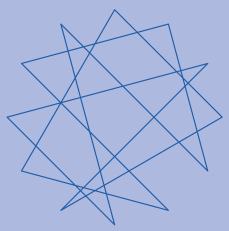
eisf



AN EISF GUIDE FOR NON-GOVERNMENTAL ORGANISATIONS

Security Audits

CHRISTOPHER FINUCANE FOR EUROPEAN INTERAGENCY SECURITY FORUM

European Interagency Security Forum (EISF)

The European Interagency Security Forum (EISF) is an independent platform for Security Focal Points from European humanitarian agencies operating overseas. EISF members are committed to improving the safety and security of relief operations and staff in a way that allows greater access to and impact for crisis-affected populations.

Key to EISF's work is the development of research and tools which promote awareness, preparedness and good practice.

EISF is an independent entity currently funded by The US Office of Foreign Disaster Assistance (OFDA), the Swiss Agency for Development and Cooperation (SDC), the Department for International Development (UK aid) and member contributions.

www.eisf.eu

Acknowledgements

Many people contributed to the development of this text. The background work commenced in 2009 when **Maarten Merkelbach** (Geneva Center for Security Policy) and **Christopher Finucane** researched the security systems of international aid organisations, seeking to understand better how NGOs were responding to increasing security challenges. The research continued with support from the Center for Refugee and Disaster Response at Johns Hopkins Bloomberg School of Public Health, where the methodology was refined with the guidance of Professor Gilbert Burnham. It is that research methodology that forms the basis of this comprehensive guide and tools.

This Guide was written by **Christopher Finucane** of Humanitarian Policy, and edited by **Ellie French** on behalf of the **EISF Secretariat**.

This publication would not have been possible without the participation of aid practitioners around the world, including from Save the Children, Medair, ZOA, Oxfam and War Child.

This project was made possible through financial support from EISF's donors and the Norwegian Refugee Council.

Disclaimer

design and artwork : www.wave.coop

Contents

Introduction

What is a security management system audit?

NGO security management is most effective when carried out in a systematic way. To do this, processes are applied in a logical order, to achieve desired conditions and outputs. For many NGOs, the security management system's primary purpose is to produce the conditions for an aid mission to be implemented within an acceptable risk tolerance in a given operating context.

A security management system (SMS) audit is an evidence-based review of the system's structure and functions and a test of the system's purpose. Auditing provides managers and their staff with essential information from which to identify system strengths and weaknesses, allowing resources to be focused where most needed. The audit process also serves as a tool for NGOs to conduct due diligence of their internal management processes and determine if the security management system is fit for purpose.

Why audit security management systems?

Aid organisations will audit their security management systems for two key reasons:

a. As employers, NGOs have a moral obligation towards their employees to ensure they are not placed in danger as a result of doing their jobs, and

b. In many contexts NGOs are obliged by law to exercise a duty of care towards employees, requiring clearly defined systems and processes to manage workplace risks.[1]

Understanding the structure of an SMS is essential when determining system effectiveness. What does the system actually look like? How can the system be communicated to those responsible for its implementation?

This guide first provides the process for answering these two key questions, and then presents tools to conduct an assessment of the system's design and effectiveness. Determining system effectiveness is more subjective than assessing its structure and design. In other words, it can be easier to describe what something looks like than to see how it works.

Who is this guide for?

The guide and tools are intended for aid practitioners and managers alike. Together, they present a standard audit method, supported by comprehensive guidance and supporting information. The tools are flexible, so may be applied to an entire organisational system or scaled down to address the needs of a field office.

Will I need training to audit an SMS?

By following the guidance, aid practitioners with an understanding and experience of their organisation's programme management approach ought to be able to apply the tools and audit the SMS. This guide is not intended for use solely by security focal points or security managers. While these roles may have greater insight into the nuances of the organisation's security management, by following this guidance and audit method, the system will be able to be analysed by non-security personnel with little or no training.

If NGOs were to consider in-house training on the use of the tools contained in this guide the key learning objectives would be:

- To understand the concepts, logic and processes which underpin a security management system before attempting to analyse the system
- To understand that security management systems are not stand-alone structures and will often be linked with other management systems within an organisation
- To understand that risk is often a subjective concept from an individual's point of view, thus producing widely varied attitudes and behaviours which may influence how a system is communicated and/or applied

Taking time to read this guidance before starting an audit will greatly reduce the need for training, and improve the quality of the audit outcome.

How to use the guide & tools

The guide provides useful background information and puts the tools into context. The tools are divided into three key parts, following a logical process:

- Section A is planning and preparing for your system audit
- Section B is conducting the audit
- Section C is analysing the results and determining what may be improved

This guide, while generic, forms a standard audit methodology for reference. NGOs may consider adapting parts of the audit process to better reflect their organisation's management structure.

Key concepts and definitions used are listed in the Glossary.

Many definitions are aligned to ISO 31000:2009 *Risk Management Principles and Guidelines* and ISO Guide 73 *Risk Management Vocabulary*.[2]

Throughout the text:

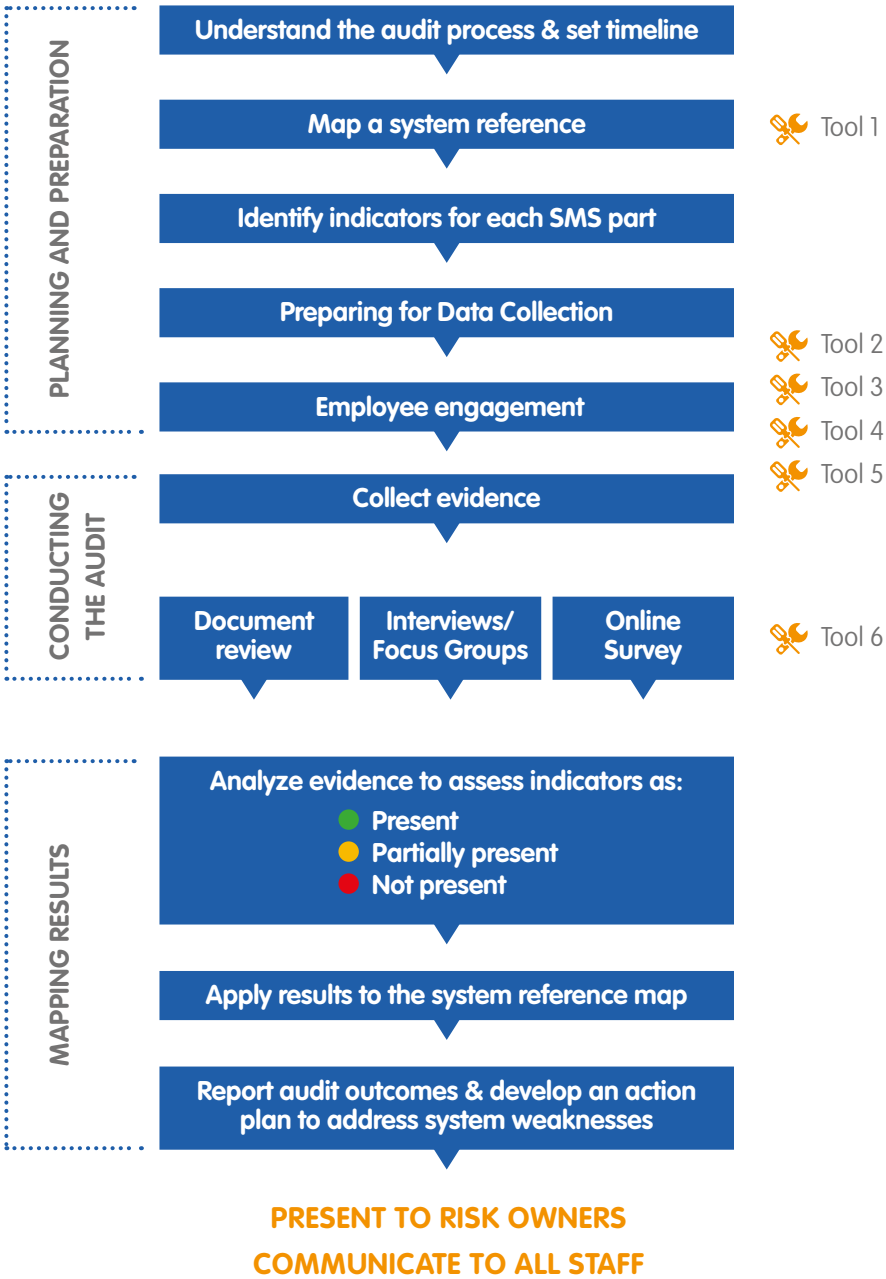
- crucial points and tips are indicated with
- cross-references to other parts of the guide are indicated with
- cross-references to EISF publications, available at www.eisf.eu are indicated with
- hyperlinks are provided for easy navigation

At the end of this guide are a number of practical tools. These are referenced where applicable with the tool icon shown below:

Tool 1: System reference
Tool 2: Document register template
Tool 3: Document review checklist
Tool 4: Developing interview questions
Tool 5: Online survey question example
Tool 6: SMS Audit worksheet template

The tools are also available in editable format from www.eisf.eu
Tools need to be modified to suit each organisation and context.

The SMS audit process



A Planning and preparing for an audit

i. Understand the audit process

Before an audit takes place, it is important to build a common understanding of what constitutes a system. A system may be defined as *'a set of principles or procedures according to which something is done; or an organised scheme or method'*.[3]

In the context of NGO security, part of such a system is the security risk management framework (SMF)[4] that has formed a central part of the aid sector's approach to risk management. In itself the SMF is not a holistic system, but more a sub-system to a broader set of principles and procedures that need to be considered by NGOs when designing and implementing a security management system suitable to their needs.

ii. Set a timeline

It is equally important to recognise that conducting an SMS audit requires an appropriate allocation of time and effort. It is not generally the case that an audit can be conducted in a day. This is especially the case for institutional audits that are looking across the whole organisation where a time allocation of up to two weeks is recommended (excluding any training time).

Smaller country offices may take less time if seeking to audit their local SMS, and not take account of the broader SMS structures. The actual time to conduct an audit will vary and is mostly influenced by availability of key personnel and therefore access to key information.

Tool 1
System Reference

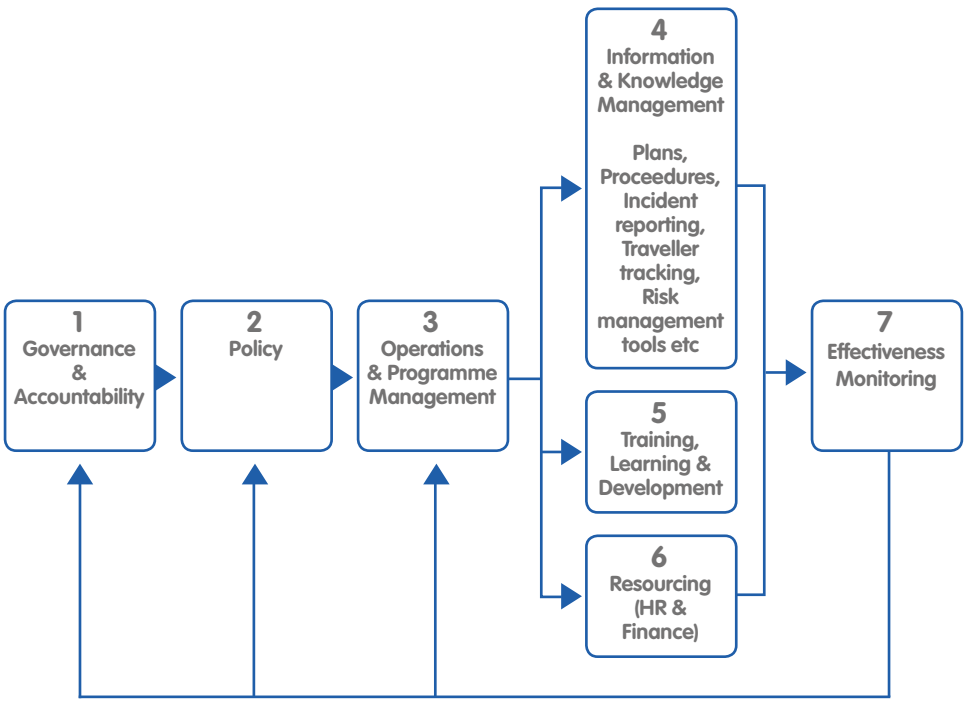
iii. Mapping a system reference

The first step in the audit process is to read this guide, then determine a system reference. This involves mapping the basic system as you understand it. A simple block diagram is a useful way to produce your reference.

This reference will be used throughout the audit to plan, guide and review the outcomes.

A generic system reference is presented in Figure 1 as an example. The reference illustrates seven key parts, arranged in a logical order, considered essential for an NGO SMS. Part 1 begins the system, providing the first set of outputs which drive the subsequent parts. Each part provides inputs to the next. Specific indicators are then applied to the system parts to allow an evidence-based audit to be conducted. This approach allows an examiner to scrutinise each part of the SMS.

Figure 1 **System reference map**



Aid organisations vary widely in almost every conceivable way: size of budgets, workforce, geographic scope, approach to programming, etc. These differences are a result of the principles, values and individual mission objectives of an organisation, and are routinely shaped by their workforce. As a result of these variables, and to reflect individual characteristics and operating nuances of organisations, security management systems will also vary.

Figure 1 above demonstrates the seven security management system parts. These are:

1. Governance & Accountability
2. Policy
3. Operations & Programme Management
4. Information & Knowledge Management
5. Training, Learning & Development
6. Resourcing
7. Effectiveness Monitoring

The diagram illustrates that security management is systematic and logical. Governance structures (Part 1) set the overall guiding principles and explicit risk tolerances of the organisation. This informs and shapes the organisation's risk management policies (Part 2), which in turn are implemented through operations and programme management (Part 3).

Information and knowledge management encapsulate the risk assessment processes (and this is where the Security Management Framework (SMF) sub-system will traditionally fit) (Part 4). The system should include mechanisms to address the workforce's capacity and competence to manage risks, achieved through a training, learning and development strategy (Part 5).

Resourcing (Part 6) is the system part where financial and human resources are determined and communicated. And the system concludes with continual monitoring (Part 7), providing feedback to allow governing and policy matters to be adapted in response to contextual developments.

Each system part is considered essential for an aid organisation security management system, as is the order of the processes. The details within each process will be specific to the organisation and the operating context.

The audit process steps through the system in the same order as the generic reference, beginning with Part 1 and concluding at Part 7. Throughout this guide, reference to system parts remains consistent and applies a simple index to correlate a system part with its specific indicators. For example, Part 1's Governance and Accountability indicators are numbered 1.1, 1.2, 1.3 and 1.4. Part 2's indicators are numbered 2.1, 2.2, 2.3, 2.4 and so on. This will be shown in more detail later in the guide.

iv. Risk Ownership

For some SMS parts, the guide provides two generic sets of indicators. The first set applies to the organisational security management system (marked in **blue** text), and the second to a country or field office (marked in **purple** text). The differences between the two reflect the level of risk ownership, which is the key distinguishing feature between head office and field office management.

Risk ownership is defined as '*the person or entity with the accountability and authority to manage a risk*'.[5] With this definition in mind, auditing an SMS at the institutional level will infer risk owners at the board and executive level. At the field level, risk owners will be the regional and country directors, and their nominated delegates.

Primary risk owners will often be members of the board of trustees, council or similar oversight bodies, in conjunction with the organisation's executive. These are the people who are responsible for putting in place the necessary systems to prevent things from going wrong, and are the people who will ultimately be held accountable if things do go wrong. The level of responsibility is usually delegated down the management line, through head office departments to the field managers and staff.

An SMS first and foremost reflects the risk attitude[6] and risk tolerance[7] of an organisation. It aims to protect the workforce and reputation from harm by identifying and managing foreseeable risks.

System analysis therefore seeks to map and assess the system firstly at the head office or institutional level. When a system is scaled down to regional, country or field offices, it should still reflect that of the organisation as a whole. Local contextual issues will influence how the system is applied, but should have little effect on the system structure.

v. Identify Indicators for each SMS part

To guide an assessment of system structure, indicators are applied to each system part. Indicators are considered against available evidence and assessed as either being:

- Present within the system
- Partially present – Some indication may be found during the audit, but not with sufficient clarity to say for certain that the indicator has been met
- Not present – No evidence can be attributed to the indicators

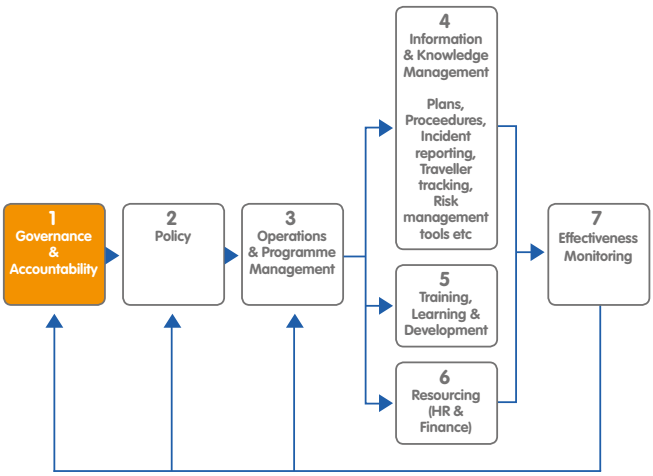
In other words, indicators describe what you are looking for in the body of evidence and/or institutional knowledge about the SMS.

This guide presents four generic indicators against each system part of the reference model. These indicators have been developed over the past years and have been successfully used to audit the SMSs of several international NGOs. The indicators are adapted to various management levels by simply adjusting the level of risk ownership.

As a starting point, this guide recommends using the generic indicators before creating organisation-specific indicators. Naturally some nuancing may be required to align the generic indicators to your organisation, but these changes are likely to be minimal.

Indicators for Part 1: Governance and Accountability

Governance and Accountability is defined as a process of oversight and accountability for security risk management performance. The organisation's primary risk owners will determine and communicate the governance structure.



Tool 6
SMS Audit worksheet template

Indicators:

1.1	A statement of accountability and governance pertaining to safety and security risk management, and the organisation's risk attitude and limits are explicitly communicated by the Board of Trustees / Country Director
1.2	Board of Trustees / Country Director assigns specific safety and security risk management responsibilities to one or more functional parts of the organisation / country office
1.3	Board of Trustees / Country Director officer is explicitly assigned responsibility for governance oversight of safety and security risks for the organisation / country office
1.4	A reporting and accountability process (with defined content and frequency) exists for informing the Board of Trustees / Country Director of safety and security risk issues and organisation / country office performance

See section iv: Risk ownership

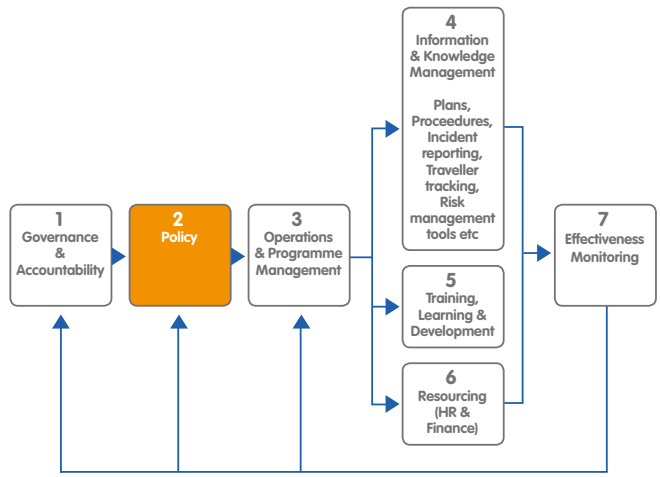
Indicators for Part 2: Policy

While all parts of the system are essential for it to function, policy is particularly important. In the context of the SMS, 'Policy' is defined as communicating the security management position and guiding principles that an NGO has decided to take. This should include the articulation of the role and decisions of board members and executives, and delegation of management responsibilities.

Some NGOs may choose to have policies explicitly at the institutional or head office level. Other NGOs with more decentralised management structures may have a greater emphasis on policies at the field level (e.g. regional or country offices). This guide and the audit methodology may be used for either management structure by adjusting the policy indicators to reflect how the organisation determines and communicates security policy.

Tool 6

SMS Audit worksheet template



Indicators:

2.1	Policies articulate and implement the position and decisions of the Board of Trustees / Country Director on safety and security risk management including the organisation's risk attitudes and limits[8]
2.2	Policy implementation (through plans, procedures and/or guidelines) is appropriate to the local context
2.3	Policies detail employee responsibilities and obligations regarding safety and security and communicate these to all relevant parts of the organisation
2.4	Policy documents are available to employees in all applicable languages

▶ *See section iv: Risk Ownership*

Policy vs. procedure

A common error is the inclusion of detailed procedure in policy documents. Although closely linked, matters of policy are not the same as matters of procedure and should be communicated to the workforce accordingly. Policy is the position taken about a certain issue. Procedure is how the policy is implemented, taking account of contextual influences. In other words, policies lay out key responsibilities and obligations, whereas procedures show the processes used to implement the policy.

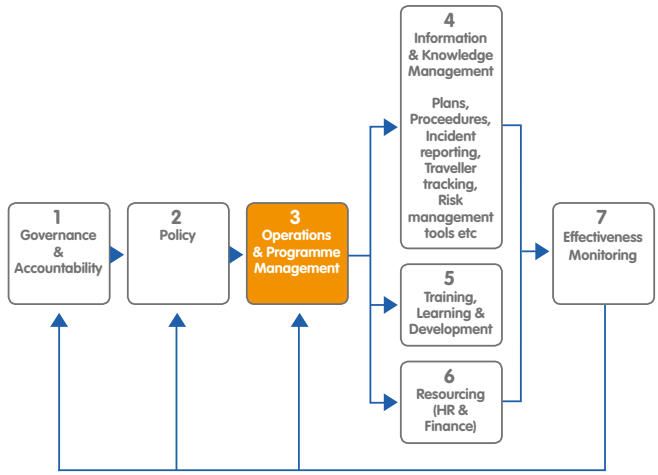
An example of this difference could be expressed as an NGO having a policy that all programme activities include a security risk assessment as part of programme planning. This policy is relevant to all programmes in all countries. How the risk assessments are carried out is a procedural matter that may differ between countries. In a low-risk country the risk assessment may be carried out by the programme manager and reviewed annually. In a higher risk country the assessment may be carried out by specialist security managers and reviewed quarterly. In both cases, the policy remains unchanged when applied.

Tool 6

SMS Audit worksheet template

Indicators for Part 3: Operations & Programme Management

This part of the system aims to mainstream security management. It is the process of integrating security management within operational procedures and programme management cycles.

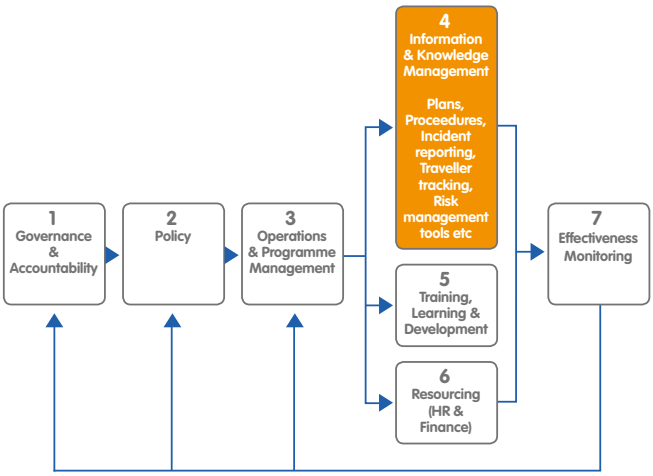


Indicators:

3.1	Security decision-making authority (i.e. risk ownership) is clearly documented in employment contracts, job descriptions and/or personnel performance appraisals
3.2	Security management is actively promoted by managerial employees throughout the organisation, and is demonstrated by communications and reporting trails, workshop events, and/or other internal initiatives
3.3	Context-specific security strategies or approaches are articulated and communicated to all relevant parts of the organisation
3.4	Accountability and compliance processes are documented, with explicit processes for managing breaches of security policies, plans or procedures

Indicators for Part 4: Information & Knowledge Management

Information and knowledge management is where traditional approaches to security management will usually be found, such as the application of a security risk management framework.[9] This system part is described as the body of institutional knowledge (developed by the organisation) to record and communicate the implementation of policy positions. This will include safety and security toolkits (e.g. risk assessment tools) and context-specific plans and procedures and incident reporting mechanisms. It is also where the recording of acceptance or other security strategies would best fit.



Tool 6

SMS Audit worksheet template

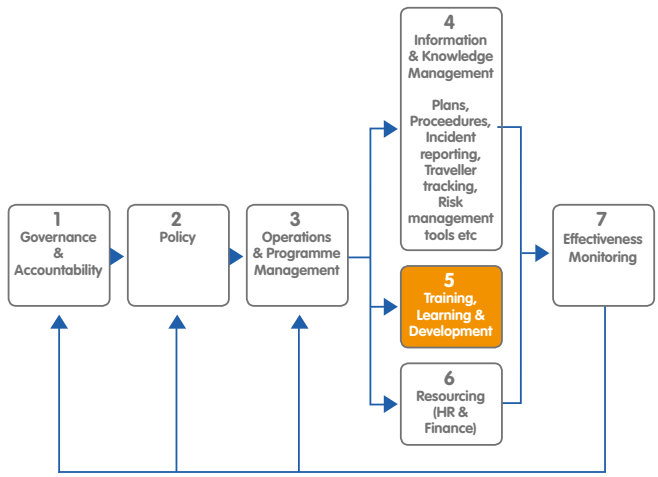
Indicators:

4.1	A functioning safety and security information management system and incident reporting tools are available to all employees
4.2	Organisation actively participates in security management forums or consortia and shares safety and security information with others
4.3	Context-specific safety and security plans and procedures are documented and reflect the organisation's policy position
4.4	Safety and security plans and procedures explicitly state individual and organisational responsibilities and obligations

Indicators for Part 5: Training, Learning & Development

Aid organisations often recognise that their greatest asset is their workforce. Building a competent workforce requires careful recruitment and the implementation of capacity-building strategies to enhance the skills and knowledge required to deliver programme objectives.

Explicit training, learning and development processes ought to be identifiable within an SMS. This system part is defined as a documented strategy that identifies training, learning and development needs for the workforce, and identifies the resources required to ensure these needs can be addressed. This part of the system is an important indicator of an NGO's approach to exercising duty of care and demonstrates a commitment by the employer to develop a competent workforce[10] capable of managing security risks. Security management training strategies are challenging to implement as they need to take account of limited financial resources, be able to reach a dispersed workforce, and cope with staff turnover rates.



Tool 6

SMS Audit worksheet template

Indicators:

5.1	Performance benchmarks are determined and communicated throughout the organisation
5.2	Documented training, learning and development strategy (and/or plan) is accessible to all employees
5.3	Demonstrated management commitment to ensure all employees have access to safety and security training, learning and development opportunities
5.4	Accredited authorities recognise training courses (where available)

Performance Benchmarks

The strategies also need to have the capacity to reach pre-defined performance benchmarks. Performance benchmarking is a useful management tool that provides quantifiable outputs, especially if combined with SMART objectives (Haughey, 2000).

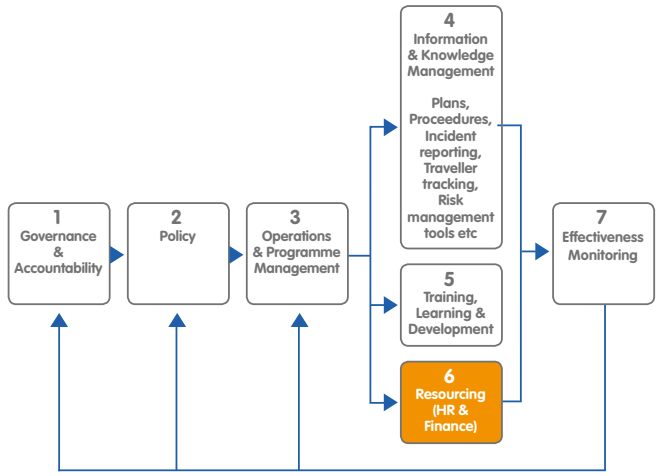
SMART benchmarking means performance objectives are Specific (S), Measurable (M), Achievable (A), Realistic (R), and Timely (T).[11] For example, an organisation may decide that 1 in 5 field staff should be trained in basic first aid, within a defined time, and maintained over a defined period.

Another example would be the benchmark that 1 in 2 staff members working in higher-risk contexts will complete specialist training such as hostile environment awareness training (commonly referred to as HEAT training), again within defined SMART criteria.

Indicators for Part 6: Resourcing

This part of the SMS ensures security management resources are included in programme proposals, planning documents and budgets.

A system cannot function without adequate and prioritised resources.



Tool 6

SMS Audit worksheet template

Indicators:

6.1	Explicit budget lines for security requirements are present in all programme budgets
6.2	Grant requests include explicit budget lines for future security costs and details of how these costs have been estimated
6.3	Budget amounts are deemed sufficient to meet all resource requirements, with clear and logical processes for estimating these amounts
6.4	Insurance policies (Medical, Travel, Crisis, etc.) are in place and the amount of cover is considered adequate to meet potential risk costs

Risk Management Expense Portfolio (RMEP) Tool

Implementing risk management actions will require recruitment and procurement of insurances, equipment, training or specialist services. All of these need to be explicitly communicated to donors and accompanied by sound justification for the expense. The Risk Management Expense Portfolio (RMEP) is a useful tool to ensure this part of the security management system is present and functioning.

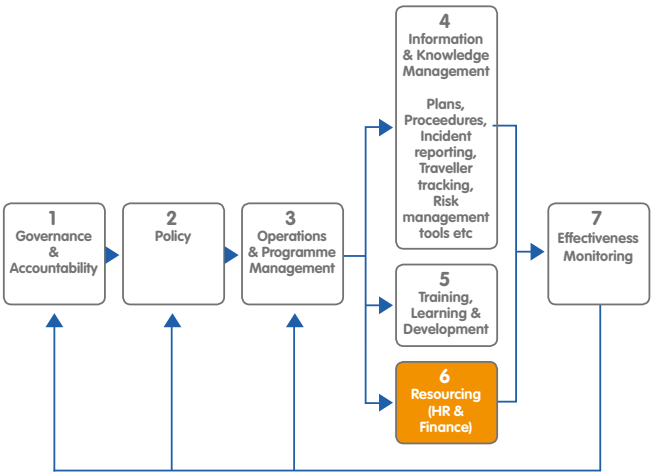
EISF Report: The Cost of Security Risk Management for NGOs

EISF Tool: The Risk Management Expense Portfolio

Indicators for Part 7: Effectiveness Monitoring

This final part of the system is described as a documented monitoring and evaluation process that includes performance management indicators, incident response analysis and recording of lessons learned, frequent review of policies and procedures, and clear reporting responsibilities for evaluating security management system implementation.

The system reference presented in this guide is not a cyclical system. It is designed to allow risk owners to demonstrate a logical process from governance through to programme implementation. Monitoring the system provides a means of internal review, making way for adjustments to the governing mechanisms in response to organisational or contextual changes in the working environment.



Tool 6

SMS Audit worksksheet template

7.1	Employee performance management systems have explicit reference to safety and security responsibilities, and compliance with the organisation's policies
7.2	Persons responsible for monitoring safety and security system implementation and compliance have these responsibilities explicitly stated in their job descriptions
7.3	Outcomes of lessons learned, reviews, post-incident analysis, and audits are actively used to improve the security management system and/or its sub-systems and processes
7.4	Management demonstrate accountability processes are applied for non-compliance

This evidence may be more subjective or anecdotal[13], and therefore more difficult to identify during an audit, but it is equally important to examine and record.

Users of this guide may consider amending the indicators proposed here to align with their organisational needs. Where this occurs it is recommended that the same set of indicators is applied across the organisation to allow for a consistent approach and a valid means of comparing the systems of differing country programmes.

Indicators should focus on the key issues. For this reason, this guide uses only four indicators for each system part, aiming to reflect the most important issues to examine during a system audit.

vi. Preparing for data collection

Preparing for data collection will involve:

- requesting information from the organisation for the document review
- inviting people to participate in interviews and/or focus group discussions
- developing and posting an online survey for the wider workforce

Tool 1

System Reference

Tool 1 provides a baseline of what the audit is actually looking for – the system's design and structure. Once the user has an idea of the basic system, it is time to collect as much information as is available in order to analyse it during the audit. The first (but not only) source of information will be the organisation's records and communications. Information will also be found within the organisation's workforce, and obtained via key informant interviews, focus group discussions and/or online surveys.

What is evidence?

Indicators are intended to be assessed against evidence, which may be tangible, anecdotal or a combination of both. There are different types of evidence. The term 'evidence' is defined as '*the available body of facts or information indicating whether a belief or proposition is true or valid; or signs or indications of something*'[12]

In the context of SMS audits, factual evidence amounts to published records and communications of the NGO and well-established cultural norms within the management processes; things that can be clearly and consistently identified.

However, it is also essential to explore actual behaviour of staff within the organisation. A process or behaviour may exist and function as part of the SMS without being documented. By conducting interviews and focus groups, it is possible to examine how the organisation actually functions in regard to security, collecting evidence that would not otherwise be available for analysis.

vii. Preparing for the document review

Documented evidence sources will often be cross-cutting and provide information for more than one part of the SMS. Keep in mind that the amount of documents can be overwhelming, especially in large, established NGOs. A document register is a useful tool to keep track of what has been requested, received and reviewed. A register will also assist with cross-referencing evidence to system indicators.

Tool 2

Document register template

Tool 3

Document Checklist

viii. Employee engagement

It is crucial when planning and preparing an audit to obtain participation by key employees. An organisation's workforce is often its greatest asset and this collective body of knowledge will be essential when examining the SMS.

It is very important to secure the participation of senior employees, particularly if the employees are risk owners. CEOs and other executive officers and senior managers are critical to the audit process. It may be a challenge in some environments to secure their participation due to their workloads and often busy schedules.

ix. Preparing for key informant interviews

Key informant interviews seek to

1. determine the level of knowledge and understanding of the security management system of the organisation; and
2. capture recommendations from staff on what can be improved.

Key informants should be drawn from the widest possible spectrum of the workforce, with particular attention to risk owners (i.e. those with responsibility and accountability for security management decision-making).

▶ *See section iv: Risk ownership*

Tool 4

Developing interview questions

A typical key informant interview list for an international NGO includes:

- Chief Executive Officer (CEO) or equivalent title
- Heads of Departments or Directorates including international programmes, human resources, finance, audit and risk, and sector-specific functional areas of the organisation (e.g. humanitarian)
- Legal officers
- Programme advisors
- Technical advisors
- Regional and Country Directors

- Field-based programme managers
- Security-specific employees (e.g. security directors, managers or security focal points)

Interview time guide

Time will often limit the number of interviews that can be conducted as part of a review or audit. As a guide, interview times should allow for a minimum 45 minutes for discussions. Should a key informant interview be particularly useful, an additional interview time (on a different day) may be arranged. For planning purposes, approximately six key informant interviews per day are recommended.

Tool 1

System Reference

x. Preparing for focus group discussions

Focus groups are a useful way to engage a number of employees at one time. For this to be effective the groups should be made up of people with a common connection. For example, one focus group could be made up entirely of staff from a particular field office, while another group could be made up of security focal points for a specific country or region.

Tool 4

Developing interview questions

Focus group discussions will follow a similar structure to the interviews. Sessions may begin by introducing the audit process and the system reference produced from Tool 1, then present questions, ensuring they are adjusted to the local context where necessary.

xi. Preparing for online surveys

Online surveys are a useful tool for receiving input from the wider workforce, beyond the key informant interviews and focus groups. These ought to be kept relatively short, focusing on a few key questions directly related to the SMS indicators.

Tool 5

Online survey question example

The purpose of a survey is to test the level of understanding and interpretation of the system across a wide sample group. Keep in mind that time is a precious resource for all staff, particularly those in the field. Surveys should not take longer than 10 to 15 minutes to complete.

Surveys should be developed and posted online during the planning and preparation stage of the audit, providing clear guidance on who should complete the survey and by when. This will allow the survey responses to be available during the time allocated to conducting the audit.

B Conducting the audit

Careful planning and preparation enables the audit to be conducted as effectively and efficiently as possible. It also provides the optimal conditions for accurate audit outcomes. This is why considerable effort is required when applying Section A of this guide.

Conducting the audit involves the following key activities:

- A comprehensive document review
- Carrying out key informant interviews and focus group discussions
- Collecting online survey responses
- Conducting follow up interviews (for clarification, additional information, etc.)

The aim of these activities is to consider the evidence and decide whether SMS indicators are:

- Present within the system
- Partially present, where some indication may be found during the audit, but not with sufficient clarity to say for certain that the condition has been met; or
- Not present, where no formal evidence can be attributed to the indicators

Assessors take an informed decision based on careful analysis of all available information to identify evidence of indicators. Keep detailed notes from all activities as this will assist your analysis and ensure an accurate outcome. Tool 6 provides an example for the audit worksheet, which allows for evidence and notes to be cross-referenced to individual indicators.

Tool 2
Document register template

Tool 3
Document Checklist

Tool 4
Developing interview questions

Tool 5
Online survey question example

Tool 6
SMS Audit worksksheet template

C Mapping results and identifying action items

xii. Mapping the system

Interpreting the results is relatively simple if the indicators have been assessed as recommended above. The evidence suggests indicators are present, partially present or not present. This can be recorded using the common 'traffic light' system:

Green for an indicator assessed as being demonstrated within the organisation's security management system

Amber for those indicators that show some presence but the evidence is more anecdotal

Red for indicators that could not be supported with any recorded evidence.

Assessing SMS Parts

Mapping this way provides a very useful indication of the overall health of the system as each SMS part can be recorded as a table of indicators, with the colour-coded assessment. The below figure shows an example of how this may be recorded.

Figure 2 **Indicator example**

This example of Resourcing indicators shows an assessment of 6.1 and 6.3 not present, 6.2 is partially present, and indicator 6.4 is present in the SMS.

6.1	Explicit budget lines for security requirements are present in all programme budgets
6.2	Grant requests include explicit budget lines for future security costs and details of how these costs have been estimated
6.3	Budget amounts are deemed sufficient to meet all resource requirements, with clear and logical processes for estimating these amounts
6.4	Insurance policies (Medical, Travel, Crisis, etc.) are in place and the amount of cover is considered adequate to meet potential risk costs

Tool 1

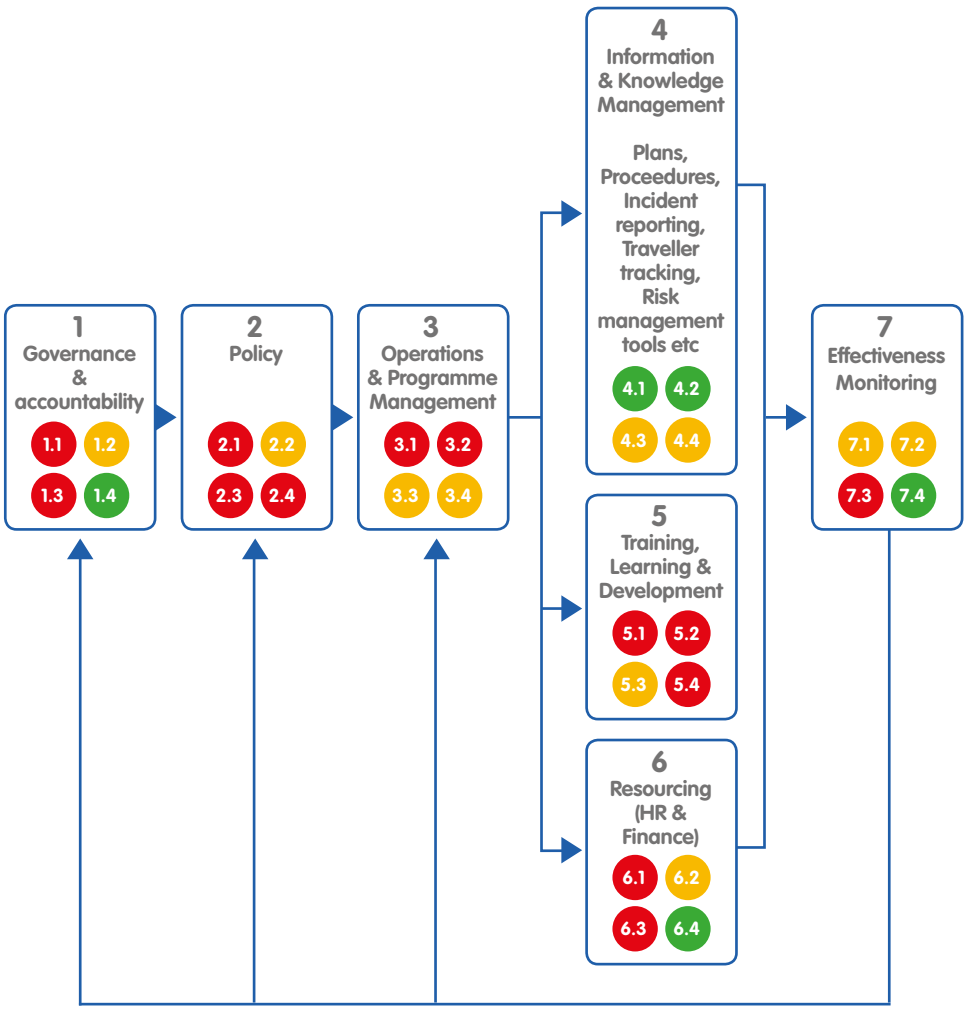
System Reference

Assessing the overall SMS

The overall health of the SMS can be recorded and communicated by transferring each individual indicator assessment to the system reference produced from Tool 1.

Figure 3 **Indicator assessment**

Indicators and their assessed result can be overlaid to their corresponding system part



xiii. Identifying strengths & weaknesses

In simple terms the system's health can be illustrated by the indicator results. The more indicators are present (shown in green in Figure iii above), the more the system may be considered fit-for-purpose. The audit can draw attention to parts of the SMS that demonstrate partial or not present indicators.

Indicators assessed as partial or not present will require further examination. They may indicate that evidence was missed in the initial data collection efforts or, more commonly, they may indicate a system deficiency. Visualizing the system in this way provides direction on where to focus efforts for further review or improvement.

It is important to remember that as each part forms the input to the next, if one part is weak, this will reduce the strength of following parts, degrading the whole system.

For example, Figure (iii) shows an example where policy indicators are weak, and the knock-on effect can be seen throughout the system. Improving the governing and policy mechanisms and processes for the system should in theory strengthen the entire SMS.

xiv. Taking action

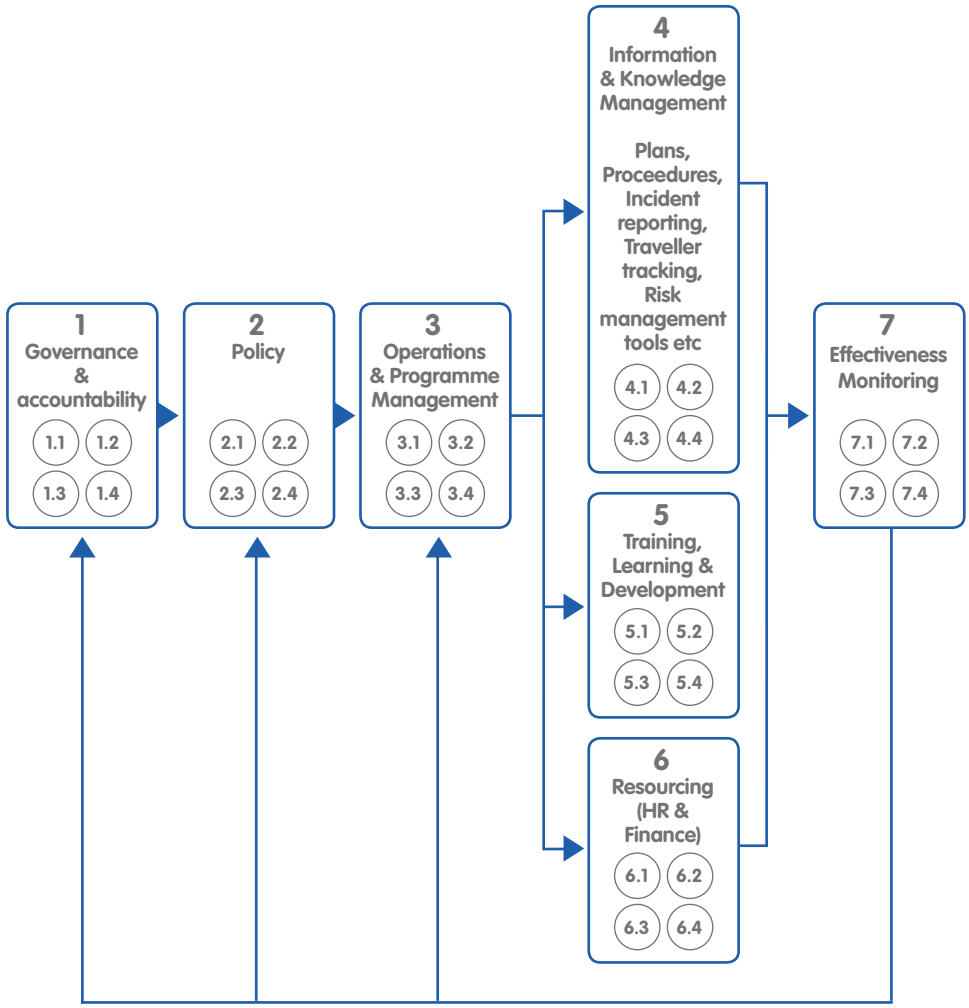
The final step in a security management system audit is to ensure action items are recorded and communicated to risk owners for their action. Where improvements are desired, such as additional resources for training, a plan should be developed with realistic objectives and timeframes.

Ensure the audit results are communicated to those who participated, and also to the wider workforce. Sharing the audit outcomes with staff not only supports transparency but also helps employees understand one of the most important management systems within their organisation.

Tools

Available to download and edit from **www.eisf.eu**

Tool 1
System reference



Tool 2 **Document register template**

Title	Version / Date of Publication	Cross reference to Indicators	Notes

Tool 3 Document review checklist

In preparation for an audit the following documents will provide evidence or useful information about the SMS. The tool separates document types according to the SMS part that is most relevant to the content.

Part 1: Governance & Accountability

- ◯ Minutes of Board and/or Executive meetings when security issues have been an agenda item for discussion and/or decision-making
- ◯ Formal communications from the Board and/or Executive to the workforce regarding security management
- ◯ Formal communications between the Board and/or Executive and donors regarding security management
- ◯ Codes of Conduct for employees and/or others
- ◯ Applicable laws and regulations governing employment, negligence (tort law), health & safety, etc.
- ◯ National and/or international standards used to inform security management
- ◯ Risk management standards (national or international)

Part 2: Policies

- ◯ Security management policies
- ◯ Crisis management policies
- ◯ Other related policies such as whistle-blowing policy
- ◯ Personnel policies
- ◯ Procurement policies
- ◯ Programme management policies
- ◯ Other risk management policies

Part 3: Operations & Programme Management (i.e. plans and procedures)

- ◯ A selection of country-specific security management plans and associated standard operating procedures
- ◯ Security guidelines
- ◯ Other related procedural documents such as handbooks, etc.

Part 4: Information & Knowledge Management

- ◯ Incident reports (for the past 12 months) including 'near miss' reporting
- ◯ Post-incident communications (action items, decisions in response to incidents, etc.)
- ◯ Formal communications regarding any serious or crisis incident (start to finish)
- ◯ Risk assessment tools and guidelines

Part 5: Training & Learning and Development

- ◯ Security management training strategy (global)
- ◯ Security management training plans (regional and country level)
- ◯ Skills & competencies lists or criteria
- ◯ Information guiding the use of external training providers including examples of tenders
- ◯ Internal training programme agendas
- ◯ Employee evaluations of internal or external training

Part 6: Resourcing

- ◯ Security management funding strategy (global)
- ◯ Security budget/s (global)
- ◯ Security management funding plans and budgets (regional and country level)
- ◯ A selection of programme budgets (regional and country level)
- ◯ Job descriptions, employment contracts and terms of references for security managers, security advisors, or security focal points
- ◯ Job descriptions, employment contracts and terms of references for programme directors (regional and country) and programme managers
- ◯ A selection of programme proposals and accompanying budgets for existing programmes (to show how security requirements are included and communicated to donors)
- ◯ A list of present donors and the donor proposal and/or reporting guidelines

Part 7: Monitoring

- ◯ Documented processes for security management performance monitoring and review
- ◯ Formal reports and/or communications throughout the management lines regarding security management performance (organisational)
- ◯ Documented examples of previous security reviews, audits or evaluations

Tool 4 Developing interview questions

Questions for key informant interviews and focus group discussions ought to follow the same logic as your system reference.

Tool 1
System Reference

Begin interviews by introducing the audit process and the system reference produced from Tool 1.

Ask general questions first, then move to context-specific questions as the interview progresses. Examples of key questions include:

- **Do you believe the organisation's approach to security management to be systematic and organised, or ad hoc?**
- **Can you describe the organisation's security management system?**
- **What are the key parts and processes of the system?**
- **Where do you think the key areas for improvement are?**

Other questions specific to the key informant's role may then follow. For example, questions about security responsibilities in job descriptions may be put to human resource managers, or governance questions put to the NGO's executive officers.

Interview questions should directly address the indicators for each part of the SMS. A useful method is to step through the system reference one part at a time, asking key informants for their opinion on whether the indicators are present, partially present or not.

When conducting an institutional audit it is important to consider how the SMS is communicated and understood at both head office level, and at the country office or field level. This will involve asking country office risk owners to discuss the system and their understanding of it in the context of the wider organisation (i.e. institutional level) as well as how this institutional SMS is implemented in practice.

See section iv: Risk ownership

Tool 5 Online survey question example

Security Management Resources

In your opinion are the indicators present in your organisation, partially present or not present? Mark your response for each separate indicator below.

6.1	**Explicit budget lines** for security requirements are present in all programme budgets			
	Present	Partially present	Not present	Don't know
6.2	**Grant requests include** explicit budget lines for future security costs and details of how these costs have been estimated			
	Present	Partially present	Not present	Don't know
6.3	**Budget amounts are deemed sufficient** to meet all resource requirements, with clear and logical processes for estimating these amounts			
	Present	Partially present	Not present	Don't know
6.3	**Insurance policies** (Medical, Travel, Crisis, etc.) are in place and the amount of cover is considered adequate to meet potential risk costs			
	Present	Partially present	Not present	Don't know

Tool 6 SMS Audit worksheet template

Ref	Indicators	Assessment Notes & Evidence
Part 1: Governance & Accountability		
1.1	A statement of accountability and governance pertaining to safety and security risk management, and the organisation's risk attitude and limits are explicitly communicated by the Board of Trustees[16] / Country Director	
1.2	Board of Trustees / Country Director assigns specific safety and security risk management responsibilities to one or more functional parts of the organisation / country office	
1.3	Board of Trustees / Country Director officer is explicitly assigned responsibility for governance oversight of safety and security risks for the organisation / country office	
1.4	A reporting and accountability process (with defined content and frequency) exists for informing the Board of Trustees / Country Director of safety and security risk issues and organisation / country office performance	

Ref	Indicators	Assessment Notes & Evidence
Part 2: Policy		
2.1	Policies articulate and implement the position and decisions of the Board of Trustees / Country Director on safety and security risk management including the organisation's risk attitudes and limits[17]	
2.2	Policy implementation (through plans, procedures and/or guidelines) is appropriate to the local context	
2.3	Policies further detail employee responsibilities and obligations regarding safety and security and communicate these to all relevant parts of the organisation	
2.4	Policy documents are available to employees in all applicable languages	
Part 3: Operations & Programme Management		
3.1	Security decision-making authority (i.e. risk ownership) is clearly documented in employment contracts, job descriptions and personnel performance appraisals	
3.2	Security management is actively promoted by managerial employees throughout the organisation, and is demonstrated by communications and reporting trails, workshop events, and/or other internal initiatives	
3.3	Context-specific security strategies or approaches are articulated and communicated to all relevant parts of the organisation	
3.4	Accountability and compliance processes are documented, with explicit processes for managing breaches of security policies, plans or procedures	

Ref	Indicators	Assessment Notes & Evidence
Part 4: Information & Knowledge Management		
4.1	A functioning safety and security information management system and incident reporting tools are available to all employees	
4.2	Organisation actively participates in security management forums or consortia and shares safety and security information with others	
4.3	Context-specific safety and security plans and procedures are documented and reflect the organisation's policy position	
4.4	Safety and security plans and procedures explicitly state individual and organisational responsibilities and obligations	
Part 5: Training, Learning & Development		
5.1	Performance benchmarks are determined and communicated throughout the organisation	
5.2	Documented training, learning and development strategy and/or plan is accessible to all employees	
5.3	Demonstrated management commitment to ensure all employees have access to safety and security training, learning and development opportunities	
5.4	Accredited authorities recognise training courses (where available)	

Ref	Indicators	Assessment Notes & Evidence
Part 6: Resourcing		
6.1	Explicit budget lines for security requirements are present in all programme budgets	
6.2	Grant requests include explicit budget lines for future security costs and details how these costs have been estimated	
6.3	Budget amounts are deemed sufficient to meet all resource requirements, with clear and logical processes for estimating these amounts	
6.4	Insurance policies (Medical, Travel, Crisis, etc.) are in place and the amount of cover is considered adequate to meet potential risk costs	
Part 7: Effectiveness Monitoring		
7.1	Employee performance management systems have explicit reference to safety and security responsibilities, and compliance with the organisation's policies	
7.2	Persons responsible for monitoring safety and security system implementation and compliance have these responsibilities explicitly stated in their job descriptions	
7.3	Outcomes of lessons learned reviews, post-incident analysis, and audits are actively used to improve the security management system and/or its sub-systems and processes	
7.4	Management demonstrate that accountability processes are applied in cases of non-compliance	

Sources of further information

International Non Governmental Organisations' Accountability Charter, 2005

Stillman, G.B., *NGO Law and Governance: A Resource Book*, ADBI Policy Papers No. 11, 2006

Antares Foundation, *Managing Stress in Humanitarian Work: A Systems Approach to Risk Reduction*, 2008

Center for Safety & Development (CSD), *CSD Matrix & NGO Security Quick Scan*, 2012

K. Micheni, *Christian Aid MOSS Compliance Checklist*

HAP International, *2010 HAP Standard in Accountability and Quality Management*

P. Daudin & M. Merkelbach, *From Security Management to Risk Management – Critical Reflections on Aid Agency Security Management and the ISO Risk Management Guidelines*, Security Management Initiative, 2011

International Standards Organisation, ISO 31000:2009 *Risk Management Principles and Guidelines*, 2009

International Standards Organisation, ISO Guide 73 *Risk Management Vocabulary*, 2009

People in Aid, Code of Good Practice in the Management and Support of Aid Personnel, 2003

C. Finucane & M. Merkelbach, *Irish Aid Guidelines for NGO Professional Safety & Security Risk Management*, Dept. of Foreign Affairs and Trade, Government of Ireland, 2013

Glossary

This guide uses several terms from International Standard ISO 31000:2009 Risk Management – Principles and Guidelines. Some definitions may be modified to add clarity to the aid sector context

Mission objectives The stated aims and intended outcomes of a given activity.

Risk The effect of uncertainty on achieving objects. This includes the chance of a threat affecting the organisation or its personnel. Risk is subjective and from the point of view of the assessor.

Risk attitude The organisation's approach to assess and eventually pursue, retain, take or turn away from risk.

Risk management The coordinated activities to direct and control an organisation with regard to risk.

Risk owner The person or entity with the accountability and authority to manage a risk.

Risk treatment The process to modify risk. This may include activities to reduce the likelihood and/or impact of a threat through risk mitigation procedures.

Risk tolerance The organisation's [or risk owner's] readiness to bear [accept] the risk in order to achieve objectives.

Safety The state of being protected from foreseeable harm or injury.[18]

Security The state of being free from foreseeable danger.[19] The notion of 'safety and security' is described as a state of being free from, or protected against, harm, injury, loss or foreseeable dangers.

System 1) a set of things working together as parts of a mechanism or an interconnecting network; (2) a set of principles or procedures according to which something is done; an organised scheme or method.[20]

References

1 Kemp & Merkelbach, SMI Policy Paper, *Can you get sued? Legal liability of international humanitarian aid organisations towards their staff*, 2011

2 International Standards Organisation, ISO 31000:2009 *Risk Management Principles and Guidelines*, 2009 & ISO Guide 73 *Risk Management Vocabulary*, 2009

3 Oxford Dictionary of English, 2011

4 Good Practice Review No.8, Operational Security Management in Violent Environments, 2010, p.9

5 International Standards Organisation, ISO 31000:2009 *Risk Management Principles and Guidelines*, 2009 & ISO Guide 73 *Risk Management Vocabulary*, 2009

6 Risk attitude describes an organisation's approach to pursue or avoid risks (Definition derived from ISO31000/2009)

7 Risk tolerance refers to the risk owner's readiness to accept risks in order to achieve an objective (Definition derived from ISO31000/2009)

8 It is important to note that risk attitudes and limits should apply consistently and equally throughout the management line as these are institutional governing mechanisms

9 Good Practice Review No.8, Operational Security Management in Violent Environments, 2010, p.9

10 For more information on developing a competent workforce refer to *Irish Aid Guidelines for NGO Professional Safety & Security Risk Management*, Standard 4, p.14 (2013)

11 Duncan Haughey, http://www.projectsmart.co.uk/smart-goals.html viewed 5 August 2013, Project Smart, 2000

12 Oxford Dictionary of English, 2011

13 Based on personal accounts rather than facts anecdotal evidence can be less reliable

14 Oxford Dictionary of English, 2011

15 Based on personal accounts rather than facts anecdotal evidence can be less reliable

16 This text uses the term 'Board of Trustees' to describe the governing body of an NGO. Some NGOs may use different terms when referring to this governing body (e.g. Council, Board, Commissioners, etc.)

17 It is important to note that risk attitudes and limits should apply consistently and equally throughout the management line as these are institutional governing mechanisms

18 Adapted from the New Oxford American Dictionary, 2005

19 Adapted from the New Oxford American Dictionary, 2005

20 Oxford Dictionary of English, 2011

Other EISF publications

Briefing Papers

Security Management and Capacity Development: International agencies working with local partners
December 2012
EISF Secretariat, Iesha Singh

Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management
September 2012 (English)
September 2013 (Spanish)
Christine Persaud (author), Hye Jin Zumkehr (ed.)

Engaging Private Security Providers: A Guideline for Non-Governmental Organisations
December 2011
Max Glaser (author), supported by the EISF Secretariat (eds.)

Abduction Management
May 2010
Pete Buth (author), supportedby the EISF Secretariat (eds.)

Crisis Management of Critical Incidents
April 2010
Pete Buth (author), supported by the EISF Secretariat (eds.)

The Information Management Challenge
March 2010
Robert Ayre (author), supported by the EISF Secretariat (eds.)

Reports

The Cost of Security Risk Management for NGOs
February 2013
Christopher Finucane (author) Hye Jin Zumkehr (EISF Researcher), EISF Secretariat (eds.)

Risk Thresholds in Humanitarian Assistance
October 2010
Madeleine Kingston and Oliver Behn (EISF)

Joint NGO Safety and Security Training
January 2010
Madeleine Kingston (author), supported by the EISF Training Working Group

Humanitarian Risk Initiatives: 2009 Index Report
December 2009
Christopher Finucane (author), Madeleine Kingston (editor)

Articles

Incident Statistics in Aid Worker Safety and Security Management: Using and Producing them
March 2012
Koenraad van Brabant (author)

Managing Aid Agency Security in an Evolving World: The Larger Challenge
December 2010
Koenraad Van Brabant (author)

Whose risk is it anyway? Linking Operational Risk Thresholds and Organisational Risk Management (in Humanitarian Exchange 47)
June 2010
Oliver Behn and Madeleine Kingston (authors)

Risk Transfer through Hardening Mentalities?
November 2009
Oliver Behn and Madeleine Kingston (authors)

Guides

What's the message: Communication and media management in a crisis
September 2013
Sara Davidson (author),
Ellie French, EISF Secretariat (ed.)

Family First: Liaison and support during a crisis
February 2013
Sara Davidson (author),
Ellie French, EISF Secretariat (ed.)

Office Closure
February 2013
Safer Edge (authors), Ellie French and Lisa Reilly, EISF Secretariat (eds).

If you are interested in contributing to upcoming research projects or want to suggest topics for future research please contact **eisf-research@eisf.eu**

eisf

EISF Executive Director
T: +44 (0) 203 195 1360
M: +44 (0) 77 6099 2239
eisf-director@eisf.eu

EISF Research Advisor
T: +44 (0) 203 195 1362
M: +44 (0) 77 6099 2240
eisf-research@eisf.eu

www.eisf.eu

First published / September 2013

NRC NORWEGIAN REFUGEE COUNCIL