of five answer options (e.g., less confident, no change, a little more confident, somewhat more confident, much more confident). In other words, the full change is captured in one survey. With surveys of this style, you don't necessarily need to collect baseline data in advance (like with the pre-test) because participants select the answer that shows their level of improvement (e.g., much more confident).

One issue with surveys, and sometimes with pre- and post-tests depending on how they are written, is that they rely on self-reporting rather than demonstrating evidence of change. It's possible people may understate or overstate when reporting on their knowledge, attitude, or behaviour, especially if reporting through a show of hands or concerned others will see their answers. Because some data can only be captured or is best captured through self-reporting, the limitations of these methods are an accepted risk in evaluation. Still, it's important to decrease the risk as much as possible (e.g., only using a show of hands because you did not plan in advance and create a survey).

🔑 *See Annex B for an example of a survey.*

Light version

The light version of the framework will not give you as much impact data as the full version, but it should be useful in cases where the orgsec process is shorter or lighter. You can also use this version if you are new to measuring impact and want a simpler method to start with. If you use this tool with long-term support, we recommend that you use this version multiple times throughout the support period (e.g., every three months or every six months) to see what has improved each time.

This version uses a traffic light method of reflecting change instead of the more complicated scoring method. There are three traffic lights, to choose from:

1. **Red light**: not enough progress (or backslide from yellow)
2. **Yellow light:** some progress (or backslide from green)
3. **Green light:** excellent progress

You choose a 1, 2, or 3 from the dropdown box to get the right colour. The averages for each section will come up automatically, giving you a good sense of how the organisation is doing at a glance. Note that the colours for the averages show the spectrum between each colour. If the organisation averages a 2.25, for example, it will show up as light green instead of the full green of a 3 or the full yellow of a 2.

Note also that this version has fewer outcomes. We chose the indicators that reflect lighter or shorter support, but you can add any outcomes you wish.

Including comments about an organisation's progress is a simple way to add more context for future reference or for anyone reviewing the impact.

Annex A: Pre-/Post-test example

🔑 *To be used before and after individual training workshops, a series of trainings, or other learning processes. You will expect to see higher numbers in the post-test, reflecting change.*

Please circle your answer.

1. How well do you understand secure password management?

   1 - Not at all   2 - Slightly   3 - Moderately   4 - Very well   5 - Extremely well

2. Have you ever used a password manager?

   No   Unsure   Yes

3. How many of your personal and work devices are password protected?

   None   Less than half   Half   More than half   All

4. How confident are you in your ability to create secure passphrases?

   1 - Not at all   2 - Slightly   3 - Moderately   4 - Very confident   5 - Extremely confident

5. How often do you use social media logins for other accounts?

   1 - Never   2 - Rarely   3 - Sometimes   4 - Often   5 - Always

6. On how many accounts have you enabled two-factor authentication?

   None   Less than half   Half   More than half   All

Annex B: Survey example

🔑 *To be used after trainings, other learning processes, or direct support. Do not use alongside pre-/post-tests but in place of them. You can also use knowledge questions after a training and then give people time to put knowledge into practice before following up with practice questions.*

Please circle your answer.

1. Do you now have a better understanding of secure password management?

   1 - Not at all   2 - Slightly   3 - Moderately   4 - Definitely

2. Are you using the recommended password manager?

   1 - Not at all   2 - Rarely   3 - Sometimes   4 - Often   5 - Always

3. Are all of your devices now password protected?

   No   Unsure   Yes

4. Based on the guidance, have you created secure passphrases for your most important accounts?

   No   Unsure   Yes

5. Do you now have a better understanding of the risks of using social media logins for other accounts?

   1 - Not at all   2 - Slightly   3 - Moderately   4 - Definitely

6. On how many accounts have you enabled two-factor authentication?

   None   Less than half   Half   More than half   All