This NGO Security Training Research and Reference Curriculum targets humanitarian and development NGOs that operate in various security risk contexts all over the world. It provides a baseline of good practice for NGO security training that must be informed by and adapted to each organisation, their needs, profile of management, operations, working environments and personnel.

NGO Safety and Security Training Project

How to Create Effective Security Training for NGOs

Researcher and Author: Christine Persaud

Research Produced by the European Interagency Security Forum (EISF) and InterAction

2014

Acknowledgements

InterAction, EISF and the author are very grateful to the members of the NGO Security Training Project Steering Committee who provided guidance and feedback throughout the research process: Rafael Khusnutdinov (Save the Children), Tim McAtee (International Medical Corps), Rebekka Meissner (Medair), Noemi Munoz (Handicap International), Paul Muniz (ADRA), Ira Russ (EDC) and Barry Steyn (CARE International).

We also would like to extend our gratitude to the 55 individuals who participated as key informants through interviews, the 41 individuals who participated in the Geneva, Dublin and Washington, D.C. working sessions, and the 65 field and headquarters staffers from InterAction and EISF member organizations who participated in the online questionnaires and surveys.

The author would like to thank InterAction and EISF for the opportunity of contributing to this project, particularly InterAction Security Director Laky Pissalidis for his significant support and dedication to the project and EISF Executive Coordinator Lisa Reilly for her extensive knowledge and support and InterAction Editor Katherine Ward. Also special thanks to Jane Barry, Phil Candy, Elizabeth Detwiler, Ellie French, Lucy Hodgson, Robert MacPherson, Joel Mcnamara, Ruth Quinn, Lauren Rajczak, Emmanuel Rinck, Kamran Saeed and Ian Woodmansey.

About the Author

Christine Persaud has been working in humanitarian assistance since 1999 and began as a project coordinator for various NGOs including Médecins Sans Frontières. In 2003, she was approached to conduct security assessments and security trainings until she became the security manager for CARE Canada in 2006. She then decided to continue as an independent consultant in safety and security and in emergency assessments and trainings to counter balance her artistic projects. She has been the principal writer for several major agencies' global security policies, principles, training materials, country-specific security planning and guidance documents, crisis management plans and hostage incident management policies and procedures. She has also worked for the Canadian International Development Agency as a senior program officer in the Humanitarian Assistance Directorate. Currently, she is the security advisor for the Canadian Red Cross on a term contract.

Disclaimer

Preface

The idea for this project was conceived in 2011 during a discussion between InterAction Security Advisory Group co-chairs Ike Evans (Child Fund), Norman Sheehan (AED), Lisa Reilly (EISF) and Laky Pissalidis (InterAction). We felt that selecting appropriate security training was a key challenge for our NGO community. A solution that we discussed was to audit the existing courses and identify the most appropriate ones. However, we soon realized that we did not have a standard by which to judge any security training. What we did have was the InterAction/OFDA "Safety in Insecure Environments," NGO security training course that was developed approximately 16 years ago by InterAction and RedR through a grant from USAID's Office of Foreign Disaster Assistance (OFDA).

Although the course remains relevant today and provides a strong foundation for NGO security practices, it is outdated. It does not address the current and emerging operational realities. For example, in today's world, security actors include private security services providers operating in the humanitarian area; they offer products such as security training, while not necessarily understanding the complexities involved in the humanitarian working environment. The lack of appreciation for those complexities often results in security trainings that are not appropriate for NGOS. In addition, NGO security management structures have become increasingly complex, and those complexities, as well as approaches that some NGOs have instituted over the intervening years, are not reflected in the original security curriculum. For example, the notion of risk transfer and the Saving Lives Together initiative did not exist 16 years ago. With today's multitude of NGOs, all with differing mandates, capacity, attitudes, and structures requiring training, there is a need for stronger consistency and guidance concerning NGO safety and security training relevant to today's humanitarian sector.

The intent of this project was to research current safety and security training practices by consulting the NGO security community. We also wanted to assure that NGO security training addresses the sector's security and operational requirements for delivering effective assistance. NGO security has unique principles and features that are not common in the private or government sectors and NGO security training must reflect these unique factors. Our goal became to create a reference curriculum that NGOs could use as a tool when they develop or refine security training courses for their own use. Two question guided this project: (1) What should an NGO security training curriculum cover?; and (2) How should it be delivered?

As a result, this document provides a comprehensive package of components that humanitarian and development organizations can use as guidance when they are developing, refining and implement security trainings for their own use. The material provided here cover identifying training needs and gaps, developing a security training framework. They also provide a security training reference curriculum, which identifies core and elective topics to meet today's security needs. There is also information on training methods and guidance on how to choose the right provider.

Laky Pissalidis
InterAction Security Director

Lisa Reilly
Executive Coordinator – European Interagency Security Forum

Table of Contents

EXECUTIVE SUMMARY

About the Project

Late in the 1990s, InterAction, along with RedR and USAID's Office of Foreign Disaster Assistance (OFDA), developed a curriculum and course materials for safety and security training based on the operational realities that NGOs routinely faced in the field. These materials quickly became the basis of NGO security training, and their focus was on the safety and security of humanitarian and development staff, organizations' assets and operations.

It has been over 16 years since the development of these materials and some parts are no longer up to date. Nonetheless, they still highlight relevant core topics based on the principles of humanitarian aid that remain at the heart of NGO security management today.

Several issues have surfaced over the ensuing years. For example, the emergence of security training providers from outside the NGO community that have started developing their own security training curricula without a solid understanding of the particular needs and perspectives of the NGO sector.

Another issue is that many NGOs do not know how to select an effective training curriculum for their staff, but they need such training to support their security frameworks and fulfill their duty of care. As a result, these organizations may select courses that are at best minimally relevant, and, at worst, are detrimental not only to their own safety, but also to the safety of the NGO community as a whole.

This project was created to address these realities by producing an updated curriculum and supporting materials. Importantly, the voice of NGOs has been at the heart of the effort, which included extensive consultations with NGO security and program professionals through interviews, surveys and working sessions. The project also studied existing training courses, identified current trends and issues in NGO security and operational management, and compared them to the existing InterAction/RedR/OFDA course.

This report and curriculum present current best practices for NGO security training and take into account the fact that each NGO has its own structural, financial, operational and capacity-related realities that will affect how it structures such training for its staff. As users navigate the process of creating the right training products for their organization, the materials included here can help them:

- Assess training needs and choose the best ways to meet those needs.
- Design their training courses and determine which topics to include.
- Select the best ways to present the training materials.
- Effectively select and communicate with internal and external trainers to maximize learning results.
- Educate others about the importance of security training to the organization's overall operational success.

This project's focus is on the safety and security of humanitarian and development personnel, not the security of beneficiaries. While there are obviously links between the security of humanitarian and development personnel and beneficiary protection, that topic is outside the scope of this project. For the purpose of this document "safety" is implied whenever referring to security.

The surveys, questionnaires and interviews yielded extensive data, much of which reflected participants' personal experiences. These data were then confirmed through cross-referencing with trainers and key staff as well as numerous print and online materials. Given the variables, time and geographic constraints, an important diversity (geographic, organizational, gender, job positions) was captured. Several important and open consultative opportunities also fed into the research process. These sources support the main findings and development of the reference curriculum for NGO security training provided in Section B below.

What This Document Provides

This document has three sections:

Section A: Project Report
Section B: Reference Curriculum
Section C: Guidance Tools

The sections are interrelated and reflect current best practices. They are provided to help organizations assess their training needs, develop an appropriate security training strategy and monitor the effectiveness of that training.

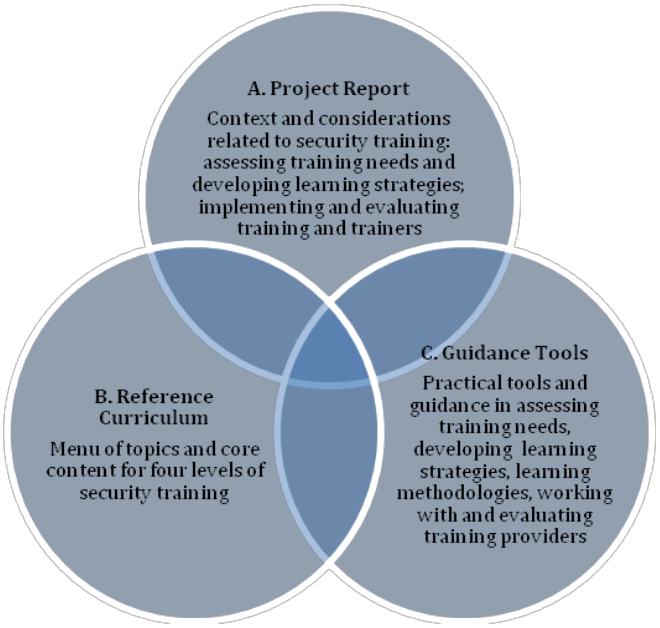


Figure: Guide for Security Training Strategy Development

Section A is a narrative project report that provides some key findings from the research and outreach to NGO community members. It also offers a framework for how to approach security training, bearing in mind practical and good practice considerations. It also offers recommendations to improve security training sector-wide.

Section B presents the NGO Security Training Reference Curriculum, developed based on findings from the research. It should be used in conjunction with the narrative report in Section A. The curriculum is divided into four training levels reflecting the fact that different staff members have different training needs:

LEVEL I **Personal Security:** for all agency staff working in or travelling to various security risk environments.

LEVEL II **Operational Security:** for those with day-to-day responsibilities for implementing security such as security focal points, drivers, guards and program staff.

LEVEL III **Security Management:** for those with a decision-making role in developing and implementing risk management and policy, such as members of the global security management team and regional and country management.

LEVEL IV **Global Strategic Security:** for headquarters staff with decision-making authority and responsibilities related to the organization's legal duty of care and/or its global operations. This includes those involved in corporate governance (e.g., board members, CEOs and presidents), and headquarters-level technical senior management (e.g., security directors, human resources, operations, administration, finance and communications).

Section C provides guidance tools that compliment Sections A and B. These include guidance on: assessing security training needs; learning and development strategies; learning methodologies; selecting and working with training providers; and evaluating the effectiveness of training.

Methodology and Sources

Methodology. The research methodology of this project is grounded in some of our sector's most important principles: consultation, open participatory approaches, and comparing information from across the humanitarian and development community. To maximize community input, interviews, surveys and focus groups discussions were used to garner insights from practitioners and other experts. Extensive research on existing training materials and operational realities and practices was also conducted. The materials that have been produced for this project are designed to be reviewed and updated regularly (see the report recommendations at end of section A).

Sources. This project mostly reflects insights from qualitative data, mainly experiential references and case studies from a wide range of information resources, including: background research; interviews; online surveys; working sessions; a task force of experienced volunteers from both InterAction and the European Interagency Security Forum' s memberships who provided feedback and helped revise drafts; and the experience of the author and both project managers (the InterAction security director and the EISF executive coordinator).

Background research. The project reflects extensive research on existing training materials and practices in the NGO community (see Annex 1 References). Resources reviewed include, for example:

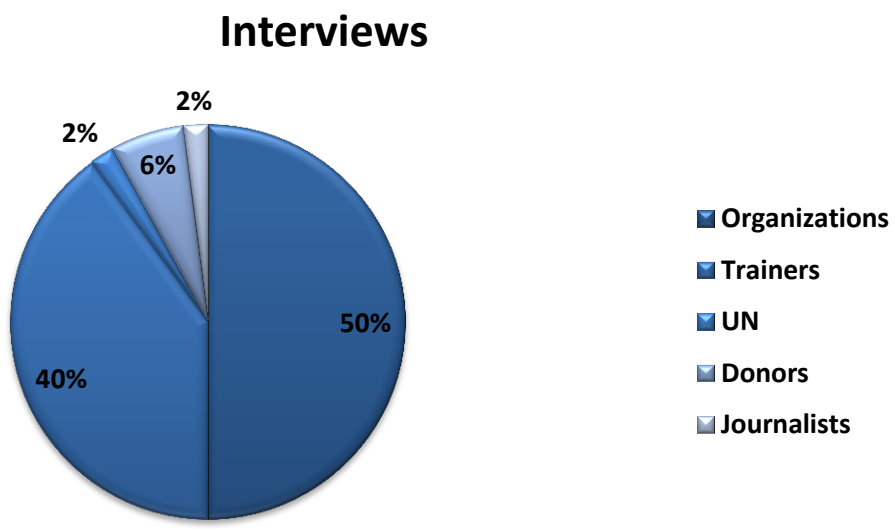
- The original InterAction/RedR/OFDA curriculum;
- ECHO training materials;
- Training materials developed by NGOs, private security trainers, independent consultants and training organizations;
- Job descriptions for relevant headquarters positions, regional advisors and security officers;
- Instructional systems design and learning and development approaches;
- Learning methods from NGOs and other sectors; and

- Research and literature on current operational practices and realities.

This research provided insights into current practices related to security training, curriculum development, and relevant humanitarian and development trends and issues.

The project also investigated innovative practices that groups outside the NGO security sector are using to improve their trainings. Examples of practices reviewed include the Canadian wilderness first aid sector curriculum, the security training approaches used by women human rights defenders, and corporate approaches to staff training.

Interviews. The project also involved over 55 interviews (each approximately 1-2 hours in duration) by phone, Skype and in person. These interviews involved a diverse range of specialists in NGO security, program management, specific sectors and capacity building (training), including personnel at headquarters and in the field.

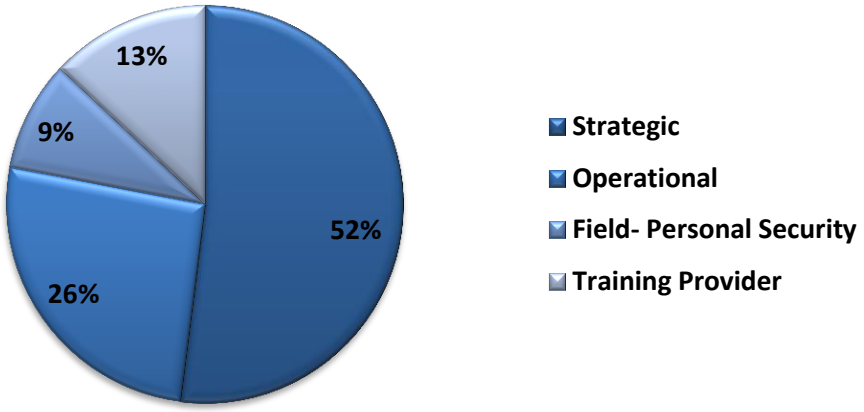


Online surveys. Four surveys were specifically developed to capture the levels of security management and personal security within the scope of this project (see Section B for details). These four surveys targeted:

- Security trainers (external and internal security training providers ranging from individuals to private companies and not-for-profit training organizations);
- Headquarters-level security and HR personnel;
- Country-level management and security focal points; and
- Field staff.

Each survey had an average of 35 multiple, ranking and open-ended questions to help identify and prioritize which topics to include in each training level. The surveys also elicited information about prioritizing training, selecting training and providers, and the effectiveness of various training methods.

Survey Respondents



Facilitated working sessions. Three working sessions, held at different points in the research process, provided opportunities for feedback from trainers and representatives from NGOs, the UN and donors. Held in Geneva, Dublin and Washington, D.C., these sessions allowed participants and the project team to discuss and shape the security training objectives and reference curriculum content while they were being developed.

Additional resources. The Security Training Steering Group, a committee of volunteers from both InterAction's and the European Interagency Security Forum's memberships, was instrumental in revising drafts and providing other extremely useful insights. In addition, the project has relied on and benefitted from the author's insights and expertise.

This page is intentionally blank.

SECTION A

NGO Security Training Project Report

NGO Safety and Security Training Project

2014

This page is intentionally blank.

SECTION A – Project Report

1. Historical Overview and Current Trends in NGO Security Training

Past projects. In 1995, the U.S. Agency for International Development's Office of Foreign Disaster Assistance (OFDA) provided InterAction with a grant to assemble a working group to develop a curriculum for nongovernmental organization (NGO) security training courses.

With this grant, the advisory working group produced two main products:

1. A security training curriculum involving a series of topics to be used by organizations to design their own courses; and
2. Two, one-week pilot training courses in January and September of 1998.

The course curriculum was then made available for others to build upon in developing their own security training resources. RedR UK adopted the curriculum as the basis for the security courses it offers to other NGOs. Other organizations also used the materials to develop their own training programs.

The project became the basis of a new field: NGO security. It provided a framework, language and forum for the dialogue that has shaped the NGO community's approach to security training and management. As such it has led to many developments and been a springboard for other products including: Good Practice Review 8 (GRP8) "Operational Security Management in Violent Environments" by Koenraad Van Brabant, published in 2000 and revised in 2010; and the security materials (report, generic guide to security management and training materials) developed by the European Community Humanitarian Office (ECHO) in 2004 and made freely available to all organizations.

Changes in the landscape. NGO security risk management has become more sophisticated in structures and resources. There are more dedicated headquarters, regional and field positions for security. Training has been enhanced to reflect the needs of governance, operational security management and personal security. Interagency security forums and opportunities for collaboration have been created. Funding has been prioritized; and, legal duty of care, depending on the organizational and/or geographic culture, has become (unfortunately) a primary motivator in achieving better security management.

Despite this significant progress, there has also been a deviation from the guiding principles of what had been developed as a holistic approach to security risk management by the InterAction working group mentioned above. Initially its proposed approach, although inspired by military, corporate and diplomatic security, was tailored to respond to NGO culture. This tailored approach was based on: the interdependency of relationships; agency and situation-specific approaches; analytical skills and decision making; risk reduction strategies; strategy-based security planning; and multidisciplinary approaches to security.

The operating landscape has also changed drastically post 9-11, with changes in perceptions about the neutrality of relief and development providers, access challenges, a huge increase in the number of development and humanitarian actors, and expansions of organizational mandates that sometimes create new security challenges. Operating environments have also become increasingly complex and are too often marked by crime and terrorism that affect both aid workers and beneficiaries.

2. Key Findings

The interviews and survey responses provided insights on current NGO security training practices. They also highlighted important gaps in NGO security training needs. The following is a summary of the key findings. Certain findings contain cross-references to guidance tools provided in Section C that can help users as they design their own training programs. Further discussion and recommendations are provided below in *3 - Creating an Organization's Security Training Framework.*

ENSURING RESOURCES AND SUPPORT

2.1 Making the case for security training

The vast majority of NGOs understand the importance of security training. But in practice, cost and access still remain important factors in how training is implemented and sustained. According to survey and interview responses, organizations use the following strategies to secure funding and build support:

- Identifying security training as a priority linked with the notion of duty of care;
- Including training in project budgets or global accruals;
- Including training in the organization's global and/or office learning and development strategy.

> *"It is all down to 'duty of care' for your staff. More and more, litigation is a concern even for aid agencies. Insurance providers are also making it a cheaper option for agencies to send staff on security/safety trainings. It is a more cost effective way of developing staff awareness and giving them tools to assist the organization to deliver its programs in a more safe and secure way. Understanding the risks and threats to organizations and staff is paramount to deciding your program implementation strategy. Training is one way to ensure all staff understand their responsibilities to themselves, colleagues and the agency." – Survey Respondent, Training Provider*

2.2 Building organizational support through integration

Survey responses ranked the following measures as the most important ways to build an effective and well-supported security training program:

- Offering safety and security training regularly (especially if the training is in-house because this helps increase access).
- Having additional access to funding and resources for training.
- Including security training in learning and development strategies.
- Including security training within personal learning plans and performance appraisals.

WHAT TO OFFER

2.3 How NGOs decide what to provide: operational realities

Survey and interview respondents cited the following factors as the most important in determining what training to provide (most important listed first):

- Cost;
- Location and timing;
- Relevance of content to the trainees' environmental and organizational context; and
- Reputation of the trainer and/or the organization providing the training.

The importance of cost was cited as paramount, and some respondents said cost has limited the provision of security training both at field and HQ levels. A number of respondents said training was often last minute, especially at the field level, meaning that it was responding to immediate circumstances.

Respondents also indicated that the following factors can help organizations decide which training to choose:

- Managing cost by sharing courses with other like-minded NGOs (alleviating cost and logistics) and/or additional support by donors;
- Proximity to field and headquarters locations;
- Contextualization of courses (geographic and institutional);
- Having more information about content that explains the courses offered; and
- Having more information about external training providers and facilitators.

However, as will be discussed later, a more concerted effort to assess staff training needs is critically needed. Both the organization and trainers (internal or external) must allocate more time to assess the specific training needs of staff to improve their performance and stay safer. Assessments also need to do a better job of identifying training priorities and changes in the operating environment.

2.4 The Tension Around The Hard Security Approach To Training

Respondents expressed a recurring concern about what is currently referred to as "hostile environment training"(HET). HET training (or variants such as HEAT and HEIST) derives from a predominantly military approach and uses terminology for personal security training for severe security risk situations.

Specific HET trainings vary in intensity and focus. There are different levels of HET training and the methods can vary from providing safe simulations to physically and psychologically challenging participants to use of live ammunition in training exercises. The majority of interviewees agree that simulations exercises can be very effective in preparing staff to react appropriately to some security

situations (ex: crossfire). However, interviewees and survey respondents also had concerns about how "HET" type trainings are run and believed that, if not facilitated effectively, they could be physically, psychologically and emotionally harmful to participants.

> *"…. from the PSCs [personal security companies] and risk management companies: I think it is the mindset and the vocabulary used. The UN also in a certain way is guilty of this practice. I feel that in general these sort of trainings put the trainer in a very confrontational way, and go away from our ideal of being close to the community. It really focuses on security at all costs, we have to defend ourselves, rather than try to be accepted and truly accepted. It looks more at techniques and tactics to be protected rather than strategies to be able to operate in dangerous environment. It is too self-centered, I am afraid, too technical, not political. And that is a problem in general in security management training; they are often provided by people who are former police and military, and I feel that there is too much emphasis on technical aspect, not enough value on the political understanding, on the political analysis ... copy paste from one context to another, and I think that is wrong." – Interview Respondent, Independent Security Consultant and Trainer*

Nonetheless, input from respondents and other research findings indicate that there is a perceived need for more than advanced personal security training for specific, severe security risk working situations. For the purposes of this project, the third level (HET equivalent) of personal security is referred to as *Personal Security for Violent Environments* (see Level IC in Section B below). This provides a conceptual shift from the survival and hard technical security focus of a HET training to the notion of personal security. The emphasis in Level IC is on helping trainees strengthen their ability to better assess and guide prevention and response strategies depending on the fluidity of possible security scenarios in violent and complex security risk environments. When there is a need for personal security for violent environments using HET or similar methods, it is important to make sure the training is presented in a way that is physically and psychologically safe (see Guidance Tool C).

> *"The risk of traumatization during training is an interesting area. For some people, simulations can be experienced as every bit as terrifying as the real thing. At [our organization] we have seen clients for counseling who have been overwhelmed during hostile environments [training] exercises. And the simple truth is, I don't believe that people learn well if they're terrified out of their wits. The fight/flight/freeze system kicks in and the part of the brain capable of absorbing information shuts down. Having said that, exposure to a certain amount of controlled anxiety can be very helpful in prepping people for the demands of the field, so it becomes a question of balance." – Interview Respondent*

A number of respondents expressed an overall concern about the frequency with which NGOs now turn to military and former military trainers:

> *"In the bigger picture, we have outsourced security training and management and believe military and former military know best. Have smart people that do good work and know the context and national staff really know the context. Stop thinking that someone else can teach you about security – abdication of that responsibility and we feed into it. There is too much leaching from the formal security sector, lack of understanding what it means to be a humanitarian worker." – Interview Respondent*

2.5 Content gaps

Survey respondents and interviewees consistently mentioned certain topics that are currently not part of security training and need to be added:

- Soft skills such as leadership, analysis, negotiating access, conflict resolution, and working with an acceptance approach to security;
- Gender and other cultural and personal considerations;
- First aid; and
- Transfer of risk.

Soft Skills. Respondents' comments on soft skills reflect the need to think of security as more of a social science than a precise science. This includes reflecting on the human aspect of security beyond the pure technical (as has been the tendency in recent years). The importance of teaching, learning and practicing soft skills and ensuing efforts to increase attention to soft skills, correlates with deeper mainstreaming issues concerning security buy-in, implementation and compliance. Skills in persuasion and negotiating, the art of leadership and communication are important, as is paying attention to personal behavior and the common sense of individuals and staff teams, dynamics and cohesion.

Gender, Cultural and Personal Considerations. For personal security, respondents felt that more attention is needed to helping individuals develop self, cultural and gender awareness (linked to security).

For example, many respondents noted that gender has been missing from existing curricula. Often considered an elective topic (mostly by male security personnel), gender and gender-based violence awareness could benefit from being built into all levels of security training as it pertains to programming and to staff members' work and domestic spheres.

> *"One [way] would be to emphasize the problem of sexual assault – often this is not covered very well, and can happen in essentially any environment, both hostile and non-hostile. It shouldn't (only) be thought of in terms of rape by armed groups, but as a daily risk faced by people." – Survey Respondent*

First Aid. First aid has been inconsistently understood and provided, and many respondents called for more first aid training. Concerns about how this essential training is currently provided include: the use of uncertified instructors; the relevancy of the type of first aid training (e.g., urban versus remote (wilderness) first aid for isolated working conditions with little to no resources available); the quality of country-specific providers; and possible litigation if first aid techniques are inappropriate or out-of-date.

Surprisingly, stress and wellness awareness did not rank high in survey responses. However, their importance within the curriculum should not be dismissed. Health and wellness challenges (illness, disease threats, medical attention and procedures) and stress (resilience, understanding how the body and brain react to threats, signs and symptoms, and management) are among the most prevalent forms of physical and psychological suffering experienced by humanitarian and development workers.

> *"In an ideal world, I think it's helpful if trainees are well briefed on stress reactions before going into an exercise, so they understand what to expect. It can also be explained that unprocessed traumas from the past, as well as significant current difficulties, can diminish people's capacity to cope with intense stress. That then gives individuals the chance to opt out if they wish, or seek*

out extra support. And without going into group therapy mode, giving people the opportunity after the exercise to share openly about how they felt can also model something really significant about the importance of discussing difficult experiences." – Interview Respondent

Transfer Of Risk. With the increasing shift of risk to national staff and implementing partners, respondents highlighted the importance of truly understanding the implications at both the strategic and operational levels. For example, an organization may require more discussion, decision-making and policy and procedural guidance for various transfer of risk scenarios.

WHOM TO USE

2.6 Choosing Training Providers *(see Guidance Tools D and E)*

Organizations have many choices when selecting training providers. They can use their own (internal) staff or choose from a range of outside (external) providers.

***Internal Security Providers*.** Comments from interviewees and survey respondents reflected a growing desire for organizations to have more in-house capacity for training. They suggested that in-house capacity helps improve the frequency of training provision and the content and quality, while also making it easier to ensure the materials reflect the organizational and environmental context. However, according to some respondents, executive buy-in to this approach is still lacking. Nonetheless, organizations with the necessary capacity and resources increasingly prefer to use internal trainers for orientations and basic personal security awareness training (often provided electronically) for their staff. More organizations are developing their own security training programs. To defray the costs of such programs, organizations are also increasingly opening their training courses to other organizations.

External Security Providers. For personal security and security management training that is open to participants from across the relief and development sector, NGOs tend to use groups that specialize in training. But for security training for hostile environments, they tend to turn to private security providers and the UN (e.g., Safe and Secure Approaches in Field Environments (SSAFE) training through the Saving Lives Together Initiative).

Organizations also tend to use independent consultants for specific needs such as crisis management, security management, technical security. Consultants were also noted for their flexibility in terms of cost and deployment, which can facilitate efforts to provide organization-specific personal security training at the headquarters and field levels. Field safety information offices, such as those run by the International NGO Safety Organisation in various locations around the world, often facilitate technical security trainings for specific groups such as driver and guard training at a country level and specific to context.

There is a proliferation of internal and external training providers. Many related issues are on the cusp of exacerbating the training market and may affect cost, quality and appropriateness for NGOs. For example, with the military drawdown in Afghanistan and other conflict areas, there is an apparent increase in new security training providers (mostly former military or police) starting up operations. This is particularly true in Europe.

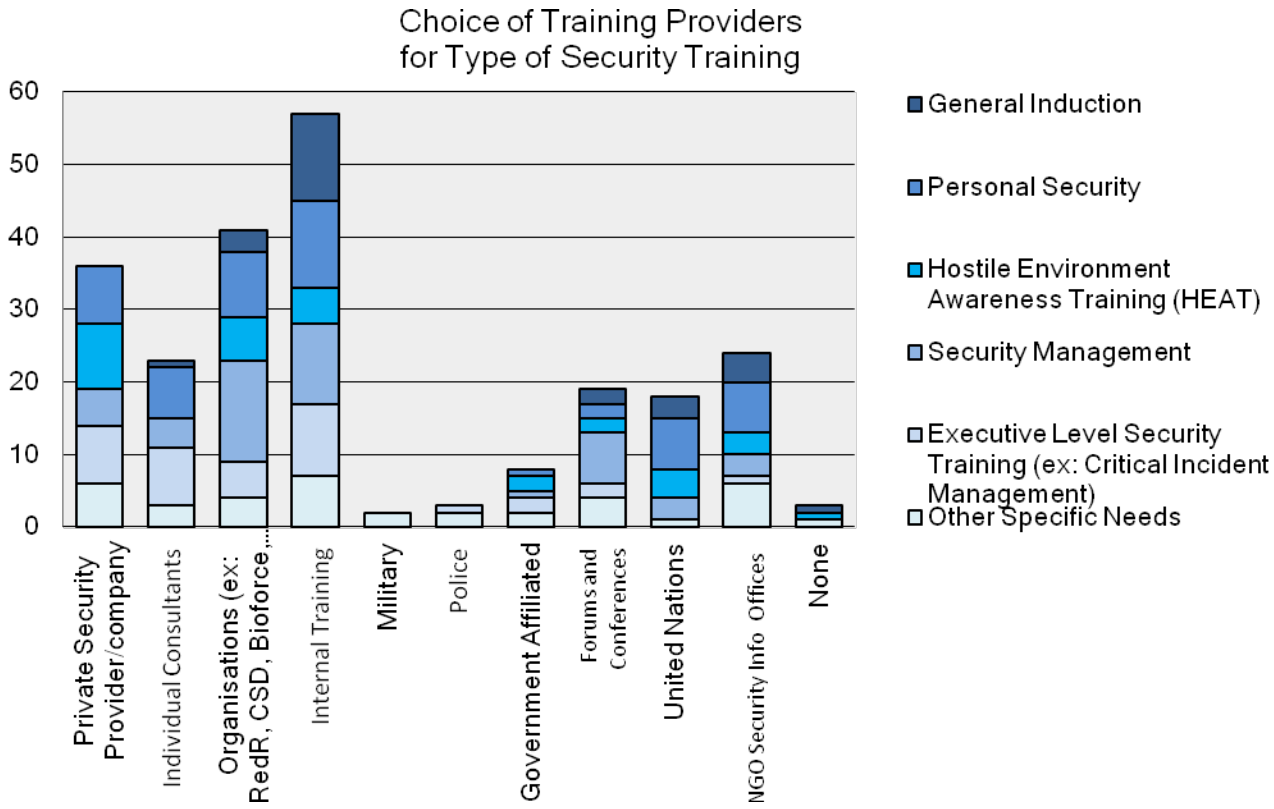
Respondents said they take into account the following criteria when selecting external training providers:

- Cost;
- Reputation and recommendations;

- The provider's experience with and understanding of NGOs;
- Timing and location;
- Proposed training content; and
- The trainer's experience in the relevant location and language.

The following chart summarizes data from our interviews and surveys about what types of trainers respondents use for different types of training. (The term "general induction" refers to general orientation provided to staff members.)

Figure: Strategic Level



Another important concern articulated was the need for greater scrutiny of the individual trainers employed by training providers. The comments of one headquarters-level respondent are illuminating in this regard. The respondent noted that a high proportion of security trainers tend to take a "directive" (this-is-what-you-do-in-x-situation) approach. But, as the respondent noted:

> "*Certainly there are better and worse courses of action in given situations, and these should be articulated, but really these trainings should make people feel able to make the right decisions and look after themselves, not to mindlessly adhere to security guidelines. That is important, but by their very nature critical incidents occur when the security guidelines have not worked or no longer apply. People need to have the skills and knowledge to make their own assessments of the best way to act when they are in a situation without guidance from outside." – Survey Respondent – Headquarters Level*

2.7 Communicating with providers: setting priorities

One key finding from both the surveys and interviews is that security training providers and NGO staff have significantly different views about what the priorities should be in security training. This applies at all levels of training and even covers matters like which topics should be required and which can be electives. This highlights very important concerns about the process of designing training courses, how they are provided and choosing a trainer. Many security training providers interviewed said they do conduct training needs assessments as part of their process for designing training programs for clients. However, organizations and providers still need to invest more time to have a two-way discussion that better ascertains the real training needs of the organization's staff so that the training courses better reflect those needs.

> *"Two sorts of negative practices: first, more among the NGO providers/consultants: Some sort of laziness; I have worked for some training providers and every year it is the same. Of course for someone who attends for the first time, that person learns a lot. But again, I think there is too much of comfort zone here, lack of self-challenging, lack of understanding that the field is constantly evolving …" – Survey Respondent, Training Provider*

MAXIMIZING IMPACT

2.8 Training Methods *(see Guidance Tool C)*

Training methods vary depending on cost, time and access.

> *"Obviously, when it is impossible to get staff to a training location, then distance learning via CD or Web-based training is going to be more useful. The use of distance learning for staff working in the field can lead to frustrations due to poor Internet access and limited free time to undertake long-distance learning courses. In all situations, the use of simulations and role plays that are relevant to the target audience is very useful and effective." – Survey Respondent, Training Provider*

E-learning. Many organizations have access to or have developed their own online training topics as part of basic personal security training. Some organizations with more resources and time dedicated to training have also developed online training for safety and security focal points.
However, respondents generally felt e-learning cannot completely replace face-to-face training. Others shared concerns about motivation, learning and retention with e-learning.

> *"I have seen this all the time: people want to just get their certificate as quickly as possible. They just rush through the CD, sometimes even get someone else to do it for them … while others need discussion, have questions and want to process." – Interview Respondent*

Other Options. Overall, survey and interview respondents said they prefer a blended learning approach (with e-learning for foundational materials and as a preparation for face-to-face training). They considered face-to-face security management training that uses both simulation and theory as generally the most effective method for individual learning, but also found simulation training effective for personal security training.

Comparing The Relative Effectiveness Of Different Options. The following charts summarize respondent data about how effective respondents rated the usefulness of various common training methods. The

first chart reflects the opinions of headquarters-level staff, while the second reflects the opinions of field-based staff.

Figure: Perceptions of effectiveness at the strategic level

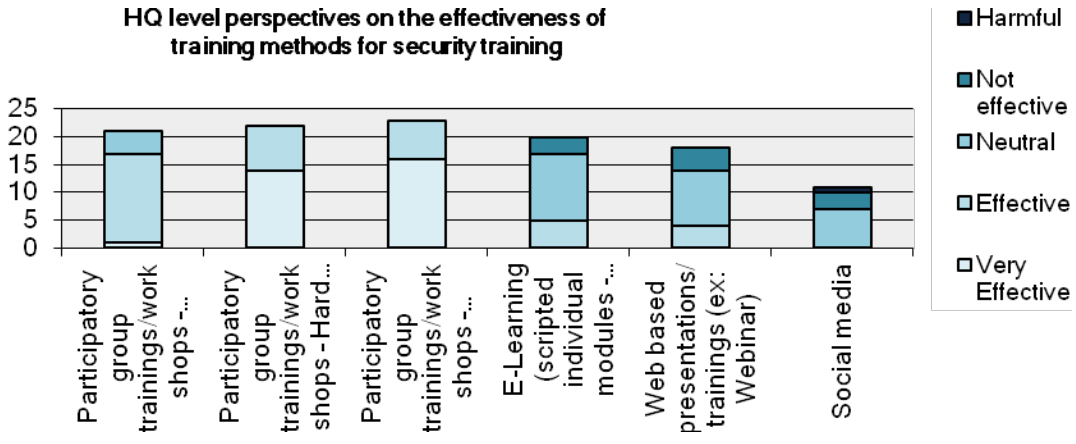
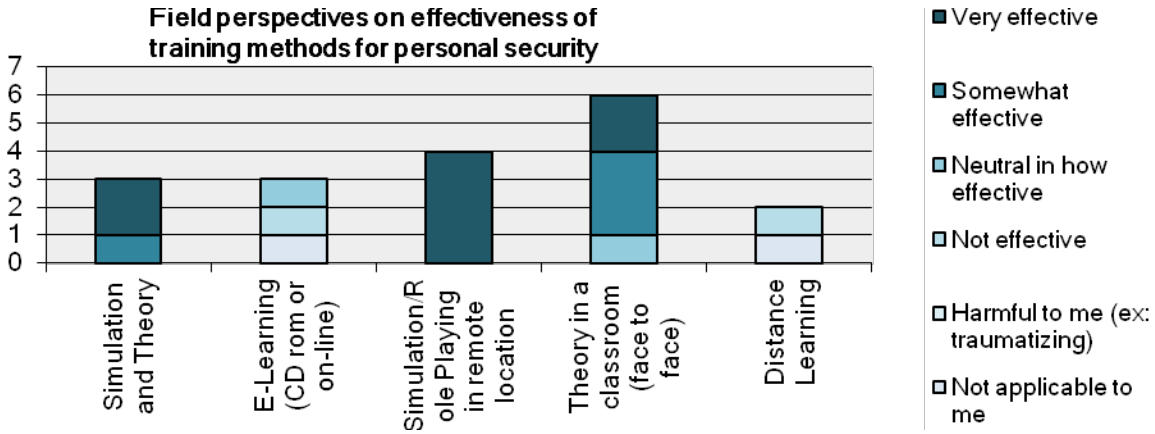


Figure: Field-level perspectives on effectiveness of learning methods for personal security



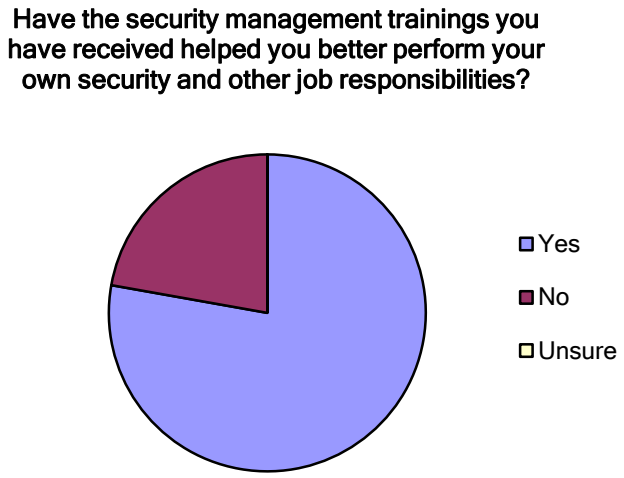
Open Courses Vs. Organization-Specific Course. Respondents said they most often use open courses for personal security training. Some groups also use open courses on general security management courses to explain basic concepts. These open courses can then be supplemented with tailored courses for individuals who need additional training. Respondents saw open courses as effective for fostering more interagency sharing, networking and learning. On the practical side, open courses provided a way to reduce training costs and ensure staff could receive training even if the organization did not have enough staffers to fill a training session on its own. On the other hand, respondents considered organization-specific courses appropriate for strategic levels of security training that center on organization-specific discussions about and testing of policies or other sensitive protocols.

2.9 Evaluation

Evaluation of training impact is one of the biggest gaps in the NGO community's current security training and management practices. Findings from interviews, surveys and research on various organizations' and training providers' methods and tendencies indicate that very few use on-going coaching, post-training support, mentoring (in-person or via Skype), email or return visits, work plans or provide follow

up sessions. In current practice, evaluation is almost entirely focused on collecting feedback immediately after the training ends. The resulting gap in longer-term follow-up and evaluation was notable and is discussed further in 3.7.2 below.

Figure: Evaluation of effectiveness at an operational security management level



2.10 Follow-up: keeping knowledge fresh

Survey respondents overwhelmingly supported the concept of using refresher courses for both security management and personal security. These types of services are already available. For example, Clarity Security Training offers a two-day refresher course two to three years after staff complete their original personal security training course. Refreshers and recertification are common practice in first aid training and must be kept current by individuals with certain job responsibilities.

2. 11 Accreditation and standards

The NGO sector is in the midst of a growing push to "professionalize." This push includes increasing calls for common standards and accredited programs for staff development. A number of training providers are linking with academic organizations to establish accreditation (e.g., RedR UK and the Centre For Safety and Development). However, many respondents in this project had mixed feelings about standards and accreditation initiatives.

> *"In a sector where consistent humanitarian occupational standards do not exist, several NGOs, INGOs [international NGOs], learning providers and universities have unilaterally moved, over the years, to address the learning and capacity building needs of workers based on their particular interpretations of identified needs. This has led to an ad hoc training offering, with gaps in provision and a lack of pathways and progression routes for the sector, both for those wishing to enter the sector and those wishing to develop professionally within the sector … [T]here is growing momentum to explore the potential for creating a unified system of professional development, accreditation and association, which could increase accountability, raise the quality and consistency of humanitarian service, open up the profession to talented new recruits, and raise the status of the humanitarian service provider to a level on a par with other professional groups."*

3. Creating an Organization's Security Training Framework

UNDERSTANDING THE BIG PICTURE

- 3.1 Security training frameworks
- 3.2 The organization's role in staff learning and development

ASSESSMENT: UNDERSTANDING THE ACTORS, ASSESSING THE NEEDS

- 3.3 Understanding the actors
  - 3.3.1 Understanding the organization
  - 3.3.2 Understanding the staff
    - 3.3.2.1 Who needs training
    - 3.3.2.2 Managing expectations
    - 3.3.2.3 Understanding how staff learn
- 3.4 Understanding the context
  - 3.4.1 Operating context
  - 3.4.2 Social and personal context

DESIGN, PROVIDERS AND COSTS

- 3.5 Design, Providers and Costs
  - 3.5.1 Building the curriculum
  - 3.5.2 Choosing training delivery methods
  - 3.5.3 Choosing a training provider
  - 3.5.4 Calculating the cost

MAXIMIZING IMPACT

- 3.6 Implementation
- 3.7 Feedback and follow-up
  - 3.7.1 Mentoring and transference of knowledge and support
  - 3.7.2 Evaluating learning and training impact
- 3.8 Increasing access to training

This section brings together the findings from the research to provide guidance on how to create an effective security training framework that meets the needs of the organization that will use it. It is important to keep these insights in mind when using the curriculum in Section B to create specific training courses.

UNDERSTANDING THE BIG PICTURE

Before delving into the process of designing a specific security training course, it is important to first step back and address a few big picture items relating to the organization's overall security training framework and the organization's role in and approach to staff learning and development.

3.1 Security training frameworks

Setting The Scope. The purpose of security training is to provide awareness, skills and tools for staff (individuals and teams) so they can perform their work duties safely and securely in their particular working environment. Training should respond to need, at the right time, for the right people, in the right place, and at a cost that is manageable.

Security training will not fix all security gaps and or satisfy all security requirements. It is only one component of a larger effort and strategy for mainstreaming security. Done right, it can and should play a critical role, and is far more than just demonstrating duty of care by ticking the box.

It is important to begin by considering a few fundamental questions:

- How does the organization foster collective responsibility around risk?
- How is the organization meeting its duty of care toward individual staff members?
- How can the organization better understand and support staff?
- How can it develop realistic, pragmatic strategic planning that fosters better security decision making by staff throughout the organization?

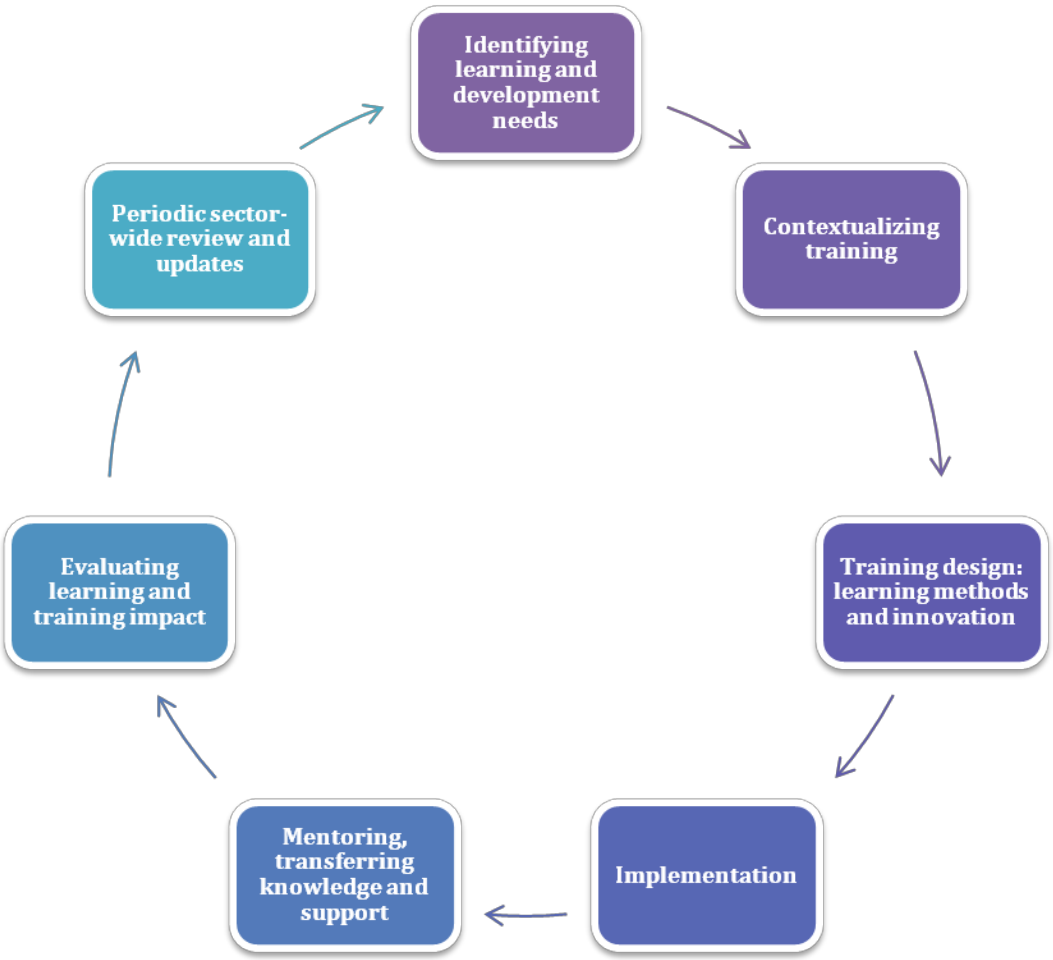
Perhaps the solution to meeting the challenges inherent in these questions is to expand our notion of risk: to understand that risk is not only physical, but also emotional, psychological and reputational. Security risk management should be more than just a focus on procedures and technical security. Security risk management and its ensuing training requirements should be grounded in the notion of collective responsibility around risk. Training should cultivate risk awareness. It should also help individuals and teams learn how to make informed decisions about risk taking and understand potential consequences of suboptimal decision making. Expanding our notion of risk also means increasing efforts to educate not just security staffers but also program staff.

This broader perspective is also important when thinking about the actual training:

> *"We really need to train large numbers of people across different organizational levels. It really is about establishing a culture, and this is hard to do with training [of] more or less isolated individuals. Finally, [we need to] train to create the attitude that security management is part of everyone's job (especially senior CO [country office] management), not something that is farmed out to a specialist security manager (though this function does have its place)." – Survey Respondent, Operational Level*

Actual delivery of security training is only one component of a larger framework organizations need to consider within a holistic approach to security-related learning and capacity building. The training itself is part of an ongoing cycle of design, education and review. The following framework is grounded in current practices and recommendations for mainstreaming sustainable NGO security training. It is inspired from principles of instructional systems design and strategic learning and development.

Figure: The NGO Security Training Cycle



This chart is not a once-around-the-loop process. While training is streamlined to be affordable, accessible, effective and shared, we also need to remember that one security training is not enough. Organizations must strive to provide a mix of learning opportunities (informal and formal), with topics that correspond to needs, location, organizational identity and the operational mantra of *right training for the right people at the right time.*

The reference curriculum in Section B and the guidance tools in Section C can help with planning for each stage of this cycle. The following chart walks through each stage, identifying practical tasks involved and ways the curriculum and guidance tools can be used.

Using the reference curriculum and guidance tools in the security training framework cycle

Framework Stage	Actions	Using the Reference Curriculum and Guidance Tools
Identifying learning and development needs	☐ Develop a learning and development strategy or integrate security training needs into existing learning and development (L&D) strategy. ☐ Security training assessment (conducted internally or by external specialist): ▪ Understanding the organization: its mission and operations, security and programming policies and needs. ▪ Understanding the staff: who needs training (and in what priority), how they learn, and their perceptions and attitudes.	See Section A 3.2 (the organization's role in L&D). See also Guidance Tools A (assessing L&D needs) and B (L&D strategies). See Section A 3 (assessment). See also reference curriculum introduction to Level I concerning staff level of risk exposure and personal security training sublevels.
Contextualizing training	☐ Determine type and level of security training needed. Can it be generic or does it need to be contextualized to the organization, location and/or staff?	See Section A 3 (assessment). Reference curriculum can be consulted to determine which trainings can be generic and which must be contextualized.
Training design: learning methods and innovation	☐ Determine which topics to include. ☐ Select the most appropriate learning methodologies.	See Section A 3.5 (design) and reference curriculum topic lists. (Lists can be basis for designing internally developed courses OR for comparing and refining course offerings proposed by external providers.) See also Guidance Tool C (overview of instructional and learning methodologies).
Implementation	☐ Identify ways to increase access to the training. ☐ Select a training provider (internal or external). ☐ Working effectively with the selected training providers.	See Section A 2.8 (training methods) and 3.10 (increasing access to training). See Section A 3.6 (choosing a training provider) and Guidance Tools D (selecting and working with training

		providers) and E (what to expect from a good trainer).
Mentoring, transferring knowledge and support	☐ Determine how the organization and management can best support staff in applying to their work the knowledge and skills gained in security training.	See Section A 3.9.1 and Guidance Tool C (overview of instructional and learning methodologies).
Evaluating learning and training impact	☐ Evaluate learning (did people learn what they needed to learn) and training impact (has it had a impact on their daily behaviour and work performance).	See Section A 3.9.2 (evaluation) and Guidance Tool F (monitoring and evaluating effectiveness and impact). See also reference curriculum learning outcomes provided for each training level. The outcomes outline competencies for job performance and staying safer.
Periodic sector-wide review and updates	☐ Gather feedback from users and the broader community on what needs to change in the reference curriculum; make revisions accordingly. ☐ Use feedback and revisions to inform and strengthen community-wide security coordination and discussion.	Ideally, reference curriculum is regularly updated based on community feedback. This creates a discussion platform between agencies and training providers.

Including Program and Human Resources Staff. Discussions about NGO security management have long called for mainstreaming security rather than treating it as a "bolt-on" component. Any effort to seriously address the interdependence of programming and security must involve increasing the consultation and participation of program staff in the security training process. HR must also be part of the training dialogue in order to strengthen coordination and ensure that HR documentation can be used to support the organization's security training efforts.

3.2 The organization's role in staff learning and development *(see Guidance Tool B)*

To get the maximum benefit out of any security training, the training should be based on and tied into the organization's overall staff training program. When an organization takes a strategic approach to supporting learning and development, it can improve job performance, change risk attitudes, and foster preventive behavior and team cohesion.

Several components form the basis of effective learning and development strategies. Organizations need to take on the following roles:

- Understanding what training and development is needed.
- Treating training as an integral component of the organization's strategic and programmatic plans.
- Allocating the money needed for training – globally or on a project-by-project basis.
- Linking learning and development to individual and team performance appraisal processes.

Learning and development strategies can be and often are linked to individual performance appraisals. Each staff member should develop personal learning and development objectives. Organizations and personnel need to be realistic and simple when designing and implementing a learning and development strategy. When learning and development strategies are too ambitious, they become difficult to implement and may not achieve learning and development goals.

The learning and development effort must include the participation and consultation of a broad range of staff members. This is essential to ensure that there is a collective understanding of the strategy. It also fosters a better strategy and facilitates implementation by creating stronger staff buy-in.

ASSESSMENT: UNDERSTANDING THE ACTORS, ASSESSING THE NEEDS

(See Guidance Tools A and B)

Organizations are often not sure how to design their security training (what content to provide, what learning platform and provider to use). This is usually because they have not conducted a proper assessment of what is needed. As a result, rather than tailored training that reaches the right people at the right time, training is sometimes allocated in a more ad hoc way: perhaps as a reward, or because of a staffer's interest (as opposed to need), or even just because the timing worked out.

Effective assessment involves understanding the two pillars of security for humanitarian and development organizations:

- Security management competencies that individuals with security responsibilities need to perform their jobs in a way that meets the organization's goals; and
- The personal security and safety awareness that each staff member needs given where they work (and live) and what they do.

From there, it becomes easier to determine when, where and how to provide the necessary training. Step one is understanding the actors: the organization and the staff. Step two is understanding the context.

Working with internal and external trainers can facilitate assessing training needs. By providing a better understanding the organization and its needs, the assessment can help efforts to maximize the usefulness of the training content. This is done by building into the core security curriculum references to existing policies, procedures, capacity and other relevant information concerning the organization. Factors to consider when selecting trainers is discussed in more detail below in 3.4.3.

3.3 Understanding the actors

One-size-fits-all training can never adequately fulfill needs. Effective training entails understanding both organizational capacity and goals, as well as the needs of individual staff members. For the former, the assessment must verify the organization's existing capacity and identify any gaps between that capacity and what is needed to meet both the stated training objectives and the capabilities needed to address changes as they arise. To assess staff member's individual needs, the assessment should include discussions with individual staff members to compare what they currently know and how they currently operate given their job requirements and organizational goals. The results can then be used to set security training priorities.

3.3.1 Understanding the organization

The starting point for this assessment is understanding the organization's identity: its mission, values, capacity, operational profile, exposure and codes of conduct. This includes its approach to risk management and its risk tolerance. Job profiles and needed competencies should clearly reflect all of this. Security training should then hone in on the skills each staffer needs to enable the realization of the organization's programmatic and overall objectives.

Another important component of understanding the organization relates to the fact that security incidents often arise from internal threats. Because of this, the assessment should include a review of incident patterns in the organization, ways in which security practices diverge from stated policies and procedures, and HR issues and indicators (e.g. staff turnovers and retention issues). This can provide valuable insights that can be built into or inform training design.

3.3.2 Understanding the staff

Determining who needs what: defining scope, setting priorities. When assessing the training needs of individuals and groups, asking three key questions can make a huge difference:

- Who needs training?
- What do they need to know?
- How do they learn?

3.3.2.1 Who needs training

To better assess staff training needs, the first step is to determine who needs training. But to do that, the organization first must identify whom to use to identify the staff who need training. They should be well suited to assess staff attitudes about security. They can be internal or external – specialists in learning and development or simply knowledgeable and experienced in HR, management and/or operations. Whatever their job profile, the organization needs to make sure they understand and bear in mind a range of matters including: the context, the relative security risks, what specific staff or staff groups need to know, how staff perceive security, what competencies staff need to fulfill tasks and stay secure, and any residual gaps.

The person or people selected need to talk to a number of key stakeholders including: senior management (those who approve and support implementation of the learning and development strategy); human resources; and line managers and staff (individuals and groups).

Keep in mind that a list of who is currently receiving training may not accurately reflect who actually needs training.

When determining staff training needs and prioritizing those needs, organizations need to know who is requesting training and what may be prompting the requests. Today, NGO security training is predominantly triggered by pressure for organizational governance to demonstrate legal duty of care. This overlooks the foundational principles of ethical and moral duty of care in actual staff care. Training provision is also often reactive, prompted by a deteriorating security environment and immediate need to address staff security. The assessment process needs to keep these issues in mind. Other factors include: staff position, responsibilities, compliance requirements, and the level of security risk in the working and or travel context.

National And Local Staff. The assessment should include fulsome consultation with national and local staff about their security training needs and how to meet these needs in way that effectively takes into account social and personal considerations such as gender, disabilities, religion and other societal factors. It is critical to capture how they view their world and their security needs. This step currently is too often neglected.

National staff represent the face of the organization and often account for the largest number of employees. Yet their access to effective security training is often inadequate. As one interview respondent explained: "It is evident that there is still not an equitable level of training for national staff; international staff have more opportunities." Follow-up on the training they do receive is also often inadequate.

The goal of this step should be to collect the information the organization will need to make sure the security training framework accurately reflects the needs of national and local staff and increases their access to effective training.

3.3.2.2 Managing expectations

Staff often have inflated expectations about what security training they will receive. The assessment process is a good time to start identifying expectations and helping people understand what will actually be provided. Obviously this process needs to continue throughout the design and implementation phases, but it should begin at this stage.

> *"I know many staff who want to take hostile environment training because it is seen as 'adventurous and fun' – not necessarily because they actually need this level of personal security training for their existing or prospective working or travel risk environment." – Interview Respondent, Headquarters Level*

Security training can also be a useful opportunity to manage other expectations of individuals and teams, especially in situations where staff have limited experience and differing expectations about their work, the operating environment and the organization. Training addresses these issues by providing a better picture of the organizational culture, security situation, and the diversity of perceptions about security and common sense.

3.3.2.3 Understanding how staff learn *(See Guidance Tools A and C)*

A training plan that looks good on paper is not worth much if the people taking the training do not understand why that training is important for them. Participant buy-in is critical. Equally and relatedly important is making sure the training uses learning methods that work well for the targeted staff.

That means that an organization needs to understand what motivates the staffers the training will target and how they learn best. Organizations should strive to:

- **Understand the personality types** of the targeted staffers. A number of relevant personality assessment tools exist to help with this process such as the Myers-Briggs Type Indicator.
- **Understand their dominant learning style(s)**. Examples include verbal, logical, visual, kinesthetic, musical, interpersonal and intrapersonal.
- **Take into account learning theory** such as Kolb's Learning Cycle: doing, observing, thinking/feeling and experimenting.
- **Determine how best to emotionally engage** the targeted staff.

- **Understand other personal factors that may inhibit or facilitate learning** such as language barriers, learning disabilities, biases and stress.

Other important variables such as common sense, decision making, judgment and behavior concerning security come into play irrespective of how much training is taken. These variables are subject to cultural, gender and educational influences that can affect learning and development. They can also cause tension within NGO working teams, despite organizational codes of conducts and other related principles.

This can help with prioritizing training and determining which staff most need the capacity building the training can provide.

Learning Methods. Different people need different ways to learn. That means that an organization must first understand how the targeted staffers learn before it selects which training method(s) to use.

Generational factors often come into play in terms of what style of learning may work best. Baby boomers are often accustomed to learning through lectures, workshops and manuals. Generation Xers often have more familiarity with hands-on exploratory learning, role playing and PowerPoint. Millennials tend to use all those methods plus e-learning, including Internet, laptop, handheld and cellphone-based systems.

Changes in the technological environment can also affect the outlook that staffers bring with them to classroom:

> *"You can only guarantee peoples' attention when they are in the room, because they are busy people. And that isn't even always true, because even when they are in the room they will disappear, or they will turn up late and say sorry and do some emails. They are pretty good in the training room. I would say they are getting worse not better in terms of attention, because of wi-fi and everything. Ten years ago you got people in the room in Kenya and you had them. Now they are on the phone." – Interview Respondent*

Information from this part of the assessment is particularly useful when selecting the way to provide the training, a topic discussed in further detail in 3.5.2 below.

Emotionally Engaging The Targeted Staff. Staff buy-in is critical. Staff who feel that the training they are taking will help them in their daily work are much more likely to be actively engaged in both learning and applying what they have learned to their jobs.

As a result, the assessment should investigate current attitudes about the relevance (or lack thereof) of security training to a staff member's work. It should also assess how to create a training framework that is most likely to encourage the targeted staff to become actively engaged in the learning process.

> *"E-learning is only based on a very linear perception of security; people must believe they are worth it. Emotional and psychological locks must be cleared before there is a desire and openness to learn. We believe that we want tools, formulas, matrixes … but is this learning? ... not really. People want to process with their hearts and spirit so the whole being is able to tap into response and resiliency. Systems, rules and regulations only work if everyone agrees and has a structure that makes it happen." – Interview Respondent*

3.4 Understanding the Context

As mentioned previously, there will never be an effective one-size-fits-all security training. The spectrum of humanitarian and development organizations is too broad and their approaches and needs are too varied. Staff need training that reflects their real world needs. So putting training into context is critical. This involves making sure the training will reflect three key dimensions:

- Organizational context (the organization's mission, philosophy and operating realities) (see 3.3.1 above for details);
- Operating context (realities and risks on the ground where the trainees work and live); and
- Social and personal context (relevant considerations involving gender and other cultural and personal matters).

3.4.1 Operating context

This research found that one of the most salient training considerations is the need to understand and adapt training to location-specific realities and the security threat environment. This includes not only situation-specific security context, but also a myriad of other location-specific factors such as political, environmental, technological, social and geographic conditions, incident patterns and other logistical considerations that affect security. Ensuring the training provided reflects these factors allows participants to recognize the real-life factors that affect their security. It can also help them better understand how the training can help them not only stay safe, but also more effectively perform their jobs.

In some locations, regional security coordination bodies are helping organizations create this sort of contextualized training. For example, the NGO Safety Program (NSP) Somalia has developed and piloted security management trainings for country directors and security focal points. These trainings provide good practice guidelines on how to mainstream security into their organizational structure through understanding the specific challenges of Somalia in terms of security and the links between programming and security in the Somali context. They also include a checklist of practical actions.

3.4.2 Social and personal context

Security hinges not only on the organizational and operating context, but also on individual staff and staff teams and how they communicate with each other. A variety of social and personal considerations such as gender, disabilities and religion affect the perception, design and impact of training. Examples include: assessing the perspectives, sensitivities and fears about security; and ascertaining and factoring in the implications of training such as the impact on existing gender roles, levels of physical and psychological health, social and religious beliefs (e.g., touching or exposing body parts in first aid training), interactions between men and women and any ensuing consequences. Beliefs often take precedence over learning. This raises important cultural and gender considerations that may or may not be obvious, but convey implicit and subtle messages that may have negative ramifications.

Consultations can be used to gain a better understanding of how security is perceived by both international and national staff, and how training can be best delivered given existing cultural and gender specific factors.

There are some very important questions that also need to be asked and addressed:

- Should the training be sex-segregated or mixed sexes?
- Which staff should attend?
- Where should the training take place?
- When and how should it be delivered?
- What are the possible internal and external perceptions of this training?
- What positive or negative impact could ensue and how should the organization mitigate potential negatives?

A gendered and holistic approach centers on the strengths and attributes of a person and how he or she reacts as a human being. By attending to the deeper internal context of individuals, it is easier to emotionally appeal to them and encourage learning, address their needs, and capture their perspectives on security and what it means to them and their community.

DESIGN, PROVIDERS AND COSTS

3.5 Design, providers and costs

3.5.1 Building the curriculum. (See Section B – Reference Curriculum)

The process of designing training consists of:

- Developing structured and sequenced learning objectives;
- Identifying the training needed to achieve those objectives; and
- Creating opportunities for staff to demonstrate what they have learned through their actions and task accomplishment on the job.

Once the objectives are identified, topics can be selected and developed that will facilitate learning performance tasks or gaining awareness.

The reference curriculum in Section B lays out a curriculum structure and extensive lists of objectives and topics that an organization can draw from when creating security trainings to meet its particular needs. The section provides further guidance on how to use the materials it provides. **The topics reflect issues relevant to the particular level or sublevel of training. The amount of time it takes to cover different topics may vary significantly**. This means that time spent on any particular suggested topic can vary depending on the organization's profile, the relevancy of the topic, its importance for job performance, and how much participants already know the topic's content. For those familiar with the term "module" as used by the training community, keep in mind that "topic" as used in this document is not the same thing.

3.5.2. Choosing training delivery methods. *(See Guidance Tool C)*

In addition to selecting the topics, course design involves selecting the most effective way to offer that material to the targeted staff. This includes determining which training method(s) to use, the level of depth for each topic, and what facilitation style the trainer should use.

There are many types of training methods and strategies that can be considered and implemented, as long as they can effectively achieve the learning objectives. Examples include face-to-face learning, blended learning, distance learning, e-learning and virtual learning. Guidance Tool C provides an overview of learning methods.

Learning is interactive and should not be limited to the acquisition of theoretical knowledge disconnected from practice and reality. Although subject matter should dictate the delivery method(s), a

blended learning approach consisting of various combinations of e-learning, face-to-face workshops, CD-ROM, books, articles and webinars can be very effective for NGO security training. For example, online learning and other preparatory assignments can be used to prepare staff for a face-to-face course. This can improve learning readiness and reduce the time and costs associated with face-to-face training.

Keeping in mind insights garnered from the needs assessment, an organization may do well to consider several of these options when designing a particular training course. The main objective is to determine which technique is likely to be most effective for this particular course and group of learners.

Informal training and further information dissemination*.* Not all learning comes from formal trainings. Informal learning can be just as effective. When designing a training package, consider informal opportunities as well as formal ones. For example, all staff (national local and relocated, international, volunteers, interns, consultants and even agency visitors) should receive an overview of safety and security in their orientation to the organization and to their job. All staff should also, ideally, receive country-specific security briefings upon hiring, arrival in country and periodically thereafter as needed. They should also be debriefed at the end of a work assignment. Staff meetings, peer networks and mentoring can also provide opportunities for ongoing learning and development.

"80% of our learning is informal; some estimate it is more" – Interview Respondent

Refresher training. Even staff with field experience need security training. Operating environments constantly change, their previous experience may not be relevant, and they probably have new responsibilities and team members. Refresher courses are a useful way to address this need. This is similar to first aid courses that require refreshers and recertification to keep learners appraised of updates in practices, and provide an opportunity to practice their skills and increase their self-awareness.

Using integration to increase security training opportunities. Another way to increase staff exposure to security training is to integrate security topics into other existing trainings such as human resources, risk management, strategic planning, project management, leadership, management, proposal development and writing, and emergency preparedness and response. This does not eliminate the need for separate training dedicated specifically to security. Instead, it offers a way to supplement and reinforce that training.

Level of detail**.** Less is more. Simplicity is important when conducting training. Packing too much information into a day or course agenda can undermine retention. On the other hand, focusing on core concepts and effective delivery practices can increase retention and strengthen the end results.

Separate modules. Organizations may also want to consider "modularizing" some of the topics in the reference curriculum in Section B. This can consist of creating a separate mini-course for a particular topic (e.g., acceptance) or a mini-course for a small group of related topics. In either format, the goal is to create more in-depth learning opportunities dedicated to a specific area for staff with a particular need to develop expertise on the issue.

Open training v. organization-specific training. Organizations must also decide if open or organization-specific courses are the best way to achieve their training objectives. Both can be useful and both types are used by many organizations.

Open courses are courses with participants from multiple organizations. Rather than honing in on one organization's perspectives, these courses are generic and present knowledge that is useful to people across the sector. Staff must adapt the material in the course to their own specific organization and working environment. Open courses provide a more neutral starting point, facilitate sharing and networking between organizations, and foster learning outside existing assumptions. These courses are an excellent way to provide staff with a solid base of the principles, while subsequent training and guidance can provide them with organization and country-specific material.

Organization-specific courses are those with participants from only one organization. They are very useful for covering topics and material that may be unique to an organization. They are also very useful when the organization is focused on developing specific policies, strategies and procedures. For example, crisis management must be organization-specific.

3.5.3 Choosing a training provider *(See Guidance Tools D and E.)*

There are several options for training providers. Depending on needs and available resources, organizations may choose to use their own staff to do the training (internal) or outside (external)individuals or groups with the necessary expertise. Internal security training is possible if the organization has dedicated trainers and is willing and able to commit the necessary time and resources. Depending on location, availability, timing, course content and cost, organizations can also consider external training providers. These include organizations, private companies and individual consultants, UN entities and other organizations that have opened their internal trainings to other agencies. There are also numerous open-source training materials and other learning opportunities available through forums, conferences and subject matter experts. While there is no master list of such sources, the International Federation of the Red Cross and ECHO (European Commission – Humanitarian Aid and Civil Protection) are good sources to start with.

Regardless of the type of chosen provider, organizations should bear in mind that training involves a particular skill set. As an instruction systems design specialist we interviewed explained: "For organizations, they need to accept that training is a specialty. Just because you can stand up in front of a group doesn't mean you can train. People do not respect training as an area of expertise."

Many established training organizations and private companies live on reputation – reputation being one important factor in training provider selection. However, the quality and success of training often hinges on the particular trainer who actually conducts the training, more than on the reputation of his or her employer.

Organizations need to determine who the actual trainers are (internal or external) who will stand in front of their staff (keeping in mind gender, experience, sensitivity, teaching ability, leadership, facilitation skills and training content). Organizations also must be mindful of how the protential trainer interacts with learners. An effective trainer should have both the relevant experience and the ability to teach and facilitate. Ideally, their core values should more or less match the organization's values. They need to possess the skills to emotionally and intellectually appeal to and move participants. They should be sensitive to the organization's culture by having a solid comprehension of programming, organizational structures, standards, policies, procedures and frameworks.

> *"The choice of the trainer is important, as it already indicates how we want to cope with security risks. Trainers usually focus the sessions according to their backgrounds and while some will emphasize protective or deterrent measures, others will treat security with a more holistic approach."*

Organizations also need to be more mindful of trainer-to-learner ratios.

Finally, keep in mind that customized training requires significant investments of time before and after the training. Organizations must communicate throughout the process with training providers and verify that the curriculum and other training details match their objectives, culture and needs. Pretraining preparation could include questionnaires to establish a baseline of where staff are, conducting an audit, and questioning participants about what are they doing and how they perceive security.

3.5.4 Calculating the cost

Securing funding can be challenging. Training costs are justified costs. But to garner stronger budget support, they need to be accurately determined, factored into overall risk management expenditure (context-specific or global), and better communicated by program management, security personnel and proposal writers. Cost-benefit analysis is an important part of this process.

There are three key components:

- Know the costs of your training needs (see assessment section above);
- Know the costs of your training options; and
- Know the cost of not providing effective training.

***Know the costs of your training*.** Resource allocation and budgeting should be informed by the training needs analysis, and the organization's learning and development strategy and training plan.

***Know the costs of your training options*.** Not all training options cost the same. Armed with an understanding of the learning styles that will work for the targeted staff as discussed above, organizations can more easily identify potentially effective training options *(see Guidance Tool C)* and quantify the actual costs of each option.

In general, in-house options are less expensive than using outside providers. But this is not always the case. Some in-house options can be surprisingly expensive. For example, more and more organizations are creating their own e-learning materials. This can be expensive and production costs can be exorbitant, especially if the materials will need regular updating.

There are many other lower-cost learning opportunities, such as on-the-job training or self-managed learning. Another way to save money is to share training costs and resources with other units of the organization and/or with other like-minded organizations, especially at the field level. This can be an effective way to save money while also responding to calls for more frequent training in locations that need it most.

There are also free resources available. For example, many organizations that do not have the resources to develop their own e-learning materials use a free, online, personal security course provided by the International Federation of the Red Cross through its Stay Safe learning platform.

Regardless of the option, it is always critical to remember (and to remind decision makers) that best price does not mean the best option. Quality and effectiveness are paramount.

***Knowing (and quantifying) the cost of not providing effective training*.** Quantifying the costs of something that did not happen certainly presents challenges. However, being able to provide budget

decision makers with examples of the costs incurred in responding to incidents that could be avoided (or made much less likely) through proper security training can be a helpful tool in the budget justification process.

MAXIMIZING IMPACT

3.6 Implementation

Implementation consists of ensuring the delivery of learning and development as a solution to addressing performance and awareness. There must be specific objectives, actions and indicators. The responsibility for overseeing learning and development must also be clearly established.

A number of stakeholders play important roles in ensuring effective implementation:

- **Senior management** must be involved to ensure consistency of vision, provide necessary decision making, assign responsibility, and promote a culture of learning.
- **Human resources and learning and development personnel** must: determine learning and development needs; develop strategies and training plans; participate in consultations and analysis; organize delivery of training; and identify internal and external resources.
- **Line managers** need to help identify needs, participate in facilitating events, support attendance, and evaluate the impact of training.
- Finally, **job holders** must be responsible for their own learning and development by identifying needs and training opportunities, and by actively engaging in on-the-job and self-learning.

3.7 Feedback and follow-up

3.7.1 Mentoring and transference of knowledge and support

Too often, knowledge gained in training is not fully leveraged to produce actual changes in workplace behavior. Organizations need to remember that the process of making sure that transfer does occur is just that: a process, not a one-off event. It entails post-course work and continued support.

Post-training event follow-up, coaching, mentoring, interventions, validation, homework (tasks and action plans), and recognition can help support transference of knowledge into work behavior that enhances job performance. Line managers should consider providing ongoing learning and development opportunities, refresher trainings and mentoring opportunities in parallel with other informal learning opportunities.

While this may initially seem burdensome on top of the other resources required to design and conduct the training, these post-training investments are actually fiscally and operationally wise in that they improve the impact of resources already committed, help avoid security incidents, and may lessen the frequency of the need for additional formal training sessions.

> *"I think in conjunction with quality training, there is a place for remote support. And this is what we are working on now, introducing pre-work and post-work support. And it is an uphill struggle ... we are trying to get agencies to say we cut the face-to-face training time if we can introduce the basics beforehand, and somehow monitor how people are using it in their everyday work." Interview Respondent – Training Provider*

3.7.2 Evaluating learning and training impact *(See Guidance Tool F)*

Evaluating the impact of security training is one of the most important gaps in current security training practices. It is usually the final stage of a training cycle that involves assessing the effectiveness of training at various levels.

To date, most evaluation efforts concerning security training have focused on gathering feedback immediately after a training event. Unfortunately this only captures information about participant satisfaction with the training right after it ends. It does not collect the information needed to evaluate the impact of the training on professional performance, changes in behavior, organizational results and return on investment.

The ultimate goal of security training is to equip staff with the knowledge and skills they need to perform their duties safely and effectively. To determine if the training is having that effect, the organization must monitor and evaluate staff performance over time. This can also be used to determine what other supplementary learning is needed to improve performance or increase awareness and what remedial (corrective) actions should be considered for ensuring continuous improvement and maintenance of training.

Certainly many factors come into play, such as time, priorities, staff turnover and capacity. However, organizations should ask whether the training they provide to their personnel is:

- Actually reaching those who need it;
- Positively influencing performance;
- Positively affecting behavior; and
- Increasing safety and security.

Organizations should treat this impact verification as part of a larger process of assessing in the short, medium and long term (if possible) how training has influenced progress on learning and development objectives, human resource goals and overall organizational objectives. Managers are in the best position to evaluate and observe changes in staff behavior, demonstration of skills and application of knowledge. These evaluation activities may face challenges such as high staff turnover, lack of time, lack of prioritization and lack of staff interest. However, the challenges must be met in order to create truly effective security training instead of training that is merely reactive and focused on the short term. In particular, organizations should actively look for ways to get staff to engage in the evaluation process, including ways to create a monitoring and evaluating process that is interesting and part of learning.

Other evidence of training effectiveness may be anecdotal as staff feel more aware, empowered secure or safer. Other indicators could include the reduction of security incidents, increased compliance with security procedures or team cohesion. The impact of change and learning can never be under-estimated as it is a key contributor to organizational success.

3.8 Increasing access to training

Organizations should look into ways to increase the frequency of security trainings in the locations that need it the most, similar to surge capacity. Organizations and outside training providers should also continue to develop teaching and learning methods for distance learning. To help alleviate the cost and logistics of training, organizations could consider coordinating and cost-sharing with other like-minded agencies especially at the field level.

4. Conclusion – Strengthening Security Training Across the NGO Sector

As mentioned before, this project consolidates and enhances current and good practices for NGO security training at four distinct levels. It is designed to help organizations sort through their options as they work to develop and evaluate the most appropriate security training for their personnel: so staff can stay safe while also effectively carrying out work responsibilities. However, the NGO reference curriculum, guidance and tools produced for this project are not definitive and must be regularly revised over time. There should not be another 15-year gap before the community revisits this issue and set of materials.

If implemented, the following recommendations would serve to strengthen NGO security training:

Revisions to the NGO security training reference curriculum. We, as an NGO security community, need some level of understanding (not necessarily agreement) about what is core to learning and good for security training practices. Periodic reviews by members of both the NGO security and programming communities could serve as a way to discuss, provide feedback and suggest any changes to learning materials: identifying what needs to be included or modified, and what needs to be communicated to organizations' leadership, operations and training providers. Training practitioners also agree that they need to better respond to organizations' training needs: adapting the training they provide to the organization's particular identity, operational realities and needs.

***Collective voice of organizations*.** The InterAction and EISF forums would be effective platforms for organizations and members of the NGO security community to discuss and revise security training needs, emerging issues, necessary competencies and skills, and update the reference curriculum to reflect what is necessary and needed for tomorrow. This mechanism and consultative approach would ensure that this project's security training reference curriculum is appropriately updated, sustainable and continues to reflect the changing operational context of NGOs, their evolving operational habits and emerging security threats.

***Further analysis*.** Ideally, this reference curriculum should be monitored and evaluated for a full year (or two) after it is released to the NGO community. While the framework provided by the project is a template, the evaluation should include a review of how the materials are actually used and how useful prove to be. This analysis should be used to update its content; doing so will increase the longer-term relevance of the materials. Following the more intensive first-year monitoring, the materials should still be reviewed and updated annually thereafter. The evaluation and analysis of the impact of security training on individuals, teams and organizations would be an interesting if not critical piece to our understanding of the role and effectiveness of training.

***Auditing*.** There are also interesting opportunities to conduct audits of different types of NGO security training courses (e.g., online, face-to-face) and to develop more general organization security audits. EISF is producing a tool to assist in general security audits scheduled for publication in 2013.

***Compendium of security trainings*.** Currently there is no compendium of existing trainings. Creating such a resource would be very helpful for many organizations. The compendium should list available trainings (open source, specialized, outsourced and internal) to give organizations a better view of what is available, where and at what cost. It should also examine how money is spent on training, what is being done, what can be shared, and what other relevant trainings exist outside of the NGO community.

***Vetting trainers and training providers*.** The continuation of rosters of individual trainers, training providers and technical specialists vetted by organizations via security platforms would be beneficial. Although they do not currently carry the weight of formal professional certifications, such rosters (and the references they provide) offer some historical and reputational appraisal organizations can use to match their security training needs with the most appropriate individual trainers and training providers.

SECTION B

NGO Security Training Reference Curriculum

NGO Safety and Security Training Project

2014

SECTION B – NGO Security Training Reference Curriculum

1. Introduction: Key Principles and Structure

The purpose of this reference curriculum is to provide useful guidance to organizations working to establish effective security training for their staff. It covers both personal safety and security management training.

It reflects extensive research conducted as part of this project. It draws on available training materials, security and organizational community consultations, interviews and survey responses, posted job descriptions, as well as relevant trends in humanitarian and development practice. It captures good practice and global understanding regarding quality and consistency of NGO security training. This curriculum should be considered a guideline not a minimum or a standard.

The suggested topics reflect community agreement on ideal training regimes for various staff members, based on their risk exposure and job responsibilities. However, good practice and reality are not always the same thing and **there is no one-size-fits-all answer to training**. Organizations should use the reference curriculum as a guidance tool: creating their own curricula that reflect their particular missions, learning strategies, operational realities and staff needs. It should be used in conjunction with the narrative report in Section A. Note that this curriculum does not specify how much time to be spent on a particular topic. That decision should be determined on a case-by-case basis taking into

consideration a number of factors including the need and relevancy of the topic to the participants in that training.

Organizations can use the curriculum to design training that takes various forms: formal or informal, tailored to the needs of the organization or more broadly constructed to appeal to a wider range of participants. The curriculum is meant to welcome innovation and consideration not only of topic content, but also of which teaching methods might be most effective. It is a living document open to further development and future modifications. Ideally, it should be revised regularly by the NGO community.

The reference curriculum, along with narrative report in Section A and guidance tools in Section C, is also designed to assist organizations with selecting appropriate external and internal training providers, and to ensure the providers are meeting the needs of the organization. Working with training experts, organizations can also use this document to develop a systematic way to evaluate the operational impact of the training over time.

Structure. The curriculum is divided into four training levels, reflecting the fact that different staff members have different training needs:

LEVEL I **Personal Security Training** for all staff (and volunteers) working in or travelling to various security risk environments.

LEVEL II **Operational Security** for those with day-to-day responsibilities for implementing security (e.g., security focal points, drivers, guards and program staff).

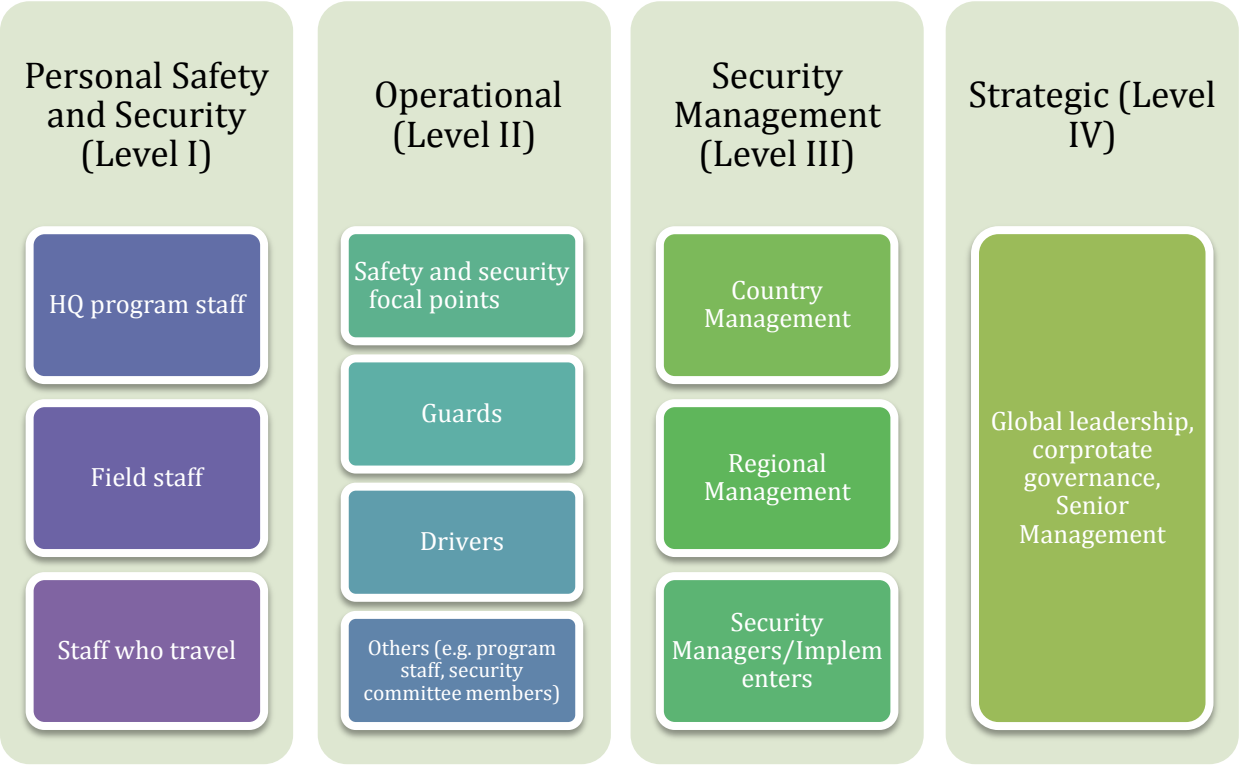
LEVEL III **Security Management** for those with a decision-making role in developing and implementing risk management and policy, such as (but not limited to) members of the global security management team and regional and country management.

LEVEL IV **Global Strategic Security** for headquarters staff with decision-making authority and responsibilities related to the organization's strategic vision, overall duty of care and/or its global operations. This *may* include those involved in corporate governance (e.g., board members, CEOs and presidents), and headquarters-level technical senior management (e.g., security directors, human resources, operations, administration, finance and communications).

Levels I and II are further divided into sublevels, with separate reference curricula tailored to varying working environments and job responsibilities. A more detailed discussion of the guidelines for determining the appropriate personal security training level for an individual is provided in the introduction to Level I below.

The following chart summarizes the overall structure, noting which training levels are recommended for which types of staff.

Figure 7: Selecting the right training level



2. Learning Methodologies

Each level (and, where relevant, sublevel) starts by describing the intended audience, and then turns to relevant core and recommended elective topics. For each topic, it summarizes the scope and then lists key issues the organization should consider including in the training it designs. The list is not exclusive and the organization may choose to include additional issues appropriate to specific needs. **The topics reflect issues relevant to the particular level or sublevel training. The amount of time it takes to cover different topics may vary significantly.** For those familiar with the term "module" as used by the training community, keep in mind that "topic" as used in this document is not the same thing.

The topics can be tailored to create a generic course that works for multiple organizations, or a contextualized course that works across a single organization or a specific operating environment. Generic training allows a diversity of organizations and individuals to participate. In generic training, topics convey more generalized theoretical and practical knowledge and may use simulations and case studies.

Contextualized training can take several forms. The most common are training tailored to a particular organization and training tailored to a specific operating environment. Organization-specific training allows the course to integrate the organization's culture, systems, policies and practices. It is especially suitable for higher-level topics that require deeper field-level strategy discussions about internal and/or confidential issues such as critical incident management. Context-specific training can include individuals from the same organization or from different organizations working in the same operating environment. The training reflects their working realities, using situation-specific knowledge and examples to better address context-relevant considerations and practices.

Each level (I-IV) also lists complimentary trainings and includes a summary table detailing the key objectives, learning outcomes and topics for that level, further broken down by sublevels where applicable. The curriculum does not include suggested timeframes for completing the topics. Organization must set their own timelines based on their particular goals and institutional needs.

Table 1.1 makes it easier to compare how the focus of topics related to key issues varies across different training levels. For example, at Level IV, acceptance focuses on acceptance as a security strategy, while Level III concentrates on how to conceptualize and develop acceptance strategies within a particular context. Level II focuses on understanding and implementing acceptance strategies in a specific context; and Level I concentrates on understanding and implementing acceptance as a personal security strategy. The table can be found below immediately after "3. Evaluation and Monitoring."

This curriculum is built around putting theory into practice. Participants acquire the hard and soft skills they need to conduct their daily security responsibilities. To be effective, organizations must address considerations about how to present the material, including the following:

2.1 Blended approach

Using a blended approach to present the materials is usually more sustainable and effective for training on the job. Elements include:

- In-person workshops;
- Mentoring and peer learning;
- On-the-job learning;
- Learning groups; and
- E-Learning (including online and computer-based topics).

2.2 Supportive environment

The effectiveness of the curriculum also depends on attention to other factors that the organization must address. Examples include:

- Use of a blended learning approach and provision of continuous learning opportunities (formal and informal) for target staff.
- Ongoing, direct support for staff both during participation and afterwards to help them apply what they have learned to their daily work.
- Attention to cultural considerations in designing and implementing the curriculum.
- Incorporating situation-specific security considerations into how and where training is provided (as opposed to providing generic training).

2.3 Other security learning opportunities

Security learning should not be limited to a single training session or online course. The following environments are examples of other situations that organizations should consider using.

2.3.1 New staff orientation

New staff orientation should include some basic components of personal security awareness. Orientation should make clear that personal security is part of operational security. Orientation should also explain the core content of personal security in light of the organization's security architecture and

policies, work assignments, the relevant operating and social context, standards and contingencies. Topics to cover include:

- Overview of the organization's security culture, mission, programs, capacity and values;
- Overview of security responsibilities for various actors (e.g., the country management team, individual staff members and host country authorities);
- Overview of basic principles and rules of international humanitarian law;
- The organization's security and safety policies;
- Overview of relevant humanitarian principles and codes of conduct;
- Other related policies (e.g., sexual harassment);
- Travel policies and procedures;
- Health and wellness;
- Relevant compliance requirements and disciplinary procedures;
- Organizational support resources; and
- Insurance and benefits.

2.3.2 Country-specific security briefings

Country-specific security briefings should provide staff and visitors with the most updated situation-specific information and guidance for security, safety, health risks and security measures specific to a particular area. They are also a valuable opportunity for individuals to ask questions. Ideally, visitors and staff should receive a supporting information package before arrival or travel. Country-specific briefings usually include:

- Situation overview;
- Overview of responsibilities for office and local security;
- Key security risks;
- Related safety and security procedures and contingencies;
- Key health and safety risks, prevention and contingencies;
- Local emergency and medical contacts and outlets;
- Other information such as office contacts, and logistical and other matters specific to the office or operating environment.

2.3.3 Post-assignment debriefs

Post-assignment debriefs are important but often overlooked opportunities for organizations to monitor security matters and support their staff. They afford an opportunity for individuals to report incidents and near-misses, provide feedback on security and safety practices, and to deal with any cumulative, vicarious or traumatic stress. Organizations can use debriefs to support staff by sharing information on support systems available to the person being debriefed.

2.3.4 Staff meetings

Staff meetings can also be used for ongoing security learning. For example, they can be used to highlight important topics, as well as to communicate security-related information or changes. Staff meetings for specific staff members (e.g. guards) can provide additional focus.

3. Evaluation and Monitoring

Training should be monitored and evaluated for both the effectiveness of presentation and for its actual impact on workplace behavior over time. Steps to consider include, for example:

- Monitoring attendance rates and participation to gauge participant involvement and which methods and subjects are well received;
- Collecting participant feedback at the end of the training;
- Having managers assess any changes in behavior or integration of learning into day-to-day performance of security responsibilities by the participant;
- Conducting formal follow-up with participants to evaluate if the training was effective and if it has had an impact on their performance;

Table 1.1: Reference Level Comparison

This table compares how the focus of selected issues varies across different training levels. Each issue is listed in the left-hand column, followed by separate columns explaining the learning goals for that issue at each relevant training level. Red indicates the numbered topic is a core topic. Green indicates the topic is an elective. Boxes without text indicate that the issue is not critical to that level of training. The numbered topics reflect issues relevant to the particular level or sublevel training. The amount of time it takes to cover different topics may vary significantly. For those familiar with the term "module" as used by the training community, keep in mind that "topic" as used in this document is not the same thing.

ISSUE	Level IV GLOBAL STRATEGIC	Level III FIELD STRATEGIC	Level II FIELD OPERATIONAL	Level I: Personal Security IA: BASIC	 IB: ADVANCED	 IC: FOR VIOLENT ENVIRONMENTS
Acceptance	**IV.14 Security Planning** ***Understand*** *acceptance as a security strategy.*	**III.5 Acceptance** ***Conceptualize and develop*** *context-appropriate acceptance strategies.*	**II.A.26 Practical Issues in Building Acceptance** ***Understand, develop and implement*** *context-specific acceptance strategies.*	**I.A.10 Acceptance** ***Understand*** *the link between image, acceptance and security.*	**I.B.5 Acceptance** ***Understand and implement*** *proactive personal acceptance security strategies.*	**I.C.12 Acceptance** ***Understand and implement*** *acceptance as a security strategy in a violent environment.*
Access and Programming	**IV.8 Programming and Security** ***Understand*** *the link between security and programming, highlighting the impact of program design and decisions on security.*	**III.21 Programming and Security** ***Analyze*** *vulnerabilities related to presence, programming and operational habits.* **III.32 Negotiating Access** ***Understand*** *how safe access negotiation can enable programming.* **III.39 Cash Security** ***Understand*** *good practice for cash security and* ***develop*** *mitigation procedures.*	**II.A.4 Programming, Policy, Operations and Security** ***Understand, assess and develop*** *appropriate security measures considering overall vulnerability due to presence, programming and operational habits in the particular working environment.*	**I.A.13 Programming and Security** ***Understand*** *the organization's identity and overall vulnerability due to context-specific presence, programming and operational habits.*		

ISSUE	Level IV GLOBAL STRATEGIC	Level III FIELD STRATEGIC	Level II FIELD OPERATIONAL	Level I: Personal Security IA: BASIC	IB: ADVANCED	IC: FOR VIOLENT ENVIRONMENTS
		III.41 Integrating Safety and Security in Emergency Response ***Understand*** *safety and security for emergency response.*				
Budgeting and Resources for Security	**IV.9 Budgeting and Resources for Security** ***Determine*** *risk management costs and how to adequately finance them.*	**III.12 Budgeting and Resources for Security** ***Understand and develop*** *risk management costs, how these costs are justified to headquarters and donors in proposals and budgets.*				
Civil-Military Relations	**IV.21 Civil-Military Relations** ***Determine*** *guidance and the organization's policy for civil-military relations.*	**III.45 Civil-Military Relations** ***Understand*** *civil-military relations and related security implications in the field.*	**II.A.29 Civil-Military Relations at the Operational Level** ***Understand*** *the security implications of civil-military relations.*			
Communications	**IV.12 Communications and Information Management** ***Effectively communicate and manage*** *information internally and externally.*	**III.13 Information Management** ***Understand*** *how to manage and secure information.* **III.34 Media Training** ***Understand*** *how to work with media in emergency situations.*	**II.A.31 Communicating and Working with Senior Management** ***Understand*** *how to communicate effectively with senior management in the country team.*			**I.B.9 Field Communications** ***Understand and develop skills*** *for different communication technologies and relevant security considerations for effective communications*

ISSUE	Level IV GLOBAL STRATEGIC	Level III FIELD STRATEGIC	Level II FIELD OPERATIONAL	Level I: Personal Security IA: BASIC	 IB: ADVANCED	 IC: FOR VIOLENT ENVIRONMENTS
Context and Situation Analysis		**III.2 Context Assessment and Situational Analysis** ***Analyze*** *the complexity of the working context and* ***use*** *analytical tools to* ***undertake situation analysis.***	**II.A.5 Situational Analysis - Using Security Tools** ***Understand and develop*** *a situational analysis.*	**I.A.3 Situational Awareness** ***Understand*** *situational awareness to assess specific situations and take appropriate action.*	**I.B.2 Situational Analysis** ***Able to assess*** *the complexity of one's working environment.*	
Crisis Management	**IV.6 Crisis Management** ***Develop*** *crisis response process including decision-making roles.*	**III.26 Crisis Management** ***Develop*** *decision-making ability to coordinate a response in conjunction with headquarters.*	**II.A.9 Supporting Incident and Crisis Management** ***Able*** *to support response in crisis situations.*			
Dealing with Aggression	**IV.15 Dealing with Aggression** ***Able*** *to use interpersonal communications skills to defuse aggression in various situations.*	**III.29 Dealing with Aggression** ***Able*** *to use interpersonal communications skills to defuse aggression in various situations.*	**II.A.27 Dealing with Aggression** ***Able*** *to use interpersonal communications skills to defuse aggression in various situations.*	**I.A.12 Dealing with Aggression** ***Equip*** *participants with awareness and techniques in how to best defuse anger and aggression in various situations.*		
Duty of Care	**IV.4 Duty of Care** ***Understand*** *duty of care and legal liability and how to reduce risk of legal actions including through due diligence.*	**III.19 Duty of Care and Legal Liability** ***Understand*** *these terms, the potential impact of legal action, and how to demonstrate due diligence.*				
Engaging Private Security Providers		**III.31 Engaging Private Security Providers** ***Understand*** *important considerations in deciding whether to use private security providers.*				

ISSUE	Level IV GLOBAL STRATEGIC	Level III FIELD STRATEGIC	Level II FIELD OPERATIONAL	Level I: Personal Security IA: BASIC	 IB: ADVANCED	 IC: FOR VIOLENT ENVIRONMENTS
Evacuation, Hibernation, Relocation and Suspension		**III.27 Evacuation, Hibernation, Relocation and Suspension** ***Understand*** *decision making, security considerations, planning and protocols concerning evacuations, hibernation, relocations and suspension.*				**I.B.12 Evacuation, Hibernation and Relocation** ***Understand*** *evacuations, hibernation, relocations and suspension situations and procedures for individual staff members.* **I.B.13 Grab Bags** ***Understand*** *procedures for using grab bags.*
Gender-Based Violence		**III.33 Gender-Based Violence – Prevention and Case Management** ***Understand*** *GBV as a widely under-reported security incident and how to manage staff cases.*		**I.A.9 Gender-Based Violence (GBV)** ***Understand*** *gender-based violence and protection from sexual exploitation and abuse.* ***Awareness*** *of forms, policies, risk, prevention and response and how this differs for men and women.*		
Gendered Cultural and Personal Considerations in Security	**IV.11 Cultural, Gendered and Personal Considerations in Security** ***Appreciate*** *the importance of taking into account staff diversity of cultural, gendered and personal considerations when* ***developing*** *security policies.*	**III.11 Cultural, Gendered and Personal Considerations in Security** ***Understand*** *how specific gendered, cultural and personal considerations of individual staff members affect the organization's duty of care and know how to* ***develop*** *appropriate security strategies.*	**II.A.14 Cultured, Gendered and Personal Considerations** ***Appreciate*** *the importance of considering the gendered, cultural and personal considerations of staff members when developing security plans and related measures.*	**I.A.4 Awareness of Gendered, Cultural and Personal Considerations** ***Awareness*** *of cultural, religious, nationality and gender-specific considerations during travel and how this relates to security.*		

ISSUE	Level IV GLOBAL STRATEGIC	Level III FIELD STRATEGIC	Level II FIELD OPERATIONAL	Level I: Personal Security IA: BASIC	IB: ADVANCED	IC: FOR VIOLENT ENVIRONMENTS
Guards and Drivers		**III.25 Managing Guards and Drivers** ***Understand and manage*** *guards and drivers.*	**II.A.16 Managing Guards and Drivers** ***Manage and effectively communicate*** *with guards and drivers, including training and supervision as part of related procedures and standards.*			
Health and Wellness		**III.43 Health and Wellness** ***Understand*** *health and wellness considerations and logistics.*				
Hostile Observation Awareness		**III.42 Hostile Observation Awareness** ***Understand*** *the risks of hostile observation and* ***develop*** *preventive and responsive procedures.*	**II.A.30 Hostile Observation Awareness** ***Awareness*** *of hostile observation activities, and able to* ***implement*** *preventive and responsive procedures.*	**I.A.14 Hostile Observation Awareness** ***Awareness*** *of hostile observation activities, identify the risks of hostile observation and develop preventive and responsive procedures.*		
Human Resources	**IV. 10 Human Resources and Security** ***Understand*** *HR-related security issues requiring executive-level consideration.*	**III.10 HR and Security** ***Understand*** *how HR issues can affect security.*				

ISSUE	Level IV GLOBAL STRATEGIC	Level III FIELD STRATEGIC	Level II FIELD OPERATIONAL	Level I: Personal Security IA: BASIC	 IB: ADVANCED	 IC: FOR VIOLENT ENVIRONMENTS
Implementing Partners	**IV.17 Security Implications of Working with Implementing Partners** ***Understand*** *security policy and practical implications of remote management and working with implementing partners, including possible moral and legal responsibilities related to transference of risk.*	**III.36 Working with Implementing Partners: Security Considerations** ***Understand*** *issues related to security and local implementing partners, and* ***develop*** *tools to improve security management support for them.*				
Implementation and Compliance	**IV.13 Implementation and Compliance** ***Implement*** *the organization's security principles, operating standards and security measures to ensure compliance by the organization's staff.*	**III.7 Implementation and Compliance** ***Implement*** *the organization's security principles, operating standards and security measures to ensure compliance by the organization's staff.*	**II.A.23 Practical Issues in Implementing Security** ***Understand*** *how to implement the organization's security principles and operating procedures in the local context.*			

ISSUE	Level IV GLOBAL STRATEGIC	Level III FIELD STRATEGIC	Level II FIELD OPERATIONAL	Level I: Personal Security IA: BASIC	IB: ADVANCED	IC: FOR VIOLENT ENVIRONMENTS
Incidents (Reporting, Analysis and Recovery)	**IV.18 Incident Reporting, Monitoring and Analysis** ***Understand*** *the importance of and good practice for incident reporting and the critical need to analyze data at an organization-wide level.*	**III.22 Incident Reporting, Monitoring and Analysis** ***Develop*** *appropriate incident reporting and analysis systems, including how to integrate findings into security management revisions at various levels.* **III.23 Managing the Full Spectrum of Incidents and Post-Incident Recovery** ***Able to manage*** *specific incidents and* ***understand*** *post-incident recovery mechanisms.*	**II.A.10 Incident Reporting and Analysis** ***Understand*** *the importance and good practice for incident reporting, the organization's reporting system and the participant's role; able to* ***implement*** *incident reporting and analysis at country and field levels.*	**I.A.11 Incident Reporting** ***Understand*** *the importance of reporting incidents and near-misses, including options for reporting incidents, near-misses and sensitive incidents while maintaining confidentiality.*		
Information Security and Management	**IV.12 Communications and Information Management** ***Understand*** *internal and external communications and information management and security in order to* ***develop*** *related policies and protocols.*	**III.13 Information Management and Security** ***Develop*** *information management and security procedures.*	**II.A.20 Information Management and Security** ***Implement and monitor*** *the organization's information management and security measures.*	**I.A.15 Information Security** ***Understand*** *information security to support personal awareness of external surveillance and related organizational practices.*		

ISSUE	Level IV GLOBAL STRATEGIC	Level III FIELD STRATEGIC	Level II FIELD OPERATIONAL	Level I: Personal Security IA: BASIC	IB: ADVANCED	IC: FOR VIOLENT ENVIRONMENTS
International Legal Instruments and Humanitarian Frameworks and Principles	**IV.2 Strategic Planning** ***Understand*** *relevant international humanitarian law and how it relates to strategic planning for the organization.*	**III.28 International Legal Frameworks** ***Understand*** *how guiding humanitarian principles and legal frameworks relate to safety and security and how they can be used to increase security and protection of civilians and aid workers.*	**II.A.1 Humanitarian Principles and International Humanitarian Law** ***Understand*** *key concepts of international legal frameworks and how they relate to the organization's security management.*			
Leadership and Management	**IV.3 Security Management Architecture and Capacity** ***Understand*** *security management options to clarify security management architecture, roles, responsibilities and reporting lines.*	**III.9 Leadership and Management at the Country and Regional Levels** ***Understand and develop*** *good management and leadership skills for better acceptance of and compliance with security polices and measures.*	**II.A.15 Leadership and Management** ***Understand*** *good management and leadership skills to increase staff acceptance of and compliance with security procedures.*			
Mainstreaming Security	**IV.1 Security Risk Management** ***Understand*** *the most relevant framework(s) for security risk management to ensure a systematic approach to managing security throughout the culture of the organization.*	**III.7 Implementation and Compliance** ***Implement*** *security risk management consistently to ensure a systematic approach to managing security throughout the organization.*	**II.A.31 Communicating and Working with Senior Management** ***Able to*** *effectively communicate and work with the organization's country senior management.*			

ISSUE	Level IV GLOBAL STRATEGIC	Level III FIELD STRATEGIC	Level II FIELD OPERATIONAL	Level I: Personal Security IA: BASIC	IB: ADVANCED	IC: FOR VIOLENT ENVIRONMENTS
Media	**IV.12 Communications and Information Management** ***Understand*** *external communications* ***develop*** *policies and protocols for dealing with media.*	**III.34 Media Training** ***Understand*** *and* ***able to implement*** *organizational policies for dealing with the media in emergency situations.*				
Monitoring Security			**II.A.24 Monitoring Security on a Daily Basis** ***Implement*** *monitoring procedures for activities and travel movements on a daily basis.*			
Operational Continuity	**IV.7 Risk Management and Operational Continuity** ***Understand and develop*** *policy on comprehensive risk management and operational continuity.*	**III.44 Operational Continuity** ***Understand and develop*** *security-related plans for operational continuity based on the organization's continuity policies and concepts.*				
Organization Security Management and Architecture	**IV.3 Security Management Architecture and Capacity** ***Understand*** *options to clarify existing security management positions, roles, responsibilities and reporting lines.*	**III.17 The Organization's Security Management Architecture** ***Understand*** *the organization's security management policies, architecture, reporting lines, and related roles and responsibilities.*	**II.A.2 Roles and Responsibilities** ***Awareness*** *of the organization's security structure and the roles and responsibilities within it.*			

ISSUE	Level IV GLOBAL STRATEGIC	Level III FIELD STRATEGIC	Level II FIELD OPERATIONAL	Level I: Personal Security IA: BASIC	IB: ADVANCED	IC: FOR VIOLENT ENVIRONMENTS
Orientation and Training		**III.20 Security and Training** ***Develop and deliver*** *security orientations and trainings.*	**II.A.21 Security Briefings and Orientations** ***Develop and deliver*** *security orientations and briefings.*			
Personal Awareness				**I.A.2 Personal Awareness and Behavior** ***Awareness*** *of one's personal strengths, weaknesses, behavioral habits and attitudes to security.*		
Policy, Principles and Standards	**IV.5 Security Policy, Principles, Standards and Guidance** ***Able to develop,*** *revise and implement the organization's security policy.*		**II.A.4 Programming, Policy, Operations and Security** ***Understand*** *how to assess the organization's mission and overall vulnerability where the participant works, based on its local presence, programming and operational habits.*			
Remote Management and Transfer of Risk	**IV.17 Security Implications of Working with Implementing Partners** ***Understand*** *security policy and practical implications of remote management and working with implementing partners, including possible moral and legal responsibilities related to transference of risk.*	**III.37 Security Implications of Remote Management of Programs** ***Understand*** *and* ***able to implement*** *remote management of programs considering issues of transfer of risk.*				

ISSUE	Level IV GLOBAL STRATEGIC	Level III FIELD STRATEGIC	Level II FIELD OPERATIONAL	Level I: Personal Security IA: BASIC	IB: ADVANCED	IC: FOR VIOLENT ENVIRONMENTS
Residential and Office Security		**III.16 Site Selection and Security** ***Evaluate and select*** *sites that optimize safety and security while achieving operational objectives.*	**II.A.19 Site Security** ***Understand*** *site security management activities to optimize the safety and security of staff and property.*		**I.B.7 Residential and Office Security** ***Understand*** *key measures for residential and office security.*	
Risk Reduction Strategies		**III.4 Risk Reduction Strategies** ***Understand and develop*** *security strategies for appropriate risk reduction measures.*	**II.A.7 Risk Reduction Strategies** ***Understand*** *and* ***apply*** *security strategies and appropriate risk reduction measures.*	**I.A.5 Personal Risk Assessment and Risk Reduction** **Understand** and **apply** personal risk assessment and risk reduction measures.	**I.A.5 Personal Risk Assessment and Risk Reduction** **Understand** and **apply** personal risk assessment and risk reduction measures. **I.B.4 Risk Reduction Strategies** ***Understand*** *specific security strategies for reducing security risk.*	
Risk Threat and Vulnerability		**III.3 Risk Assessments and Understanding Risk Thresholds** ***Develop*** *skills to assess security risk and establish thresholds of acceptable risk.*	**II.A.6 Risk Assessments** ***Develop*** *practical skills to assess situation-specific security risk.*	**I.A.5 Personal Risk Assessment and Risk Reduction** ***Understand*** *what threat and vulnerability mean, the link to programming and how to assess real or perceived risk*	**I.B.3 Risk Assessment** ***Able to assess*** *situation-specific security risks to make more informed decisions on how to best reduce risk exposure and minimize the potential impact.*	
Safety Threats					**I.B.11 Safety Threats** ***Understand*** *safety and how to assess safety risks in specific working environments.*	

ISSUE	Level IV GLOBAL STRATEGIC	Level III FIELD STRATEGIC	Level II FIELD OPERATIONAL	Level I: Personal Security IA: BASIC	 IB: ADVANCED	 IC: FOR VIOLENT ENVIRONMENTS
Saving Lives Together	**IV.23 Saving Lives Together** ***Understand*** *the principles of SLT.*	**III.46 Saving Lives Together** ***Understand*** *SLT, ways to use it and manage expectations.*	**II.A.32 Saving Lives Together** ***Understand*** *how SLT works at the field level.*			
Security Assessments		**III.15 Field Security Assessments, Advisory and Monitoring Activities** ***Understand and able to conduct*** *field security assessments, advisory and monitoring activities.*	**II.A.5 Situation Analysis – Using Security Tools** ***Able to*** *assess the working environment (country and location-specific);* ***understand*** *available situational analysis tools and how to use them.* **II.A.13 Consultative Processes** ***Understand*** *consultative approaches to elicit staff thoughts on and strengthen support for the organization's security policies and measures.*			
Security Planning	**IV.19 Security Planning** ***Understand*** *strategies, techniques and tools to develop, monitor, evaluate and revise security plans.*	**III.6 Security Planning – Development and Review** ***Develop, implement, monitor, and revise*** *security plans.*	**II.A.8 Standard Operating Procedures and Contingency Planning** ***Develop and implement*** *field-level standard operating procedures and contingency plans using security risk reduction strategies.*			

ISSUE	Level IV GLOBAL STRATEGIC	Level III FIELD STRATEGIC	Level II FIELD OPERATIONAL	Level I: Personal Security IA: BASIC	IB: ADVANCED	IC: FOR VIOLENT ENVIRONMENTS
			II.A.25 Practical Issues in Updating Security Information and Planning ***Update*** *security information and planning and effectively* ***communicate*** *changes.*			
Security Risk Management Frameworks	**IV.1 Security Risk Management** ***Understand*** *the most relevant framework(s) to systematically integrate security risk management throughout the organization's culture and operations.* **IV.7 Risk Management and Operational Continuity** ***Understand*** *comprehensive risk management.*	**III.1 Security Risk Management Frameworks** ***Understand*** *security risk management frameworks and* ***able to identify and apply*** *the best framework for an organization.*	**II.A.3 Security Risk Management Framework** ***Understand and able to implement*** *an effective security management framework.*	**I.A.1 NGO Security Concepts** ***Understand*** *the most relevant security concepts and terminology to enable a common understanding of security.*	**I.B.1 Security Framework** ***Understand*** *the most relevant security risk management framework for the organization and for the participant's work.*	
Security Roles, Responsibilities			**II.A.2 Roles and Responsibilities** **Understand** the organization's *security structure and the roles and responsibilities within it.*			

ISSUE	Level IV GLOBAL STRATEGIC	Level III FIELD STRATEGIC	Level II FIELD OPERATIONAL	Level I: Personal Security IA: BASIC	 IB: ADVANCED	 IC: FOR VIOLENT ENVIRONMENTS
Security Self-Assessments		**III.24 Security Self-Assessments and Audits** ***Understand*** *and able to* ***audit*** *all aspects of the organization's security management practices for a specific office or location.*				
Security Stakeholders and Coordination	**IV.20 Security Networks** ***Understand*** *security information and coordination platforms and headquarters-level security stakeholders.*	**III.14 Security Stakeholders** ***Analyze*** *motives, attitudes and relationships of actors who might influence programmatic success including security.* **III.30 Security Networks** ***Understand*** *networks, their benefits and how to use them.*	**II.A.12 Security Stakeholders** ***Understand and analyze*** *motives, attitudes and relationships of actors who might influence programmatic success.* ***Understand*** *security initiatives, how they may be accessed, and what benefits and support they can provide.*		**I.B.10 Security Stakeholders** ***Understand*** *how to identify, analyze and interact with stakeholders and actors who might influence security and programs.*	
Strategic Planning	**IV.2 Strategic Planning** ***Develop and integrate*** *security within the organization's strategic planning processes to guide the organization's overall leadership, staff and stakeholders.*					

ISSUE	Level IV GLOBAL STRATEGIC	Level III FIELD STRATEGIC	Level II FIELD OPERATIONAL	Level I: Personal Security IA: BASIC	IB: ADVANCED	IC: FOR VIOLENT ENVIRONMENTS
Stress Management	**IV.16 Stress Management in Traumatic or Critical Incidents** ***Understand*** *the importance of psycho-social well-being to an organization; able to use an evidence-based approach to* ***develop*** *related policy.*	**III.8 Stress Management in Traumatic or Critical Incidents** ***Able to prepare for and implement*** *response to traumatic or critical incidents using an evidence-based approach.*	**II.A.11 Stress Management** ***Understand*** *stress and able to* ***develop*** *coping and resilience mechanisms.*	**I.A.7 Resiliency and Stress Management** ***Understand, recognize*** *and* ***manage*** *different types of stress.*	**I.B.8 Personal and Team Resilience** ***Cultivate*** *personal and team resilience dealing with trauma and traumatic events including critical incident response.*	
Threat-Specific		**III.38 Kidnapping, Abduction and Hostage Taking** ***Understand*** *these security threats and able to* ***develop*** *measures to reduce the probability and impact.* **III.40 Managing Situation-Specific Threats and Incidents** ***Understand*** *and able to* ***manage*** *context-specific security threats.*		**I.A.8 Crime Awareness and Prevention** ***Aware*** *of different criminal threats and good practice in prevention and response.*	***Aware of*** *and able to* ***respond*** *to the following situation specific security risks:* **I.C.1** Terrorism **I.C.2** Improvised Explosive Devices and Bombs **I.C.3** Landmines and Explosive Remnants of War (Unexploded Ordnance) **I.C.4** Indirect and Direct Fire, Shelling and Weapons **I.C.5** Crowds, Mobs and Demonstrations **I.C.6** Kidnapping, Abduction and Hostage Taking **I.C.7** Advanced Hostile Observation Awareness **I.C.8** Hostile Checkpoints **I.C.9** Helicopter Landing Procedures **I.C.10** Convoy travel **I.C.11** Protective Equipment **I.C.12** Acceptance	

ISSUE	Level IV GLOBAL STRATEGIC	Level III FIELD STRATEGIC	Level II FIELD OPERATIONAL	Level I: Personal Security IA: BASIC	IB: ADVANCED	IC: FOR VIOLENT ENVIRONMENTS
Travel Safety and Security			**II.A.17 Travel Safety and Security** *Daily oversight and* ***management*** *of travel protocols and activities.*	**I.A.6 Travel Safety** ***Understand*** *how to prepare before travel and deployments, and considerations during travel.*		
Vehicle and Fleet Safety and Security			**II.A.18 Travel and Movement Tracking** ***Understand and apply*** *effectively and consistently conduct travel and movements tracking.*		**I.B.6 Travel Safety and Security** ***Understand*** *vehicle and travel safety including how to prevent and respond in vehicle related incidents.*	
Using Armed Guards and Escorts	**IV.22 Using Armed Guards and Escorts** ***Understand*** *considerations and issues that can inform decisions regarding the use of armed protection; able to* ***develop*** *appropriate policies.*	**III.35 Working with Armed Protection and Private Security Companies** ***Understand*** *considerations and issues for* ***selecting and using*** *armed protection including private security companies.*	**II.A.28 Working with Armed Escorts and Private Security Companies** ***Understand*** *the issues related to working with armed protection.*			

Level I Personal Safety and Security

NGO Security Training Curriculum

4. REFERENCE CURRICULUM

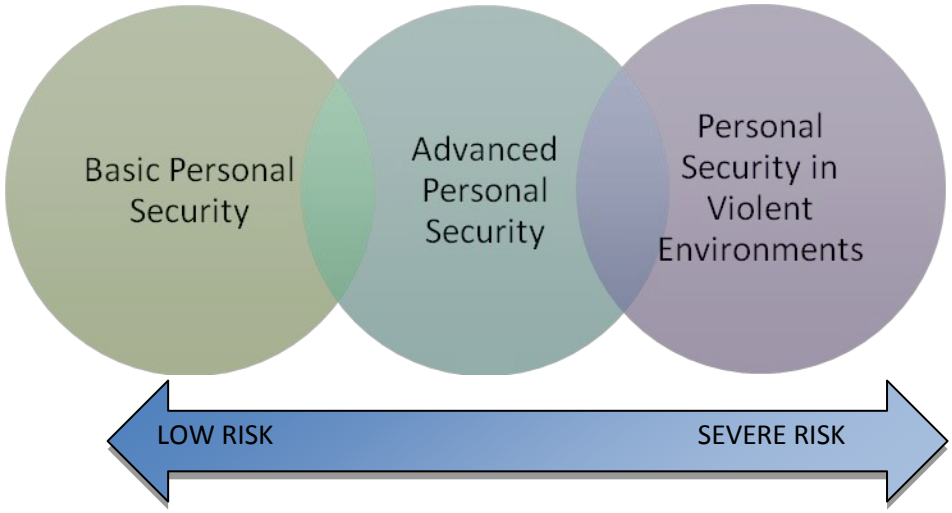
Level I Personal Safety and Security

Introduction

The goal of Level I is to provide humanitarian and development workers with personal safety and security awareness training to help them keep safe while carrying out their work. It is aimed at individual staff members and volunteers, and is based on the principle that each staff member's safety and security is fundamental to the organization's overall security and programmatic effectiveness.

Different operating environments involve differing levels of risk, and training must match content with risk level. Therefore, the personal security training in Level I has three sublevels designed to fulfill staff needs in different risk conditions ranging from low to severe:

Level IA - Basic Personal Security
Level IB - Advanced Personal Security
Level IC - Personal Security in Violent Environments



Different Personal Security Training Needs for Different Staff. Figure 1.2 can be used to help determine which sublevel of personal security training a person may need for a particular situation. If a training needs assessment has been conducted (see Section A 3.3 and Guidance Tool A) or the organization has a learning and development strategy (see Section A 3.2 and Guidance Tool B), Figure 1.2 should be used in conjunction with those materials.

	Security Risk Level			
Staff Exposure	**Low**	**Medium**	**High**	**Severe**
Travellers	IA - Basic Personal Security	IB - Advanced Personal Security	IB - Advanced Personal Security	IC - Personal Security in Violent Environments
Deployed - short term	IA - Basic Personal Security	IB - Advanced Personal Security	IB - Advanced Personal Security	IC - Personal Security in Violent Environments
Deployed – long term	IA - Basic Personal Security	IB - Advanced Personal Security	IC - Personal Security in Violent Environments	IC - Personal Security in Violent Environments
Permanent international, national and local staff	IA - Basic Personal Security	IB - Advanced Personal Security	IC - Personal Security in Violent Environments	IC - Personal Security in Violent Environments

Level IA - Basic Personal Security: This level of personal security training provides basic security and personal awareness training for staff who work in or travel to low security risk situations. It emphasizes teaching practical skills, good practices, and general safety and security guidance.

Level IB - Advanced Personal Security: This level targets all staff travelling to or based in medium-risk security environments. It is also for staff who travel to or who undertake short-term deployments to high-risk environments. It provides more technical information about good practices, increased levels of self-awareness and team cohesion concerning security. It also reinforces key points and deepens understanding through simulations and scenarios.

It includes all components of IA Basic Personal Security in addition to other relevant core and elective topics and introduces conceptual notions central to NGO security. It requires staff members to understand the concepts and be able to apply them in different contexts.

Level IC- Personal Security in Violent Environments: This is an intensive, threat-specific level of personal security training. It is for individuals travelling to or based in severe risk environments. It is also for staff on long-term deployments in high-risk environments and permanent staff (international, national and local) in high-risk environments. It includes high- and severe-threat situation-specific information, protocols, more active simulations and scenarios.

Level IC includes the topics covered in IA and IB Personal Security, with additional focus on specific and relevant topics. Keep in mind that at this level in-country staff may have different training needs than international staff. Training must to be tailored to meet the particular needs of each group.

This table provides a comparative overview of the three sublevels in Level I, with IA as the most basic and IC as the most advanced. Each subsequent sublevel assumes that the material in the previous sublevel has been covered in a separate training course or will be covered in the course being provided. For example, Level IB would include topics in Level IA, or participants would complete a IA course before taking the Level IB course. The topics reflect issues relevant to the particular level or sublevel training. The amount of time it takes to cover different topics may vary significantly. For those familiar with the term "module" as used by the training community, keep in mind that "topic" as used in this document is not the same thing.

	IA BASIC PERSONAL SECURITY	IB ADVANCED PERSONAL SECURITY	IC PERSONAL SECURITY IN VIOLENT ENVIRONMENTS
GOAL	Provide an introduction to personal security and how one's behavior affects safety and security by teaching participants about self-awareness, relevant security matters and how to respond to security risks in low-risk environments.	Develop self and team awareness for higher security risk environments by teaching participants' security management and good practices in prevention and response to security situations.	Teach participants the contextualized security awareness and skills (prevention and response) they need for specific security threats in severe security risk environments.
KEY OBJECTIVES	1. Encourage self-reflection about personal vulnerabilities, limits, strengths, resilience, emotional intelligence and other key objectives. 2. Explain the operating environment and cultural, gender and personal considerations as they relate to security.	1. Explain how to recognize and analyze security risks in medium- to high-risk working environments. 2. Provide an overview of security management concepts, good practice and strategies. 3. Prepare participants to assess and manage situation-specific security and safety risks.	1. Teach participants about threats and risk in their in working environments and their and their organization's vulnerability to these threats. 2. Provide guidance on how to prevent and respond to specific threats.

	3. Present security concepts and how they relate to security strategies and programming. 4. Explain common threats and present information on good practice in personal security response. 5. Explain how to develop a personal safety and security strategy and set a personal risk threshold.	4. Prepare participants to identify, mitigate and respond to security threats (training includes use of simulations. 5. Encourage additional self-assessment to help participants refine their personal risk thresholds.	3. Explain risk mitigation and teach participants how to use mitigation tools; use simulation exercises to help participants practice and to test participant mastery of those skills and their skills for identifying and responding to security risks.
TOPIC	***Core topics:*** I.A.1 NGO Security Concepts I.A.2 Personal Awareness and Behavior I.A.3 Situational Awareness I.A.4 Awareness of Gendered, Cultural and Personal Considerations I.A.5 Personal Risk Assessment and Risk Reduction I.A.6 Travel Safety I.A.7 Resiliency and Stress Management I.A.8 Crime Awareness and Prevention I.A.9 Gender-Based Violence (GBV) I.A.10 Acceptance I.A.11 Incident Reporting I.A.12 Dealing with Aggression I.A.13 Programming and Security I.A.14 Hostile Observation Awareness I.A.15 Information Security	***All materials covered in Basic Personal Security (1A) plus the following core topics:*** I.B.1 Security Framework I.B.2 Situational Analysis I.B.3 Risk Assessment I.B.4 Risk Reduction Strategies I.B.5 Acceptance I.B.6 Travel Safety and Security I.B.7 Residential and Office Security I.B.8 Personal and Team Resilience I.B.9 Field Communications I.B.10 Security Stakeholders I.B.11 Safety Threats I.B.12 Evacuation, Hibernation, Relocation I.B.13 Grab Bags	***All materials covered in Basic and Advanced Personal Security (IA and IB) plus choice of elective topics based on context and security. Electives menu:*** I.C.1 Terrorism I.C.2 Improvised Explosive Devices and Bombs I.C.3 Landmines and Explosive Remnants of War (Unexploded Ordnance) I.C.4 Indirect and Direct Fire, Shelling and Weapons I.C.5 Crowds, Mobs and Demonstrations I.C.6 Kidnapping, Abduction and Hostage Taking I.C.7 Advanced Hostile Observation Awareness I.C.8 Hostile Checkpoints I.C.9 Helicopter Landing Procedures I.C.10 Convoy Travel I.C.11 Protective Equipment I.C.12 Acceptance

Level IA - Basic Personal Security

This level of personal security training provides staff members with a general introduction to personal security and how one's behaviour affects safety and security.

Level IA covers the basic safety and security training needed for staff whose work and travel only involves low-risk environments. It teaches participants self-awareness and familiarizes them with security matters relevant to their work and how to respond to security risks in low-risk environments.

The curriculum is divided into topics. After covering some general issues, this section reviews each topic. It first summarizes the scope of the topic and then lists key content the organization can include in the training it designs. The list is not exhaustive and the organization may choose to add other topics as well. Additional information on other aspects of course design can be found in the introduction to Section B above. This includes learning methodologies, creating a supportive environment, other learning opportunities, and monitoring and evaluation.

Target Audience. Staff members whose work and travel is limited to low security risk situations.

Complimentary Trainings. Training in the following matters may be useful to supplement the materials covered in this curriculum:

- Basic first aid and CPR
- Safety training: fire, building evacuation

Topics

Core Topics

I.A.1 NGO Security Concepts
I.A.2 Personal Awareness and Behavior
I.A.3 Situational Awareness
I.A.4 Awareness of Cultural, Gendered and Personal Considerations
I.A.5 Personal Risk Assessment and Risk Reduction
I.A.6 Travel safety
I.A.7 Resiliency and Stress Management
I.A.8 Crime Awareness and Prevention
I.A.9 Gender-Based Violence (GBV)
I.A.10 Acceptance
I.A.11 Incident Reporting
I.A.12 Dealing with Aggression
I.A.13 Programming and Security
I.A.14 Hostile Observation Awareness
I.A.15 Information Security

Topic Details

I.A.1 NGO Security Concepts . Overview of key security concepts for NGO workers.

Key points include but are not limited to:
- Defining security and safety, and understanding the difference between the two concepts.
- Trends and issues in the global security picture for humanitarian and development workers.
- Overview of security management frameworks.
- Overview of security planning and what related training and support staff members should expect to receive (e.g., briefings, standard operating procedures)
- Explanation of security terms such as risk, vulnerability and threat and risk reduction strategies.
- Overview of location-specific security phases.

I.A.2 Personal Awareness and Behavior

Understanding one's personal strengths, weaknesses, behavioral habits and attitudes concerning security.

Key points include but are not limited to:
- Understanding how participants' self-perceptions and behavior affect their personal security.
- Impact of individual behavior on their personal security.
- Understanding one's impact on the local community and how that affects one's security. Impact of presence in the field – awareness of image.
- Assessing personal weaknesses, habits and strengths.
- How to recognize and manage fear and panic.
- Understanding the behavioral arousal cycle and what responses and characteristics accompany each phase.

I.A.3 Situational Awareness

How to examine the operating environment and related security issues.

Key points include but are not limited to:
- What participants need to know to understand their operating context.
- Situation-specific considerations.
- How to be aware of one's immediate surroundings and how to react.

I.A.4 Awareness of Cultural, Gendered and Personal Considerations

Strengthened participant sensitivity to personal and societal factors that affect security realities in their operating environment and during travel. These factors include gender, sexual orientation, religion, cultural and personal considerations such as disabilities.

Key points to include but are not limited to:
- How to assess different notions and understandings of security and safety, and what this means in relation to cultural, gender and personal considerations.
- Overview of personal, cultural and organizational considerations (e.g., age, ethnicity, nationality, disabilities, religion, and job position in the organization).
- Defining gender and gender-specific security considerations.
- Closer examination of personal behavior and how it relates to the local culture and perceptions.

I.A.5 Personal Risk Assessment and Risk Reduction

Understanding threat and vulnerability in the participant's operating environment, and how to understand, assess, and manage risks.

Key points to include but are not limited to:

- Different types of threat.
- Vulnerability to threats.
- Possible strategies to reduce security and safety risks.
- Basic personal security measures.
- Setting a personal risk threshold.

I.A.6 Travel Safety

How to prepare before travel and deployments, and considerations during travel.

Key points include but are not limited to:

- The organization's procedures and other good practices in preparing for travel and deployments.
- Good practice while on travel or deployment, including what to bring, communications, airports, arrivals, using taxis, airports, hotels and other accommodations.

I.A.7 Resiliency and Stress Management

Understanding, recognizing and managing different types of stress.

Key points include but are not limited to:

- Overview of different types of stress.
- Signs and symptoms of stress.
- Understanding resilience and emotional intelligence.
- How to develop personal resilience.
- Techniques for managing stress, including when and how to seek support.

I.A.8 Crime Awareness and Prevention

Understanding different criminal threats and good practice in prevention and response.

Key points include but are not limited to:

- Overview of various criminal motives and likely threats.
- Good practice in prevention.
- How to react during a robbery.

I.A.9 Gender-Based Violence (GBV)

Understanding GBV as a widely under-reported type of security incident.

Key points include but are not limited to:

- Defining GBV.
- Overview of the types of GBV.
- Overview of causes.
- The role of power in GBV.
- Understanding which personnel in the organization are most at risk.

- Identify the causes and contributing factors of GBV.
- Physical, psychological and social consequences survivors of GBV may face.
- Overview of organization-related policies and codes of conduct.
- Overview of the prevention and response measures available through the organization and in the participant's work environment.
- Overview of relevant incident reporting mechanisms and confidentiality measures.

I.A.10 Acceptance

Understanding, cultivating and verifying acceptance. Active acceptance is increasingly relevant in operational situations.

Key points to include but are not limited to:

- Overview of the acceptance approach to security.
- The link between image and acceptance.
- How an individual's behaviour can affect acceptance.
- How different groups may perceive the individual and the organization in the participant's working environment.
- Key and cross-cutting components of acceptance (e.g., stakeholders, programming, staffing decisions, behavior and composition).
- Tools to develop and strengthen acceptance.

I.A.11 Incident Reporting

Overview of the organization's incident reporting systems and rules, and how participants can report incidents, near-misses and sensitive incidents.

Key points to include but are not limited to:

- Defining what constitutes an incident and what is a near-miss and what is a sensitive incident.
- The importance of reporting incidents and near-misses.
- Incident reporting options: overview of the organization's incident reporting channels and other related policies such as whistle-blowing, and reporting sexual exploitation and abuse.
- Review of the organization's incident reporting and post-incident reporting protocols.

I.A.12 Dealing with Aggression

How to use interpersonal communications skills to defuse anger and aggression in various situations.

Key points to include but are not limited to:

- Principles of communication.
- Overview of different types of aggression and anger, and how to recognize their symptoms.
- Understanding the cultural dimension of anger and aggression.
- Techniques for de-escalating anger and aggression.

I.A.13 Programming and Security

Understanding the organization's identity and overall vulnerability due to presence, programming and operational habits in the participant's working environment.

Key points include but are not limited to:

- Review of the organization's local programming profile and potential security implications.
- Understanding the interdependence of programming and security, and the importance of integrating them.
- The project cycle and how a security framework correlates to it.
- Programming and potential security implications.
- How to conduct security assessments and implement risk reduction measures.
- How to budget for security, including needs such as training, security assets, site enhancements and security staff.

I.A.14 Hostile Observation Awareness

How to detect hostile observation activities, identify the risks of hostile observation, and develop preventive and responsive procedures.

Key points to include but are not limited to:

- The difference between surveillance and hostile observation.
- How to recognize potential signs of hostile observation activities.
- How to prevent hostile observation and other unwanted surveillance (general and context-specific).
- How to safely signal the presence of hostile observation activities to the right channels.

I.A.15 Information Security

Understanding information security and developing personal awareness of external surveillance.

Key points to include but are not limited to:

- Understanding information security concerns and needs, including concerns about social media.
- Overview of the organization's current and potential policies and measures concerning information management.
- How these measures and policies relate to the participant's work.
- Understanding surveillance and when it can become hostile.
- IT security considerations and organizational IT security systems (e.g., intranets, encryption, social media and security).
- Good practice in working with sensitive organizational, security, programming and operational information.

The Level IB - Advanced Personal Security

Level IIB provides self and team security awareness training for individuals operating in medium security risk environments. It is also for people travelling to or on short-term deployments in high security risk environments. It teaches participants personal security management and good practices in prevention and response to security situations.

The curriculum is divided into topics. After covering some general issues, this section reviews each topic. It first summarizes the scope of the topic and then lists content the organization can include in the training it designs. The list is not exclusive and the organization may choose to add other topics as well. Additional information on other aspects of course design can be found in the introduction to Section B above. This includes learning methodologies, creating a supportive environment, other learning opportunities, and monitoring and evaluation.

Target Audience

All staff travelling to or based in medium security risk situations, and all staff travelling to or on short-term deployment in high security risk environments.

Complimentary Trainings

Training in the following matters may be useful to supplement the materials covered in this curriculum.

- Basic or advanced first aid and CPR
- Safety training: fire, building evacuation

Learning Methodology

In addition to taking into account the general guidance on learning methodology provided above in the introduction to Section B, training techniques at this level must also address other needs. Most importantly, training at this level should involve participants in simulations to help them better understand how they might react in a crisis and what they need to do in such cases. Including some simulation exercises can enhance effectiveness of training at this level.

Organizations and trainers also need to bear in mind that such exercises can result in significant emotional stress for participants. As a result, organizations and trainers must take particular care to ensure that simulations are conducted in a way that does not unduly stress participants. The training should also include ways to support participants who need to process the stress they experience during the simulations.

Topics

Participants taking an advanced personal security training must cover all material in level IA prior to this level of training or must cover it as part of this level of training.

Core Topics

I.B.1 Security Framework
I.B.2 Situational Analysis
I.B.3 Risk Assessment
I.B.4 Risk Reduction Strategies
I.B.5 Acceptance
I.B.6 Travel Safety and Security

I.B.7 Residential and Office Security
I.B.8 Personal and Team Resilience
I.B.9 Field Communications
I.B.10 Security Stakeholders
I.B.11 Safety Threats
I.B.12 Evacuation, Hibernation, Relocation
I.B.13 Grab Bags

Topic Details

I.B.1 Security Framework

Understanding the security risk management framework that applies to the organization and the participant's work.

Key points include but are not limited to:

- Overview of key components of the relevant security management framework.
- Overview of cross-cutting issues related to the framework.
- When and how to revise security plans.

I.B.2 Situational Analysis

How to assess the participant's working environment.

Key points include but are not limited to:

- Overview of relevant information sources and their credibility (e.g., media, published, key informants, information coordination platforms, participatory discussions and consultation).
- The political, economic, socio-cultural, geographical and technological context in which the office operates.
- How to analyze the working environment using tools such as actor mapping, conflict analysis, violence mapping, conflict mapping, and political and economic analysis.
- Understanding the interdependence of security and the organization's presence and programming.
- Understanding how perceptions can vary and how those differences can affect the participant's work environment.
- How to use scenarios to identify and prepare for changes in the security situation.

I.B.3 Risk Assessment

How to assess situation-specific security risks. This enables participants to make more informed decisions on how to best reduce their risk exposure and minimize the potential impact.

Key points include but are not limited to:

- Defining the terms threat, vulnerability and risk.
- The relationship between the three.
- How to carry out a personal risk assessment, identifying and prioritizing context-specific threats.
- How to assess the risk.
- The importance of continuously re-evaluating and updating risk assessments.

I.B.4 Risk Reduction Strategies

Overview of risk reduction strategies (including the organization's) for reducing the participant's personal security risk.

Key points include but are not limited to:

- Overview of different types of risk reduction strategies, their advantages and disadvantages.
- Different ways strategies are implemented and the impact on local perceptions.
- The current organizational culture and strategies to reduce security and safety risks.
- How an organization's security strategies affect personal behavior and vice versa.

I.B.5 Acceptance

Understanding the acceptance approach to security. Active acceptance is increasingly relevant in operational situations.

Key aspects of this topic include but are not limited to:

- Key and cross-cutting components of acceptance (e.g., stakeholders, programming, staffing decisions, behavior and composition).
- Review of the organization's concept and strategy.
- Challenges to realizing that strategy in the participant's operating environment.
- Overview of degrees of acceptance and understanding the dynamic nature of consent.
- Image and perception (i.e., factors affecting acceptance and how to assess level of acceptance).

I.B.6 Travel Safety and Security

Good practice in travel safety, including how to prevent and respond to vehicle-related incidents.

Key points include but are not limited to:

- Understanding road, water and air safety and security risks.
- Selecting effective measures to reduce risk
- Vehicles, infrastructure, legislation, and human behavior.
- Organization-specific vehicle and field travel policies and procedures.
- How to prevent and respond to specific threats such as accidents, ambush, indirect fire, carjacking and kidnapping.
- Overview of checkpoints relevant in the participant's operating environment including: type(s), what to expect, roles and good practice.
- Overview of movements tracking protocols.
- Introduction to defensive and evasive driving techniques.
- Post-accident procedures.

I.B.7 Residential and Office Security

How to stay safer and more secure in office compounds, residences, guesthouses and warehouses.

Key points include but are not limited to:

- Awareness of office compound and residence safety concerning matters such as fire, electrical, first aid kits, lighting, and perimeter security.
- Key measures the organization uses in residential and office security.
- Managing visitors' access to compounds and corresponding procedures.
- Procedures for situations such as evacuations and hibernations, and using emergency exits and safe rooms.

I.B.8 Personal and Team Resilience

How to better cultivate personal and immediate team resilience, dealing with trauma and traumatic events, including critical incident response.

Key aspects of this topic include but are not limited to:

- In-depth review of stress: types, how to recognize in oneself and in colleagues.
- Overview of support and management options: personal, peer support and organization-specific.
- Dealing with traumatic events, including incident response and debriefing.
- Overview of psychological first aid, techniques and considerations.

I.B.9 Field Communications

Overview of field communications, including survey of possible methods, security considerations and how to communicate effectively and use field communications equipment.

Key points include but are not limited to:

- Relevant communication devices and when to use them (in which situations and understanding when they are secure).
- Overview of regulations and protocols related to communications.
- How to set up, maintain and troubleshoot communications equipment and systems.
- Guidance on communication protocols, etiquette and other communications-related security issues.

I.B.10 Security Stakeholders

How to identify, understand and interact with actors who can influence security and programming.

Key points include but are not limited to:

- Identifying stakeholders and appropriate parties to engage in dialogue and negotiation to increase security and access to key interlocutors.
- How program design and activities influence social, political and economic power structures.
- How the organization's programming and presence affect different stakeholders and how they may react.
- How to explain security messages in a way that makes it easier to ensure people understand and support them.

I.B.11 Safety Threats

In-depth review of safety and how to assess safety risks in specific working environments.

Key points include but are not limited to:

- The difference between security and safety.
- Overview of different types of safety threats, such as natural disasters, accidents, hazards, and health-related threats.
- Overview of common safety threats and how to increase participants' awareness, reduce exposure and improve response.

I.B.12 Evacuation, Hibernation, Relocation

Overview of what participants need to know about evacuation, hibernation, relocation and suspension.

Key points include but are not limited to:

- Defining each term.
- Overview of which situations could activate these contingencies.
- Pros and cons.
- Logistical and ethical considerations for hibernation, evacuation, relocation and suspension.

I.B.13 Grab Bags

Understanding grab bags and how to use them in different operating environments and security risks.

Key points include but are not limited to:

- Definition of a grab bag.
- Typical contents of a grab bag.
- When to have grab bags.

Level IC - Personal Security in Violent Environments

Level IC provides personal security training for individuals operating in severe security risk environments. It is also for staff on long-term deployment in high security risk environments and all staff (international, national and local) on permanent assignment to high security risk environments. It teaches participants the contextualized security awareness and skills (prevention and response) they need for specific security threats in severe security risk environments.

The curriculum is divided into topics. After covering some general issues, this section reviews each topic. It first summarizes the scope of the topic and then lists key content the organization can include in the training it designs. The list is not exhaustive and the organization may choose to add other topics as well. Additional information on other aspects of course design can be found in the introduction to Section B above. This includes learning methodologies, creating a supportive environment, other learning opportunities, and monitoring and evaluation.

Target Audience

All agency personnel who are working in or travelling to locations considered severe security risk situations, such as active conflict zones, and all staff on long-term deployment in high security risk environments and all staff (international, national and local) on permanent assignment to high security risk environments.

Complimentary Trainings

Training in the following matters may be useful to supplement the materials covered in this curriculum:

- Advanced or first responder first aid and CPR
- Safety training: fire, building evacuations

Learning Methodology

In addition to taking into account the general guidance on learning methodology provided above in the introduction to Section B, training techniques at this level must also address other needs. Most importantly, training at this level must involve participants in simulations to help them better understand how they might react in a crisis and what they need to do in such cases. Including some simulation exercises can enhance effectiveness of training at this level.

Organizations and trainers also need to bear in mind that such exercises can result in significant emotional stress for participants. As a result, organizations and trainers must take particular care to ensure that simulations are conducted in a way that does not unduly stress participants. The training should also include ways to support participants who need to process the stress they experience during the simulations.

***Topics*.** Participants taking personal security in violent environments training must have covered all material in IA and IB prior to or must do so as part of the course at this level. This level consists entirely of elective topics, from which the organization can select to create training tailored to the particular needs of the participants. Organizations may choose to add other topics as well.

Elective Topics

I.C.1 Terrorism
I.C.2 Improvised Explosive Devices and Bombs
I.C.3 Landmines and Explosive Remnants of War (Unexploded Ordnance)
I.C.4 Indirect and Direct Fire, Shelling and Weapons
I.C.5 Crowds, Mobs and Demonstrations
I.C.6 Kidnapping, Abduction and Hostage Taking
I.C.7 Advanced Hostile Observation Awareness
I.C.8 Hostile Checkpoints
I.C.9 Helicopter Landing Procedures
I.C.10 Convoy Travel
I.C.11 Protective Equipment
I.C.12 Acceptance

Topic Details

I.C.1 Terrorism

Understanding forms of terrorism, and how to avoid and respond to them.

Key points to include but are not limited to:

- Overview of context-specific profile of terrorism: trends, tactics and patterns.
- How to avoid likely targets.
- How to recognize potential signs.
- Response procedures in the event of an incident or exposure.

I.C.2 Improvised Explosive Devices and Bombs

Understanding improvised explosive devices (IEDs), and how to avoid and respond to them.

Key points to include but are not limited to:

- Overview of situation-specific prevalence and patterns of IEDs: trends and tactics.
- How to avoid likely targets.
- How to recognize potential signs.
- Response procedures in the event of an incident or exposure in various situations (e.g., inside a building, outside a building, and during vehicle movements).

I.C.3 Landmines and Explosive Remnants of War (Unexploded Ordnance)

Understanding landmines and unexploded ordnance, and how to avoid and respond to them.

Key points to include but are not limited to:

- Overview of different landmines, unexploded ordnance (UXO); how to recognize them and areas where they may be present.
- How to avoid being exposed to landmines and UXO.
- Overview of contingencies in situations of exposure or incidents.

I.C.4 Indirect and Direct Fire, Shelling and Weapons

Understanding indirect and direct fire, shelling and other weapons; practicing avoidance and evasive action.

Key points to include but are not limited to:

- Overview of different weapons and their effective ranges.
- How to avoid higher-risk areas and situations.
- Good practice if caught in crossfire, direct fire or other shelling.

I.C.5 Crowds, Mobs and Demonstrations

Awareness in situations involving volatile crowds, mobs and demonstrations, and related prevention and response measures.

Key points to include but are not limited to:

- Understanding the differences between each situation and how they can become or are dangerous.
- How to avoid potential situations.
- How to respond if caught up in a situation or targeted.

I.C.6 Kidnapping, Abduction and Hostage Taking

Understanding kidnapping, abduction or hostage taking risk, including prevention, response and survival.

Key points to include but are not limited to:

- Overview patterns, trends and tactics for captivity and other specific risk situations.
- Overview of potential captors and motives.
- The phases of an abduction or kidnapping.
- Strategies for surviving capture, transport holding, rescue and release.

I.C.7 Advanced Hostile Observation Awareness

Increasing situation-specific awareness of hostile observation and understanding methods to decrease vulnerability and to safely signal its existence to the right channels.

Key points to include but are not limited to:

- Overview of situation-specific forms of hostile surveillance and how to recognize them.
- How to decrease vulnerability to being observed for hostile reasons.
- How to safely signal the existence of hostile observation to the right channels.

I.C.8 Hostile Checkpoints

Understanding hostile checkpoints, roles, behavior and other protocols.

Key points to include but are not limited to:

- Overview of different types of checkpoints.
- How to recognize different checkpoints.
- How to behave when approaching and entering checkpoints.
- How to negotiate checkpoints, roles and specific conduct.
- Other procedures in case checkpoints become volatile.
- Overview of other evasive techniques.

I.C.9 Helicopter Landing Procedures

Technical understanding of helicopter loading and unloading procedures and other safety considerations.

Key points to include but are not limited to:

- Overview of helicopter safety in approaching, loading and unloading.
- Awareness of ideal helicopter landing areas.
- Learn ground to air signalling.

I.C.10 Convoy Travel

Understanding convoy travel procedures and management.

Key points to include but are not limited to:

- Overview of situations in which convoy travel is appropriate.
- Advantages and disadvantages of convoy travel.
- How convoys are managed: protocols and procedures.

I.C.11 Protective Equipment

Understanding different security and protective equipment.

Key points to include but are not limited to:

- Overview of different and relevant security and protective equipment and when they are needed.
- Advantages and disadvantages of each piece of equipment.
- How to use and maintain equipment.

I.C.12 Acceptance

Increase understanding of and provide guidance on implementing acceptance as a security strategy in a violent environment. Active acceptance is increasingly relevant in operational situations.

Key points include but are not limited to*:*

- Acceptance within the specific context.
- Overview of strategies to practice and implement acceptance

Level II Operational Security

NGO Security Training Curriculum

LEVEL II: OPERATIONAL SECURITY

Introduction

This level outlines the security training needed by field staff with operational responsibilities for implementing security policies, protocols and procedures in their areas of operation. For example, it may be appropriate for full-time security professionals and other staff with security responsibilities.

Because this involves several distinct groups of staff, the Level II curriculum is divided into three sections targeting staff with the following roles:

Level IIA – Field staff with daily security and security-related responsibilities and/or oversight responsibilities for security-related activities. Examples include:

- Safety and security officers
- Safety and security focal points
- Logisticians
- Operations managers
- Site management
- Technical staff such as head guards, fleet managers and head drivers

Level IIB – Drivers
Level IIC – Guards

Training requirements for drivers and guards are particularly important for several reasons. First, because they are often the most vulnerable staff to safety and security risks. Second, because they also play a key role as the local face of the organization, interacting on a daily basis with various actors in the community. Finally, because they have practical responsibility for the safety and security of organization staff.

	II. FIELD SECURITY MANAGERS	II.B DRIVERS	II.C GUARDS
GOAL	Provide necessary training to field staff responsible for establishing, implementing, running and/or managing the organization's field security systems.	Teach agency drivers and other staff who drive vehicles in the course of their work safe and evasive driving techniques and other good practice in vehicle and travel safety and security; provide related training for all staff responsible for the movements of personnel and assets.	Teach guards how to effectively perform their security management responsibilities.
KEY OBJECTIVES	1. Teach participants how the organization's security framework works and the participant's security responsibilities within that framework. 2. Teach participants the skills necessary to meet the office's day-to-day security needs. 3. Teach participants how to communicate effectively with staff, security coordination platforms, authorities, the local community and beneficiaries. 4. Teach participants to execute crisis management responsibilities. 5. Teach participants the skills necessary to monitor and communicate changes in the operating environment and revise field office protocols as necessary.	1. Explain the organization's vehicle and travel security policies and procedures. 2. Review the roles and responsibilities of a driver. 3. Provide technical skills on safe travel, vehicles, routines, planning and rules. 4. Teach other necessary interpersonal communications skills.	1. Explain the organization's office and premises security policies and procedures. 2. Review the roles and responsibilities of a guard. 3. Teach participants concrete technical skills regarding procedures for dealing with specific situations. 4. Teach participants other necessary interpersonal communications skills.
CORE TOPICS	IIA.1 Humanitarian Principles and International Humanitarian Law IIA.2 Roles and Responsibilities IIA.3 Security Risk Management Framework IIA.4 Programming, Policy, Operations and Security IIA.5 Situational Analysis - Using Security Tools IIA.6 Risk Assessments IIA.7 Risk Reduction Strategies IIA.8 Standard Operating Procedures and Contingency Planning IIA.9 Supporting Incident and Crisis Management IIA.10 Incident Reporting and Analysis IIA.11 Stress Management IIA.12 Security Stakeholders IIA.13 Consultative Processes	II.B.1 Mission, Policies, Procedures, Programs and Culture II.B.2 Roles and Responsibilities II.B.3 Vehicle and Fleet Safety and Security Standards II.B.4 Risk Assessments II.B.5 Vehicle Inspections, Maintenance and Basic Repairs II.B.6 Preparation and Route Planning II.B.7 Vehicle Handling, Defensive Driving and Evasive Driving II.B.8 Driving at Night, in Poor Visibility and Poor Weather II.B.9 Local Laws and Other Road Signs and Signals II.B.10 Passenger Safety II.B.11 Cargo Safety II.B.12 Accident Procedures and Reporting II.B.13 First Aid Kits	IIC.1 Mission, Policies, Procedures, Programs and Culture IIC.2 Roles and Responsibilities IIC.3 Local Laws IIC.4 Patrolling IIC.5 Risk Assessments IIC.6 Health and Safety IIC.7 Fire Safety IIC.8 Emergency Response Procedures IIC.9 Evacuation Drills IIC.10 Hostile Observation Awareness IIC.11 Dealing with Aggression IIC.12 Cultural, Gendered and Personal Considerations IIC.13 Field Communications IIC.14 Visitor Access IIC.15 First Aid Kits

	IIA.14 Cultural, Gendered and Personal Considerations IIA.15 Leadership and Management IIA.16 Managing Guards and Drivers IIA.17 Travel Safety and Security IIA.18 Travel and Movement Tracking IIA.19 Site Security IIA.20 Information Management and Security IIA.21 Security Briefings and Orientation IIA.22 Health and Safety IIA.23 Practical Issues in Implementing Security IIA.24 Monitoring Security on a Daily Basis IIA.25 Practical Issues in Updating Security Information and Planning IIA.26 Practical Issues in Building Acceptance IIA.27 Dealing with Aggression	II.B.14 Practical Issues in Building Acceptance II.B.15 Field Communications II.B.16 Dealing with Aggression II.B.17 Cultural, Gendered and Personal Considerations II.B.18 Vehicle Travel Security II.B.19 Health and Safety	IIC.16 Practical Issues in Building Acceptance
ELECTIVE TOPICS	IIA.28 Working with Armed Protection and Private Security Companies IIA.29 Civil-Military Relations at the Operational Level IIA.30 Hostile Observation Awareness IIA.31 Communicating and Working with Senior Management IIA.32 Saving Lives Together	II.B.20 Hostile Observation Awareness II.B.21 Convoys II.B.22 Checkpoints II.B.23 Driving with Armed Protection and Escorts	

Level IIA – Field Security Managers

Level IIA covers training needed for field staff responsible for establishing, running and/or overseeing over the organization's field security systems.

The training is divided into topics. After covering some general issues, this section reviews each topic. It first summarizes the scope of the topic and then lists key content the organization can include in the training it designs. The list is not exhaustive and the organization may choose to add other topics as well. Additional information on other aspects of course design can be found in the introduction to Section B above. This includes learning methodologies, creating a supportive environment, other learning opportunities, and monitoring and evaluation.

Target Audience.
Field staff with daily security and security-related responsibilities and/or oversight for security-related activities. Examples include:

- Safety and security officers
- Safety and security focal points
- Logisticians
- Operations managers
- Site management
- Technical staff such as head guards, fleet managers and head driver

Complimentary Trainings
Training in the following matters may be useful to supplement the materials covered in this curriculum:

- How to train trainers
- Negotiation skills
- Leadership development
- Fire and electrical safety
- Building evacuation
- Advanced first aid and CPR
- Advanced personal safety and security (Level IB)

Topics

Core Topics

II.A.1 Humanitarian Principles and International Humanitarian Law
II.A.2 Roles and Responsibilities
II.A.3 Security Risk Management Framework
II.A.4 Programming, Policy, Operations and Security
II.A.5 Situational Analysis - Using Security Tools
II.A.6 Risk Assessments
II.A.7 Risk Reduction Strategies
II.A.8 Standard Operating Procedures and Contingency Planning
II.A.9 Supporting Incident and Crisis Management
II.A.10 Incident Reporting and Analysis

II.A.11 Stress Management
II.A.12 Security Stakeholders
II.A.13 Consultative Processes
II.A.14 Cultural, Gendered and Personal Considerations
II.A.15 Leadership and Management
II.A.16 Managing Guards and Drivers
II.A.17 Travel Safety and Security
II.A.18 Travel and Movement Tracking
II.A.19 Site Security
II.A.20 Information Management and Security
II.A.21 Security Briefings and Orientation
II.A.22 Health and Safety
II.A.23 Practical Issues in Implementing Security
II.A.24 Monitoring Security on a Daily Basis
II.A.25 Practical Issues in Updating Security Information and Planning
II.A.26 Practical Issues in Building Acceptance
II.A.27 Dealing with Aggression

Elective Topics

II.A.28 Working with Armed Protection and Private Security Companies
II.A.29 Civil-Military Relations at the Operational Level
II.A.30 Hostile Observation Awareness
II.A.31 Communicating and Working with Senior Management
II.A.32 Saving Lives Together

Topic Details

IIA.1 Humanitarian Principles and International Humanitarian Law

Overview of humanitarian and human rights principles and legal frameworks and how they relate to safety and security.

Key points include but are not limited to:

- Overview of humanitarian principles and how they relate to security and access.
- Overview of international humanitarian law (IHL), human rights law, and situations in which they apply.
- Protections provided for specific groups under IHL.
- Overview of how humanitarian and development NGO workers are covered under IHL.
- Options available to NGOs in deciding what role they should play in responding to humanitarian needs and human rights abuses, and the accompanying security considerations.

IIA.2 Roles and Responsibilities

Overview of the organization's security structure and the roles and responsibilities within it.

Key points include but are not limited to:

- Overview of the organization's security management architecture (global picture).
- The specific role of the participant and his/her day-to-day responsibilities.
- Overview of the organization's relevant decision-making authority at the regional, country and field levels.
- Reporting lines for safety and security.
- Considerations in centralized or decentralized decision making.

IIA.3 Security Risk Management Framework

How to implement an effective security management framework. Over the years, various security management frameworks have been developed to help NGOs systematically address security. These frameworks provide guidance on how to systematically appraise and analyze an organization's security capacity, identify risks and best reduce them through mitigation measures, planning and procedures.

Key points include but are not limited to:

- Review of existing security management frameworks.
- How to implement the organization's framework in the participant's the operating environment and the organization's culture.
- Key components of the organization's security management structure.
- Cross-cutting issues related to the framework.
- Importance of using the framework systematically.
- How and when to revise the framework.

IIA.4 Programming, Policy, Operations and Security

How to assess the organization's mission and overall vulnerability where the participant works, based on its local presence, programming and operational habits.

Key points include but are not limited to:

- In-depth review of the organization's local programming profile and potential security implications.
- How to work with program staff in assessing security risk and risk reduction measures.
- How to conduct on-site assessments.
- How to conduct on-site security support.
- Other operational activities and security requirements.
- How to budget for security, including needs such as training, security assets, site enhancements and security staff.

IIA.5 Situational Analysis - Using Security Tools

How to assess the participant's working environment (country and location-specific), including a review of available situational analysis tools and how to use them.

Key topics include but are not limited to:

- Overview of information gathering tools (e.g., media, published, key informants, information coordination platforms, participatory discussions and consultation).
- The political, economic, socio-cultural, geographical and technological context in which the office operates.
- How to analyze the working environment using tools such as actor mapping, conflict analysis, violence mapping, conflict mapping, and political and economic analysis.
- Assessing the operating environment as well as the organization's presence and programming to better understand general and targeted risks the team faces.
- Understanding the interdependence of security and the organization's presence and programming.
- Understanding how perceptions can vary and how those differences can affect the participant's work environment.
- How to use scenarios to identify and prepare for changes in the security situation.
- How to identify key stakeholders in the community who can have an effect on security.

IIA.6 Risk Assessments

How to assess situation-specific security risks.

Key points include but are not limited to:

- Defining key terms such as risk, threat, vulnerability, likelihood and impact.
- The importance of risk assessments to systematically identify risk and make informed decisions about reducing exposure and minimizing impact.
- Approaches to conducting a risk assessment (interviews, pattern analysis, using indicators, and gauging threat level).
- Identifying and prioritizing context-specific threats.
- Identifying and prioritizing factors that affect staff and/or asset vulnerability.
- The link between threat and vulnerability.
- Assessing risk in immediate operations environments and determining if that risk meets the organization's acceptable risk parameters.
- Approaches and methodologies for continuously re-evaluating and updating risk assessments.

IIA.7 Risk Reduction Strategies

Overview of the organization's security strategy and how to apply it.

Key points include but are not limited to:

- The current organizational culture and strategies used to reduce security and safety risks.
- The pros and cons of each strategy and how they apply to context-specific threats.
- Ensuring choice of strategy is based on a risk assessment that takes into account the organization's culture and capacity.
- How to use the organization's strategy to reduce specific risks, keeping in mind the organization's culture and vulnerabilities.
- Resource investments (e.g., cost, time, personnel) and other implications (e.g., image, reputation and relationships) of each strategy.
- In-depth analysis of the organization's image and level of acceptance.

IIA.8 Standard Operating Procedures and Contingency Planning

How to translate security risk reduction strategies into standard operating procedures and contingency plans for the field.

Key points include but are not limited to:

- Overview of typical security plan components such as roles and responsibilities, standard operating procedures, contingency planning, evacuation relocation, hibernation planning, and crisis management plans.
- Using a consultative approach to ensure relevant standard operating procedures and security plans; practical guidance in and examples of translating risk assessments into written procedures and contingencies.
- Overview of the organization's security planning templates.
- How to use analytical frameworks to revise existing security measures to ensure relevance and effectiveness.
- Practical ways to effectively monitor situations and keep planning continuously updated.

IIA.9 Supporting Incident and Crisis Management

Overview of the participant's crisis management's responsibilities.

Key points include but are not limited to:

- Reviewing and practicing contingency responses to specific threats.
- Overview of how to analyze incident data and adjust risk assessments accordingly.
- When the participant can manage an incident, and when he/she should instead play a supporting role.
- Technical, logistical and financial needs in dealing with incidents.
- Principles and guidance on dealing with sexual assault and rape.
- How to deal with incidents such as:
    - low levels of harassment and intimidation; and
    - petty theft and other internal security incidents.
- Overview of the organization's crisis management processes and the role(s) the participant would fill.
- Overview of and guidance on planning, assessing and preparing assembly points, safe rooms, hibernation locations; other evacuation and relocation considerations.

- How to assess medical services in accordance with staff insurance standards and coverage.
- How to support or conduct a medical evacuation.
- How to identify and assess available local psycho-social support mechanisms.
- How to pre-position post-incident supplies (e.g., rape kits, post-exposure prophylaxis (PEP) kits and first aid kits) and establish related protocols.

IIA.10 Incident Reporting and Analysis

Overview of the organization's incident reporting systems and the role of the participant in reporting and analysis. Emphasis on the principles and good practice for incident reporting, stressing the need to analyze at both the country and field levels.

Key points include but are not limited to:

- Overview of current systematic and complimentary mechanisms for incident reporting.
- Defining what constitutes an incident and what is a near-miss.
- Different types of incident reports (immediate and post-incident).
- How to encourage incident reporting.
- How to keep track of small incidents and near-misses that may not be reported.
- Analyzing incident reporting and the significance of data.
- Linking incidents through incident pattern analysis and statistics.

IIA.11 Stress Management

How to understand and identify signs and symptoms of stress in one's self and colleagues, and how to build coping and resilience mechanisms.

Key points include but are not limited to:

- Overview of assumptions and evidence about stress and its adverse impacts on individuals, teams and performance.
- How to best manage personal stress.
- The role of effective leadership and team cohesion.
- How to recognize individual staff members suffering from trauma or acute stress.
- How to prepare for and respond to traumatic and critical stress; principles of psychological first aid.

IIA.12 Security Stakeholders

How to identify and understand actors who can influence security and programming, including how to analyze their motives, attitudes and relationships.

Key points include but are not limited to:

- Identifying stakeholders and appropriate parties to engage in dialogue and negotiation to increase staff security and access to key interlocutors.
- How program design and activities influence social, political and economic power structures.
- How the organization's programming and presence affect different stakeholders and how they may react.
- How to explain security messages in a way that makes it easier to ensure people understand and support them.
- How to conduct effective outreach, including by identifying and cultivating relationships.

IIA.13 Consultative Processes

Overview of consultative and participatory approaches that can effectively elicit staff thoughts on and strengthen their support for the organization's security policies and measures.

Key points include but are not limited to:

- Overview of participatory and consultative approaches and their importance for security management.
- Identifying and approaching key staff groups and other interlocutors.
- Managing meetings and focus group discussions.

IIA.14 Cultural, Gendered and Personal Considerations

Strengthened participant sensitivity to personal and societal factors that effect security realities for other staffers, and how to address those realities in security efforts. These factors include gender, sexual orientation, religion, cultural and personal considerations such as disabilities.

Key points include but are not limited to:

- How to assess different notions and understandings of security and safety, and what this means in relation to cultural, gendered and personal specific security considerations.
- Special security considerations for various groups of staff.
- Defining gender and gender equality, and how these concepts play into effective security.

IIA.15 Leadership and Management

How to be an effective security manager and leader for the organization's personnel in a way that increases support and compliance.

Key points include but are not limited to:

- Overview of what good management and effective leadership entail.
- Importance of teamwork and teambuilding and their relationship to security.
- Sources of insecurity as a result of poor management and leadership.
- Tools to use good management and leadership to improve the organization's security culture.

IIA.16 Managing Guards and Drivers

How to increase security through effective management of guards and drivers.

Key points include but are not limited to:

- Roles and responsibilities.
- Guards and drivers as representatives on the frontline of interaction between the organization and the community.
- Guards and drivers as key enforcers and implementers of security procedures and standards.
- Recruitment considerations.
- Management issues.
- Rules and related contractual considerations.
- The question of armed guards.
- Creating effective training for guards and drivers.
- Building awareness of acceptance – interpersonal communications.

IIA.17 Travel Safety and Security

Good practice in the daily management and oversight of travel protocols and activities.

Key points include but are not limited to:

- Understanding road, water and air safety and security risks.
- Selecting effective measures to reduce risk.
- Vehicles and infrastructure.
- Overview of relevant legislation.
- Consideration of the human factor: how people's behavior and local customs affect these issues.
- Major risk factors.
- Teaching staff about the organization's road safety rules (as a driver or passenger) and ensuring compliance.
- Post accident management and procedures.
- Accident data: collecting, analyzing and taking action based on findings.
- Promoting a travel safety culture in the participant's team and organization.

IIA.18 Travel and Movement Tracking

How to effectively and consistently track travel and movements.

Key aspects of this topic include but are not limited to:

- Overview of movement tracking systems, tools and protocols.
- Implementing movement tracking procedures.
- Managing day-to-day movement and travel tracking.
- Setting up procedures for what to do if a staffer does not arrive by the pre-agreed time.
- How to report noncompliance.

IIA.19 Site Security

Overview of site security management activities that optimize the safety and security of the organization's staff, residences, guest accommodations, offices, warehouses and other buildings.

Key points include but are not limited to:

- Factors to consider in selecting a site and maintaining safety and security standards for it.
- Whether to maintain a high or low profile.
- How different choices can affect how the organization is perceived.
- Overview of checklists, issues and security mechanisms that must be implemented and maintained at each site, such as visitor access, lighting, exits, electrical safety, fire safety, first aid kits and perimeter guards.
- Identifying potential threats to site security and developing measures to reduce vulnerability.

IIA.20 Information Management and Security

Overview information management and how to secure it; developing awareness of external surveillance.

Key points include but are not limited to:

- Assessing concerns and needs for information security within the organization at a field level, including concerns about social media.
- Overview of the organization's current and potential policies and measures concerning information management.

- How these policies and measures relate to the participant's work.
- Awareness of context-specific IT security considerations and organizational IT security systems (e.g. intranets, social media and security).
- Good practices for working with sensitive organizational, security, programming or operational information.
- Understanding external surveillance and when it can become hostile; and developing awareness of external surveillance.
- How to identify and make other key actors aware of breaches in information security.

IIA.21 Security Briefings and Orientation

How to develop and deliver effective security orientations and briefings.

Key points include but are not limited to:

- Developing objectives for security briefing sessions.
- Developing and prioritizing the content of security briefings.
- The who, when and how of delivering effective security briefings.
- Creating effective security materials to include in visitor welcome packets.

IIA.22 Health and Safety

Overview of the organization's health and safety policies and practices.

Key topics include but are not limited to:

- Overview of the organization's health and safety policies.
- How to comply with relevant safety practices and protocols.
- How to report and/or attend to any health and safety hazards (e.g. electrical hazards) in workplace.
- Overview of first aid kits and how to use and maintain them.

IIA.23 Practical Issues in Implementing Security

Concrete ways for participants to improve implementation of the organization's security principles and operating procedures.

Key points include but are not limited to:

- Barriers that hinder implementation.
- Ways to overcome barriers.
- How to transfer knowledge to staff.
- Tools and approaches for better implementation.
- Best options for specific situations, staff and locations (including processes, structures, roles and responsibilities, meetings, trainings, advisories and monitoring).

IIA.24 Monitoring Security on a Daily Basis

How to monitor security on a daily basis.

Key points include but are not limited to:

- How to determine what must be monitored daily to meet operational needs (e.g., roads, crime and political developments).
- Effective ways to structure a daily monitoring system.
- How to effectively interact with staff on daily monitoring matters including travel movements.

- Overview of available location-specific tools for daily oversight of security.
- The role of discipline in daily monitoring and how to make it a reality.

IIA.25 Practical Issues in Updating Security Information and Planning

How to keep staff informed about overall security planning, information and changes that occur.

Key points include but are not limited to:
- Security phase levels.
- Using indicators to modify security phase levels and measures.
- Ways to communicate security updates to other staff members.

IIA.26 Practical Issues in Building Acceptance

How to systematically cultivate and nurture acceptance in the field. Active acceptance is increasingly relevant in operational situations. This topic is important because many organizations subscribe to acceptance in principle without fully understanding the significant resources and effort involved in effective implementation.

Key points include but are not limited to:
- Review of the organization's concept and strategy.
- Challenges to realizing that strategy in the participant's operating environment.
- Image and perception (i.e., factors affecting acceptance and how to assess level of acceptance).
- Key and cross-cutting components of acceptance (e.g., stakeholders, programming, staffing decisions, behavior and composition).
- How to select and implement activities to effectively implement an acceptance approach.
- Identifying organizational and environmental challenges to implementation.
- How to monitor acceptance.

IIA.27 Dealing with Aggression

How to use interpersonal communications skills to defuse aggression in various situations.

Key points include but are not limited to:
- Principles of communication.
- Overview of different types of aggression and how to recognize their symptoms.
- Understanding the cultural dimension of aggression.
- Techniques for de-escalating aggression.

Elective Topics

IIA.28 Working with Armed Protection and Private Security Companies

Overview of issues related to working with armed protection.

Key points include but are not limited to:
- Principles to consider in deciding whether to use armed protection.
- Overview of different types of armed protection services.
- Overview of the organization's policies on using armed protection.
- How to determine if a potential service provider is well managed.

IIA.29 Civil-Military Relations at the Operational Level

Guidance on civil-military relations at the field level and related security considerations.

Key points include but are not limited to:

- Review of the organization's policy on interacting with militaries.
- Overview of local civil-military issues on the ground, relations (cooperation versus coordination), and the impact on field level security.
- Understanding the relevant military culture.
- UN frameworks and key guidance documents concerning civil-military relations.
- How to assess and minimize the impact on the organization, staff and security while working with the military and afterwards.

IIA.30 Hostile Observation Awareness

How to detect hostile observation activities, identify the risks of hostile observation, and develop preventive and responsive procedures.

Key points include but are not limited to:

- The difference between surveillance and hostile observation.
- How to recognize potential signs of hostile observation activities.
- How to prevent hostile observation and other unwanted surveillance (general and context-specific).
- How to safely signal the presence of hostile observation activities to the right channels.
- Reporting.

IIA.31 Communicating and Working with Senior Management

How to effectively communicate and work with senior management in the country team.

Key points include but are not limited to:

- Understanding and navigating management processes.
- Gaining buy-in from senior management.
- Participating in senior management meetings.
- Communicating effectively with senior management.

IIA.32 Saving Lives Together

Overview of how Saving Lives Together (SLT) works at the field level.

Key points include but are not limited to:

- Key principles of SLT.
- How SLT works in the field – pro and cons.
- Field specific-SLT information.

Level IIB – Drivers

Level IIB is for all field-based staff who drive a vehicle for the organization. This includes both individuals whose official job title is "driver" and others who drive vehicles in the course of their work. This level is also for all staff who are responsible for the movements of personnel and assets. The course teaches safe and evasive driving techniques and other good practices in vehicle and travel safety and security.

The training is divided into topics. After covering some general issues, this section reviews each topic. It first summarizes the scope of the topic and then lists key content the organization can include in the training it designs. The list is not exhaustive and the organization may choose to add other topics as well. Additional information on other aspects of course design can be found in the introduction to Section B above. This includes learning methodologies, creating a supportive environment, other learning opportunities, and monitoring and evaluation.

Target Audience

Level IIB is for all field-based staff who drive or operate a vehicle for the organization and/or are responsible for the movements of personnel and assets. This includes both individuals whose official job title is "driver" and others who drive vehicles in the course of their work. This level is also for all staff who are responsible for the movements of personnel and assets.

Complimentary Trainings

Drivers are exposed to higher safety and security threats. They are also responsible for the safety of staff and other passengers in the vehicles they operate. Therefore, participants in this level of training may also benefit from the following complimentary trainings:

- Basic or advanced first aid and CPR
- Advanced personal safety and security training (Level IB)

Topics

Core Topics

II.B.1 Mission, Policies, Procedures, Programs and Culture
II.B.2 Roles and Responsibilities
II.B.3 Vehicle and Fleet Safety and Security Standards
II.B.4 Risk Assessments
II.B.5 Vehicle Inspections, Maintenance and Basic Repairs
II.B.6 Preparation and Route Planning
II.B.7 Vehicle Handling, Defensive Driving and Evasive Driving
II.B.8 Driving at Night, in Poor Visibility and Poor Weather
II.B.9 Local Laws and Other Road Signs and Signals
II.B.10 Passenger Safety
II.B.11 Cargo Safety
II.B.12 Accident Procedures and Reporting
II.B.13 First Aid Kits
II.B.14 Practical Issues in Building Acceptance
II.B.15 Field Communications
II.B.16 Dealing with Aggression
II.B.17 Cultural, Gendered and Personal Considerations

II.B.18 Vehicle Travel Security
II.B.19 Health and Safety

Elective Topics

II.B.20 Hostile Observation Awareness
II.B.21 Convoys
II.B.22 Checkpoints
II.B.23 Driving with Armed Protection and Escorts

Topic Details

Core Topics

II.B.1 Mission, Policies, Procedures, Programs and Culture

Understanding the organization's mission and security-related policies and procedures.

Key points include but are not limited to:

- Overview of the organization's mission and programming.
- Overview of the organization's global security-related policies and procedures.

II.B.2 Roles and Responsibilities

Overview of the organization's security structure and drivers' specific roles and responsibilities within it.

Key points include but are not limited to:

- Overview of the organization's security management architecture (global and country levels).
- The specific role of the participant and his/her day-to-day responsibilities.

II.B.3 Vehicle and Fleet Safety and Security Standards

Good practice in the daily management and oversight of travel protocols and activities.

Key points include but are not limited to:

- Understanding road, water and air safety and security policies and standards.
- Selecting effective measures to reduce risk.
- Vehicles and infrastructure.
- Overview of relevant legislation.
- Consideration of the human factor: how people's behavior and local customs affect these issues.
- Review of applicable fleet management practices and standards such as travel authorizations, movement tracking and log books.

II.B.4 Risk Assessments

How to assess driving and travel safety and security risks, including a review of available tools for reducing risk and how to use them.

Key topics include but are not limited to:

- Defining key terms such as risk, threat, vulnerability, likelihood and impact.
- The importance of risk assessment to systematically identify risk and make informed decisions about reducing exposure and minimizing impact.

- Identifying and prioritizing threats.
- Identifying and prioritizing factors that affect staff and/or asset vulnerability during movements.
- How to use scenarios to identify and prepare for specific security incidents.
- How to identify key stakeholders in the community who can have an effect on security.

II.B.5 Vehicle Inspections, Maintenance and Basic Repairs

Good practice and discipline in conducting vehicle inspections, maintenance and basic repairs.

Key points include but are not limited to:

- Conducting vehicle inspections.
- Overview of maintenance requirements.
- How to conduct basic repairs in the field.

II.B.6 Preparation and Route Planning

How to effectively and consistently track travel and movements.

Key points include but are not limited to:

- Overview of movement tracking systems, tools and protocols.
- Implementing movement tracking procedures.
- Managing day-to-day movement and travel tracking.
- Setting up procedures for what to do if a staffer does not arrive by the pre-agreed time.
- How to report noncompliance.

II.B.7 Vehicle Handling, Defensive Driving and Evasive Driving

Providing vehicle handling awareness and practice in defensive and evasive driving techniques for safety and security.

Key points include but are not limited to:

- How to handle various types of vehicle such as 4X4 and armored.
- Vehicle handling including positioning and cornering.
- Defensive driving techniques and practice, such as dealing with traffic, overtaking and driving in reverse.
- Evasive driving techniques and practice.

II.B.8 Driving at Night, in Poor Visibility and Poor Weather

How to drive at night and in situations involving poor visibility and weather.

Key points include but are not limited to:

- Understanding risks of poor driving conditions in the participant's working environment.
- Strategies to avoid and manage driving in poor conditions.
- How to select other effective measures to reduce risk.

II.B.9 Local Laws and Other Road Signs and Signals

Review of relevant local laws, road signage, signals and local driving habits.

Key points include but are not limited to:

- Overview of local driving laws.

- Overview of local road signs and other signals.
- Overview of local and cultural driving habits and practices.

II.B.10 Passenger Safety

Good practice in the daily management and oversight of passenger safety.

Key points include but are not limited to:

- Overview of road, water, air safety and security risks to passengers.
- How to select effective measures to reduce risk to passengers.
- Vehicles and infrastructure.
- Overview of relevant legislation.
- Consideration of the human factor: how people's behavior and local customs affect these issues.
- How to effectively teach staff about the organization's road safety rules.
- How to strengthen driver and passenger compliance.

II.B.11 Cargo Safety

Good practice in the daily management and oversight of cargo safety.

Key points include but are not limited to:

- Understanding cargo security risks.
- How to select effective measures to reduce risk.
- Logistical considerations such as securing loads, cargo classifications and authorizations.
- Overview of the organization's restrictions and procedures for cargo.

II.B.12 Accident Procedures and Reporting

Overview of accident procedures and reporting for incidents and near-misses.

Key points include but are not limited to:

- Defining what constitutes an accident, incident and a near-miss.
- Overview of accident procedures for various situations.
- Immediate incident reporting protocols.
- Overview of post-incident reporting – timeliness, confidentiality, access, formats and content.
- Overview of insurance claim procedures after accidents.

II.B.13 First Aid Kits

Overview of first aid kits and how to use and maintain them.

Key points include but are not limited to:

- Typical contents of first aid kits.
- Assessing medical and first aid needs of passengers.
- Assessing and preparing kit contents according to needs based on particular travel, passengers and local conditions.
- How to maintain first aid kit (inventory, supplies and expiry dates).

II.B.14 Practical Issues in Building Acceptance

How to systematically cultivate and nurture acceptance in the field. Active acceptance is increasingly relevant in operational situations.

Key points include but are not limited to:

- Image and acceptance as an approach.
- Image and perception: factors affecting acceptance, how to assess level of acceptance, and how different groups may perceive the individual and the organization.
- The impact of individual behavior on acceptance.
- Specific tools to help assess and build acceptance on the individual and team levels and within programming.

II.B.15 Field Communications

Overview of relevant communications methods and security considerations, and how to communicate effectively and use field communications equipment.

Key points include but are not limited to:

- Relevant communication devices and when to use them (in which situations and understanding when they are secure).
- Overview of regulations and protocols related to communications.
- How to set up, maintain and troubleshoot communications equipment and systems.
- Guidance on communication protocols, etiquette and other communications-related security issues.

II.B.16 Dealing with Aggression

How to use interpersonal communications skills to defuse aggression in various situations.

Key points include but are not limited to:

- Principles of communication.
- Overview of different types of aggression and how to recognize their symptoms.
- Understanding the cultural dimension of aggression.
- Techniques for de-escalating aggression.

II.B.17 Cultural, Gendered and Personal Considerations

Strengthened participant sensitivity to personal and societal factors that effect security realities for other staffers and how to address those realities in security efforts. These factors include gender, sexual orientation, religion, cultural and personal considerations such as disabilities.

Key aspects of this topic include but are not limited to:

- How to assess different notions and understandings of security and safety, and what this means in relation to cultural, gendered and personal security considerations.
- Special security considerations for various groups of staff.
- Defining gender and gender equality, and how these concepts play into effective security.

II.B.18 Vehicle Travel Security

How to prevent and respond to vehicle travel security threats (e.g., ambush, car-jacking and indirect fire) in specific situations.

Key points include but are not limited to:

- Overview of situation security threats – prevention and response in relation to exposure and office procedures and contingencies.

II.B.19 Health and Safety

Overview of the organization's health and safety policies and practices.

Key topics include but are not limited to:

- Overview of the organization's health and safety policy.
- How to comply with relevant safety practices and protocols.
- How to report and/or attend to any health and safety hazards in workplace (e.g. electrical hazards).

Elective Topics

II.B.20 Hostile Observation Awareness

How to detect hostile observation activities, identify the risks of hostile observation, and develop preventive and responsive procedures.

Key points include but are not limited to:

- The difference between surveillance and hostile observation.
- How to recognize potential signs of hostile observation activities.
- How to prevent hostile observation and other unwanted surveillance (general and context-specific).
- How to safely signal the presence of hostile observation activities to the right channels.
- Reporting.

II.B.21 Convoys

How to organize and travel in convoys.

Key points include but are not limited to:

- Understanding the pros and cons of convoy travel.
- Assessing which situations are appropriate for convoy travel.
- Overview of good practice and discipline in convoy travel.
- Overview of the organization's relevant procedures and policies.

II.B.22 Checkpoints

Understanding and negotiating checkpoints.

Key points include but are not limited to:

- Overview of different types of checkpoints: general and situation-specific, hostile, formal and informal.
- Driver and passenger roles and responsibilities concerning checkpoints.

- How to appraise checkpoints.
- How to negotiate checkpoints.
- Good practice for exiting checkpoints and signalling abnormalities.

II.B.23 Driving with Armed Protection and Escorts

Overview of issues related to working with armed protection and escorts during movements and travel.

Key points include but are not limited to:

- Overview of different types of armed protection services and escorts.
- Overview of the organization's policies and procedures on using armed protection and escorts.
- Good practice when driving with armed escorts or protection.
- How to determine if a potential service provider is well managed.

Level IIC – Guards

Level IIC teaches guards how to effectively perform their security management responsibilities.

The training is divided into topics. After covering some general issues, this section reviews each topic. It first summarizes the scope of the topic and then lists key content the organization can include in the training it designs. The list is not exhaustive and the organization may choose to add other topics as well. Additional information on other aspects of course design can be found in the introduction to Section B above. This includes learning methodologies, creating a supportive environment, other learning opportunities, and monitoring and evaluation.

Target Audience
All guards working for the organization.

Complimentary Trainings
Guards are exposed to higher safety and security threats. They are also responsible for the safety of staff and visitors in the organization's compounds and facilities. Therefore, participants of this level of training may also benefit from the following trainings:

- Basic or advanced first aid and CPR
- Advanced personal safety and security training (Level IB)

Topics

Core Topics

IIC.1 Mission, Policies, Procedures, Programs and Culture
IIC.2 Roles and Responsibilities
IIC.3 Local Laws
IIC.4 Patrolling
IIC.5 Risk Assessments
IIC.6 Health and Safety
IIC.7 Fire Safety
IIC.8 Emergency Response Procedures
IIC.9 Evacuation Drills
IIC.10 Dealing with Aggression
IIC.11 Cultural, Gendered and Personal Considerations
IIC.12 Field Communications
IIC.13 Visitor Access
IIC.14 First Aid Kits
IIC.15 Practical Issues in Building Acceptance

Elective Topics

IIC.16 Hostile Observation Awareness

Topic Details

Core Topics

IIC.1 Mission, Policies, Procedures, Programs and Culture

Understanding the organization's mission and security-related policies and procedures.

Key points include but are not limited to:

- Overview of the organization's mission.
- Overview of the organization's global and local programming.
- Overview of the organization's security policies and correlated country-specific rules and protocols.

IIC.2 Roles and Responsibilities

Overview of the organization's security structure and guards' specific roles and responsibilities within it.

Key points include but are not limited to:

- Overview of the organization's global and country specific security management architecture.
- The specific role of the participant and his/her day-to-day responsibilities.

IIC.3 Local Laws

Overview of local laws and their implications for security and guarding.

Key points include but are not limited to:

- Overview of local laws and their implications for security and guarding.
- Overview of local and cultural practices and their implications for security and guarding.

IIC.4 Patrolling

Good practice and discipline in conducting compound inspections and patrolling offices, warehouses and accommodations.

Key points include but are not limited to:

- Good practice in patrolling and working with other guards.
- Conducting premises inspections.
- Reporting incidents and near-misses.

IIC.5 Risk Assessments

How to assess compound safety and security risks, including a review of available tools for reducing risk and how to use them.

Key topics include but are not limited to:

- Defining key terms such as risk, threat, vulnerability, likelihood and impact.
- The importance of risk assessment to systematically identifying risk and making informed decisions about reducing exposure and minimizing impact.

- Identifying and prioritizing threats.
- Identifying and prioritizing factors that affect staff and/or asset vulnerability during movements.
- How to use scenarios to identify and prepare for specific security incidents and changes.
- How to identify key stakeholders in the community who can have an effect on security.

IIC.6 Health and Safety

Overview of the organization's health and safety policies and practices.

Key topics include but are not limited to:

- Overview of the organization's health and safety policies.
- How to comply with relevant safety practices and protocols.
- How to report and/or attend to any health and safety hazards in workplace (e.g. electrical hazards).

IIC.7 Fire Safety

Overview of fire safety awareness, protocols and practice.

Key topics include but are not limited to:

- Overview of different types of fire.
- Overview of fire protocols.
- How to inspect, maintain and use fire extinguishers and other equipment, including alarms.
- Overview of guards' roles during fire drills.

IIC.8 Emergency Response Procedures

Overview of emergency response procedures.

Key topics include but are not limited to:

- Overview of various types of emergency situations such as natural disaster, security and fire.
- How to use safe rooms and assembly points, and implement relevant emergency procedures.
- Understanding and using hibernation stocks.

IIC.9 Evacuation Drills

How to conduct and facilitate building and compound evacuation drills.

Key topics include but are not limited to:

- How to recognize an evacuation alarm.
- When to signal alarms and conduct evacuation rehearsal drills.
- Building and compound emergency exits, procedures for exiting and assisting staff during evacuations.
- Managing assembly points and head count procedures.

IIC.10 Dealing with Aggression

How to use interpersonal communications skills to defuse aggression in various situations.

Key points include but are not limited to:

- Principles of communication.
- Overview of different types of aggression and how to recognize their symptoms.

- Understanding the cultural dimension of aggression.
- Techniques for de-escalating aggression.

IIC.11 Cultural, Gendered and Personal Considerations

Strengthened participant sensitivity to personal and societal factors that effect security realities for other staffers and how to address those realities in security efforts. These factors include gender, sexual orientation, religion, cultural and personal considerations such as disabilities.

Key aspects of this topic include but are not limited to:

- How to assess different notions and understanding of security and safety and what this means in relation to cultural, gender and personal security considerations.
- Special security considerations for various groups of the organization's staff.
- Defining gender and gender equality, and how these concepts play into effective security.

IIC.12 Field Communications

Overview of relevant communications methods and security considerations, and how to communicate effectively and use field communications equipment.

Key points include but are not limited to:

- Relevant communication devices and when to use them (in which situations and understanding when they are secure).
- Overview of regulations and protocols related to communications.
- How to set up, maintain and troubleshoot communications equipment and systems.
- Guidance on communication protocols, etiquette and other communications-related security issues.

IIC.13 Visitor Access

Overview of relevant visitor access protocols and how to implement them.

Key topics include but are not limited to:

- Relevant policies and protocols for visitor access.
- How to implement relevant visitor access protocols (e.g., verifying appointments, logging identification, signalling arrival, bag or person inspections).
- Gender and culture-specific considerations.

IIC.14 First Aid Kits

Overview of first aid kits and how to use and maintain them.

Key points include but are not limited to:

- Typical contents of first aid kits.
- Assessing and preparing kit contents according to needs based on staff and operating environment.
- How to maintain first aid kits (inventory, supplies and expiry dates).

IIC.15 Practical Issues in Building Acceptance

How to systematically cultivate and nurture acceptance during interactions at the office with visitors and neighbors. Active acceptance is increasingly relevant in operational situations.

Key points include but are not limited to:

- Acceptance as an approach.
- Image and perception (i.e., factors affecting acceptance and how to assess level of acceptance) and how different groups may perceive the individual and the organization.
- The impact of individual behavior on acceptance.
- Specific tools to help assess and build acceptance on the individual and team levels and within programming.

Elective Topics

IIC.16 Hostile Observation Awareness

How to detect hostile observation activities, identify the risks of hostile observation, and develop preventive and responsive procedures.

Key points include but are not limited to:

- The difference between surveillance and hostile observation.
- How to recognize potential signs of hostile observation activities.
- How to prevent hostile observation and other unwanted surveillance (general and context-specific).
- How to safely signal the presence of hostile observation activities to the right channels.
- Reporting.

Level III Security Management

NGO Security Training Curriculum

LEVEL III - SECURITY MANAGEMENT

Level III targets staff responsible for managing, developing, reviewing and advising on security issues. Examples include global security officers, regional management, country management, regional security, and other relevant senior management. The training teaches them the soft and hard skills they need to ensure programs are implemented within an acceptable level of security risk.

The training is divided into topics. After covering some general issues, this section provides a curriculum summary chart and then reviews each topic. It first summarizes the scope of the topic and then lists key content the organization can include in the training it designs. The list is not exhaustive and the organization may choose to add other topics as well. Additional information on other aspects of course design can be found in the introduction to Section B above. This includes learning methodologies, creating a supportive environment, other learning opportunities, and monitoring and evaluation.

Target Audience

Level III is targeted to staff responsible for developing, managing, reviewing and advising on security issues. Examples include global security officers, regional security directors, country directors, regional security advisors, and other senior management as required. The targeted staff have some level of decision-making authority and accountability in relation to the legal duty of care and the organization's global mission within their geographic and programmatic area. They report to and coordinate with their organization's global headquarters or lead members.

Complimentary Trainings

Training in the following matters may be useful to supplement the materials covered in this curriculum:

- Personal security training
- Field operational security management training for security focal points (Level IIA).

Topics

The following chart covers the goal, objectives and topics in Level III. The topics reflect issues relevant to this particular level of training. The amount of time it takes to cover different topics may vary significantly. For those familiar with the term "module" as used by the training community, keep in mind that "topic" as used in this document is not the same thing.

After the chart, the section turns to each topic in more detail. For each topic it first summarizes the scope and then provides a list of key content that the organization can include in the training it designs. The list is not exhaustive and the organization may choose to add other topics as well.

Level III (Field Strategic): Goal, Objectives and Topics

GOAL	Provide staff responsible for developing, managing, reviewing and advising on security issues with the soft and hard skills they need to ensure programs are implemented within an acceptable level of security risk.
KEY OBJECTIVES	Provide an overview of the components of security risk management. Explain the relationship between security and duty of care and the participant's relevant responsibilities. Teach participants how to use information to improve the organization's security culture. Teach participants how to manage security risk management processes and training, and supervise others with security support responsibilities. Equip senior managers to effectively handle incidents.
CORE TOPICS	III.1 Security Risk Management Frameworks III.2 Context Assessment and Situational Analysis III.3 Risk Assessments and Understanding Risk Thresholds III.4 Risk Reduction Strategies III.5 Acceptance III.6 Security Planning – Development and Review III.7 Implementation and Compliance III.8 Stress Management in Traumatic or Critical Incidents III.9 Leadership and Management at the Country and Regional Levels III.10 HR and Security III.11 Cultural, Gendered and Personal Considerations in Security III.12 Budgeting and Resources for Security III.13 Information Management and Security III.14 Security Stakeholders III.15 Field Security Assessments, Advisory and Monitoring Activities III.16 Site Selection and Security III.17 The Organization's Security Management Architecture, Policies and Standards III.18 Accountability Frameworks III.19 Duty of Care and Legal Liability III.20 Security and Training III.21 Programming and Security III.22 Incident Reporting, Monitoring and Analysis III.23 Managing the Full Spectrum of Incidents and Post-Incident Recovery III.24 Security Self-Assessments and Audits III.25 Managing Guards and Drivers III.26 Crisis Management III.27 Evacuation, Hibernation, Relocation and Suspension III.28 International Legal Frameworks III.29 Dealing with Aggression
ELECTIVE TOPICS	III.30 Security Networks III.31 Engaging Private Security Providers III.32 Negotiating Access III.33 Gender-Based Violence (GBV) – Prevention and Case Management III.34 Media Training III.35 Working with Armed Protection and Private Security Companies

III.36 Working with Implementing Partners: Security Considerations
III.37 Security Implications of Remote Management of Programs
III.38 Kidnapping, Abduction and Hostage Taking
III.39 Cash Security
III.40 Managing Situation-Specific Threats and Incidents
III.41 Integrating Safety and Security in Emergency Response
III.42 Hostile Observation Awareness
III.43 Health and Wellness
III.44 Operational Continuity
III.45 Civil-Military Relations
III.46 Saving Lives Together

Core Topics

III.1 Security Risk Management Frameworks

Overview of security risk management frameworks and how to identify and implement the best framework for an organization.

Key points include but are not limited to:

- Overview of key components of a security management framework.
- How to identify the best framework for a particular organization.
- Overview of cross-cutting issues related to the framework.
- How to systematically use the framework.
- Implementation and revision of the framework periodically or on an as-needed basis.
- Relevance of the framework to the organization's culture and philosophy.

III.2 Context Assessment and Situational Analysis

Overview of a basic framework and tools to effectively analyze an operating environment.

Key points include but are not limited to:

- Overview of information gathering tools such as media, key informants, information coordination platforms, participatory discussions and consultation.
- Tools for analyzing an operating environment (e.g., actor mapping, conflict analysis and mapping, violence mapping, and political and economic analysis).
- The impact of an organization's presence and programming in specific situations.
- Using analysis of the operating situation to better understand general and targeted risk.
- Using scenarios to prepare for changing security situations.

III.3 Risk Assessments and Understanding Risk Thresholds

How to assess security risk, safety threats and organizational vulnerability and set thresholds of acceptable risk.

Key points include but are not limited to:

- Defining key terms such as risk, threat, vulnerability, likelihood and impact.
- The importance of risk assessment to systematically identifying risk and making informed decisions about reducing exposure and minimizing impact.

- Approaches for conducting a risk assessment (interviews, pattern analysis, using indicators and gauging threat level).
- Identifying and prioritizing context-specific threats.
- Identifying and prioritizing factors that affect staff and/or asset vulnerability.
- The link between threat and vulnerability.
- How to assess risk and threat in operating environments and determine if that risk is within the organization's acceptable risk parameters.
- Approaches for continuously re-evaluating and updating risk assessments.

III.4 Risk Reduction Strategies

Review of security strategies.

Key points include but are not limited to:

- Overview of strategies currently used to reduce security and safety risks.
- Detailed analysis of the pros and cons of each strategy and how they apply to context-specific threats.
- How to use risk assessment to select the best strategy.
- Use of different strategies to reduce specific risks contextualized for the organization.
- Overview of related resource requirements (cost, time, personnel) and other implications (e.g., image, reputation and relationships) for each strategy.

III.5 Acceptance

How to conceptualize acceptance within the participants' working environment. This topic is important because many organizations subscribe to acceptance in principle without fully understanding the significant resources and effort involved in effective implementation.

Key points include but are not limited to:

- Key and cross-cutting components of acceptance (stakeholders, programming, staffing decisions – behavior and composition).
- Conceptualizing acceptance: proactive engagement, activities and actions to gain and maintain consent from stakeholders.
- Degrees of acceptance and the dynamic nature of consent.
- Picking effective indicators and how to monitor acceptance levels.
- How to effectively implement an acceptance approach.
- Identifying organizational and environmental challenges to making acceptance work.
- Factors affecting image; how to assess levels of acceptance.

III.6 Security Planning – Development and Review

How to apply an organization's principles, processes and tools to develop and implement security plans.

Key points include but are not limited to:

- Overview of typical components of a security plan (e.g., roles and responsibilities, standard operating procedures, contingency planning, evacuation relocation, hibernation planning, sensitive administrative procedures and crisis management plans).
- Integrating security planning into management processes and tools.
- Overview of processes that can produce security planning that is more accurate and accepted by staff (e.g., participatory planning processes).

- How to evaluate a security plan's relevancy and effectiveness.
- How to monitor the operating environment and continuously revise and update planning.
- Beyond the written plan: other considerations in effective security planning.
- Security risk phase levels: what they are and how to use them.

III.7 Implementation and Compliance

How to implement the organization's security policies, implement security measures and ensure staff compliance. Implementation of security measures is often a significant gap in security management. Important issues also exist concerning compliance and staff acceptance.

Key points include but are not limited to:

- Overview of barriers and other issues that hinder implementation.
- Ways to overcome barriers and other issues.
- Tools and approaches for better implementation
- Tools for specific situations, staff and locations (e.g. processes, structures, roles and responsibilities, meetings, trainings, advisories and monitoring).
- Context and/or organization-specific compliance challenges.
- Communicating plans: how to improve staff awareness of security planning.
- Other tools such as simulations and training of trainers.

III.8 Stress Management in Traumatic or Critical Incidents

Using an evidence-based approach able to prepare for and respond to traumatic and critical incidents.

Key points include but are not limited to:

- Overview of assumptions and evidence about stress and its adverse impacts on individuals, teams, the organization and performance.
- Policies and practices to foster a culture of resilience (e.g. identifying and prepositioning various support outlets – informed by need and culture).
- The role of effective leadership and team cohesion.
- How to recognize when a staff member is suffering from trauma or acute stress.
- How to prepare for and respond to traumatic stress, including principles of psychological first aid and developing protocols.
- Managing the aftermath.

III.9 Leadership and Management at the Country and Regional Levels

Understanding the centrality of good management and leadership of staff to strengthening acceptance of and compliance with security policies and measures.

Key points include but are not limited to:

- The components of good management and effective leadership.
- The importance of teamwork and teambuilding for security.
- Ways poor management and leadership can cause insecurity.
- How to use good management and leadership to help strengthen an organization's security culture.
- Creating and implementing clear compliance and disciplinary procedures.

III.10 HR and Security

Review of the important links between certain HR issues and security.

Key points include but are not limited to:

- Donor government anti-terrorism legislation: impact and considerations.
- Security considerations in staff hiring, contracts and overall management (interviews, background checks, behavior and compliance).
- Safe working environment.
- Orientations, codes of conduct and communicating other HR policies.
- Managing people – cultural and gendered approaches.
- Health and wellness.
- Insurance and benefits.
- Talent development (training).
- Dealing with corruption.
- Terminations: labor laws and good practices to avoid potential security incidents.
- Post-incident support mechanisms.
- How to strengthen communication and coordination between the organization's HR and security personnel.
- Gendered, cultural and other personal considerations of staff members.
- Including security management responsibilities in job performance assessment.
- Issues of high staff turnover and security.

III.11 Cultural, Gendered and Personal Considerations in Security

Strengthened participant sensitivity to personal and societal factors that effect security realities for other staffers, and how to address those realities in security efforts. These factors include gender, religion, sexual orientation, cultural and personal considerations such as disabilities.

Key points include but are not limited to:

- Cultivating a culture of security that integrates considerations of gender, religion, sexual orientation, cultural and other personal considerations such as disabilities.
- Principles for effective implementation of such approaches.
- Policies and procedures concerning specific contextual and operational considerations.
- Cultural, religious, nationality, sexual-orientation, gender-specific and personal considerations concerning the security aspects of programming and operational situations.

III.12 Budgeting and Resources for Security

How to accurately determine risk management expenditures, and how to justify these costs when presenting project proposals and budgets to headquarters and donors.

Key points include but are not limited to:

- The importance of introducing safety and security risk management costs in the early stages and of making them an integral part of program design, sustainability and success.
- Assessing operational security resource needs and expenses (human resources, time and financial).
- Donor-specific security requirements.
- Determining risk management costs and how to build them into project proposals and budgets.
- The cost of not investing in security risk management.

III.13 Information Management and Security

Overview information management and how to secure it.

Key points include but are not limited to:

- The link between information management and security.
- Assessing concerns and needs for information security within the organization at the regional and field levels, including concerns about social media.
- Overview of the organization's current and potential information management policies and measures.
- How these policies and measures relate to the participant's work.
- Awareness of context-specific IT security considerations and organizational IT security systems (e.g. intranets, social media and security).
- Good practices for working with sensitive organizational, security, programming or operational information.
- How to identify and manage breaches in information security.

III.14 Security Stakeholders

How to identify and understand actors who can influence security and programming, including analyzing their motives, attitudes and relationships.

Key points include but are not limited to:

- Identifying stakeholders and appropriate parties to engage in dialogue and negotiation to increase staff security and access to key interlocutors.
- How program design and activities influence social, political and economic power structures.
- How the organization's programming and presence affect different stakeholders and how they may react.
- How to explain security messages in a way that makes it easier to ensure people understand and support them.
- How to conduct effective outreach, including by identifying and cultivating relationships.

III.15 Field Security Assessments, Advisory and Monitoring Activities

How to conduct field security assessment, advisory and monitoring activities.

Key points include but are not limited to:

- How to conduct field security assessments that take into account the country and regional security context.
- Monitoring security-related communications from the field concerning incidents and planning, and how to provide feedback to questions raised.
- Monitoring security preparedness and field training.
- Report writing, including making and prioritizing recommendations.
- Developing and maintaining a security incident database.
- How to generate monthly security activity reports, including data, analysis, overview of threats and vulnerabilities, and other relevant information.
- Maintaining security networks with internal and external focal points and other stakeholders.

III.16 Site Selection and Security

Using site selection criteria that optimize safety and security while achieving operational objectives with minimal loss or harm to personnel and assets.

Key points include but are not limited to:

- Factors to consider in selecting a site for an office, accommodations, warehouse or other facility for the organization.
- Factors for evaluating and implementing site security measures, including the use of information from risk assessments.
- How different choices may affect how the organization is perceived.
- Identifying potential threats to site security.
- Selecting and implementing measures to reduce site vulnerability.
- Executing context-specific site management in medium- to high-risk areas.

III.17 The Organization's Security Management Architecture, Policies and Standards

Overview of the organization's security structure and the roles and responsibilities within it.

Key points include but are not limited to:

- Overview of the organization's security management architecture.
- Roles and responsibilities at the headquarters, regional and field levels.
- Overview of the organization's relevant decision-making authority at the regional, country and field levels.
- Reporting lines for safety and security.
- Considerations in centralized and decentralized security decision making.
- Other operational issues and solutions in centralized and decentralized security.
- In-depth review of security policies and standards.

III.18 Accountability Frameworks

Overview of the organization's accountability frameworks and requirements.

Key points include but are not limited to:

- Overview of the organization's feedback loops.
- Implementing and revising related policies and procedures.
- Overview of the organization's policies and procedures on waivers.

III.19 Duty of Care and Legal Liability

Understanding the concepts of duty of care and legal liability in the context of the organization's work, and how to incorporate those concepts into operations.

Key points include but are not limited to:

- Defining legal liability and duty of care, and how these concepts apply to the country office.
- The impact of NGO community standards on the duty of care.
- Overview of the key liability concerns for NGOs (organizational and context-specific).
- How to assess context-specific cultural attitudes and tendencies concerning legal liability.
- Review of conditions that commonly result in legal liability.

III.20 Security and Training

How to design effective security training. Managers have a responsibility to ensure staff receive security training both when they join the organization and when they take up a new assignment or switch work locations.

Key points include but are not limited to:

- Assessing staff training needs.
- Developing objectives for security briefings and training.
- How to determine the core content of the sessions.
- Accessing training options and potential providers.
- Review of required resources for training.
- Monitoring the effectiveness of training.
- Developing and implementing effective debriefings.

III.21 Programming and Security

How to assess the organization's mission and overall vulnerability in a particular location.

Key points include but are not limited to:

- Factors that may affect the organization's vulnerability.
- Analysis of the organization's specific capacities and vulnerabilities in a specific situation.
- Budgeting issues.
- Ways to reduce vulnerability.

III.22 Incident Reporting, Monitoring and Analysis

The importance of and good practice for incident reporting, and the critical need to analyze and monitor at a regional or country level. A comprehensive and systematic incident reporting mechanism can deeply enhance an organization's security management, due diligence toward staff, donor requirements and strengthen interagency collaboration. It can be an important management tool for personnel, programs and operations.

Key points include but are not limited to:

- How to develop effective systems for incident reporting.
- Review of types of information incident reporting should capture such as trends, management issues, and groups and individuals most at risk.
- How to encourage reporting of incidents.
- Incident analysis and decision making.
- Drafting reports.
- Linking incidents through incident pattern analysis and statistics.
- Using post-incident analysis to strengthen institutional memory and inform effective operational changes.

III.23 Managing the Full Spectrum of Incidents and Post-Incident Recovery

Crises are not the only type of incidents. This topic focuses on two other important and often overlooked issues: how to deal with other specific incidents and post-incident recovery mechanisms.

Key points include but are not limited to:

- How to deal with incidents, including the importance of context.

- Support needs in dealing with incidents.
- Existing principles and guidance on dealing with sexual assault and rape.
- How to deal with low levels of harassment and intimidation.
- How to deal with petty theft and other noncritical internal security incidents.
- Assessment of medical outlets.
- Medical evacuations: assessing options and establishing procedures.
- How to identify and assess psycho-social support mechanisms.
- Post-incident recovery supplies: how to preposition them and establish effective protocols.

III.24 Security Self-Assessments and Audits

How to assess and audit all dimensions of the organization's security management practices for a specific office or location.

Key points include but are not limited to:

- Creating a framework for the organization to use in conducting security audits of country and field offices.
- How to prioritize findings and make recommendations.
- How to develop action plans to address security needs.

III.25 Managing Guards and Drivers

How to increase security through effective management of guards and drivers.

Key points include but are not limited to:

- Roles and responsibilities of guards and drivers.
- Guards and drivers as representatives on the frontline of interaction between the organization and the community.
- Guards and drivers as key enforcers and implementers of security procedures and standards.
- Recruitment considerations.
- Management issues.
- Rules and related contractual considerations.
- The question of armed guards.
- Gender, cultural and disability considerations.
- Creating effective training for guards and drivers.
- Building awareness concerning acceptance – interpersonal communications.

III.26 Crisis Management

How, in coordination with headquarters, to coordinate a crisis response that will mitigate physical and reputational damage to staff and or assets.

Key points include but are not limited to:

- Composition of a field-level incident management team (IMT).
- Roles and responsibilities of the IMT and of the headquarters crisis management team (CMT).
- The initial response to an incident.
- Developing protocols for crisis management.
- Negotiation strategies.
- How to communicate with and support families.
- Crisis communications, including internal, external and media.

- Coordinating and liaising with other key stakeholders such as governments, other agencies, private security providers and insurance companies.

III.27 Evacuation, Hibernation, Relocation and Suspension

Overview of decision making, security considerations, planning and protocols concerning evacuation, hibernation, relocation and suspension.

Key points include but are not limited to:

- Definitions of each type of contingency (evacuation, hibernation, relocation and suspension).
- Review of preparation requirements for each type.
- Policy and management considerations for:
  - Hibernation: decision and preparation (stocks, how to communication with affected staff, and determining which staff hibernate, facilities and locations).
  - Suspension of activities: decision, communication, statements, staff management, and impact on presence and acceptance.
  - Relocation: decision, movement options, priority list of eligible staff, continuity plan, interagency coordination, facility and assets management, suspension procedures, return and resumption criteria.
  - Evacuation: eligible staff, continuity plan, decision-making process, indicators for evacuation, procedures, routes, communication, administrative procedures, equipment and supplies, re-entry and resumption criteria, interagency coordination.

III.28 International Legal Frameworks

Overview of humanitarian and human rights principles and legal frameworks, and how they can be used to improve the security and protection of civilians and aid workers.

Key points include but are not limited to:

- Overview of international humanitarian law (IHL), human rights law, and situations in which they apply.
- Overview of when humanitarian and development organizations are legally entitled to deliver assistance and how this affects security.
- Protections provided for specific groups under IHL.
- Overview of how humanitarian and development NGO workers are covered under IHL.
- The protection mandates of the International Committee of the Red Cross and the UN refugee agency (UNHCR).
- Options available to NGOs in deciding what role to play in responding to humanitarian needs and human rights abuses, and the accompanying security considerations.

III.29 Dealing with Aggression

How to use interpersonal communications skills to defuse aggression in various situations.

Key points include but are not limited to:

- Principles of communication.
- Overview of different types of aggression and how to recognize their symptoms.
- Understanding the cultural dimension of aggression.
- Techniques for de-escalating aggression.

Elective Topics

III.30 Security Networks

Overview of existing security information and coordination initiatives, their benefits and limitations, and how to make use of them. Security information and coordination initiatives have greatly enhanced interagency sharing, collaboration and professional development. They have also fostered the development and mainstreaming of sector-wide good practices for security.

Key points include but are not limited to:

- Overview of interagency security initiatives such as those through the European Interagency Security Forum and InterAction.
- Overview of Saving Lives Together.
- Other security coordination systems (country-specific security information coordination offices).

III.31 Engaging Private Security Providers

Understanding important considerations in deciding whether or when to use private security providers (PSPs).

Key points include but are not limited to:

- Overview of the international regulations and certifications of PSPs, including the Montreux Document and the Code of Conduct for Private Security Providers (ICoC).
- Overview of the history of and trends in NGO engagement with PSPs and why use has increased.
- Overview of hard and soft services PSPs offer.
- How to evaluate circumstances in which engaging PSPs is possible, and factors to consider including effectiveness, appropriateness and compatibility with an organization's profile, risks and opportunities.
- Overview of the decision-making processes related to engaging PSPs (e.g., contracting, selection, and monitoring and evaluation).
- Review of other tools and checklists to assist with selection, contracting and evaluation.

III.32 Negotiating Access

Understanding negotiating access as a process of communication and relationship building undertaken to ensure provision of protection and assistance to vulnerable groups, preserve humanitarian space, and promote respect for international law.

Key points include but are not limited to:

- The purpose of humanitarian negotiations.
- Review and analysis of organization-specific reasons for negotiating.
- Negotiations and staff security policies and procedures.
- How to identify stakeholders, such as partners, armed groups, government and civil society leaders.
- The international and domestic laws that effect access negotiations.
- The three phases of negotiation.
- Modes of negotiation.
- Role of culture in negotiating.
- Implications and negative outcomes: awareness and preparing.
- Suggested key principles of humanitarian access to guide negotiations with stakeholders and armed groups.

III.33 Gender-Based Violence (GBV) – Prevention and Case Management

Understanding GBV as a widely under-reported type of security incident; how to manage GBV cases in the organization according to principles and how to attend to or provide referrals for survivor psychological, medical and, if possible, legal needs.

Key points include but are not limited to:

- Understanding sector-wide principles on GBV and GBV case management, and how it differs from sexual abuse and exploitation.
- Review of the organization's policies and procedures on GBV case management.
- Understanding the varying needs of survivors, and how to conduct a holistic assessment that takes into account varying needs.
- Core knowledge and skills required to work with survivors.
- How to explain the importance of consent to the survivor.
- How to develop procedures for emergency response and reporting GBV incidents; prepositioning of post-exposure prophylaxis (PEP) and rape kits.
- How to identify outlets and specialists to support GBV incident response.
- Understanding the difference between giving information and giving advice.
- The importance of empowerment and confidentiality in assisting GBV survivors.
- How to access legal services.

III.34 Media Training

How to deal with the media in emergency situations.

Key points include but are not limited to:

- Identifying who is authorized to speak to the media.
- Review of the organization's relevant policies and practices.
- Practical tips on what to do and not do when dealing with the media.
- The impact on of poor interactions or harmful media coverage on security.
- Media as a strategic tool in for specific purposes such as increasing public acceptance or attention for specific purposes including access, advocacy and hostage release.

III.35 Working with Armed Protection and Private Security Companies

Overview of decision-making issues regarding the policy and practice of using armed protection, including private security companies.

Key points include but are not limited to:

- Overview of types and sources of armed protection.
- Reasons for using armed protection.
- The implications of using armed protection, including negative impacts and ethical considerations.
- Criteria, decision making and procedures concerning the use of armed protection.
- If and when exceptions may be needed to the organization's general procedures for using armed protection.
- How to determine if a potential service provider is well managed.
- Using armed guards: policy issues, services, training and contractual issues.

III.36 Working with Implementing Partners: Security Considerations

Understanding security matters related to working with local implementing partners including possible moral and legal responsibilities, and approaches and tools to improve security management support for local partners. This is a growing area of importance as the increasing use of local implementing partners has highlighted questions and issues of security management and responsibility.

Key points include but are not limited to:

- Overview of different models of partnership between international NGOs and their local implementing partners including contractors.
- The moral, ethical or legal duty of care associated with each model.
- Overview of tools and options for supporting local implementing partners.

III.37 Security Implications of Remote Management of Programs

Understanding security implications associated with remote management of programs and the related transference of risk.

Key points include but are not limited to:

- Definition of remote management.
- Considerations before deciding to implement it and its impact on program effectiveness.
- Policy and procedural guidance.
- Implications of remote management including risk transfer, cost and effects on programming.
- How to improve remote management.

III.38 Kidnapping, Abduction and Hostage Taking

Overview of threats related to kidnapping, abduction and hostage taking.

Key points include but are not limited to:

- Definitions and management response implications.
- Overview of situation-specific threats, and how to conduct a pattern analysis of local incidents.
- Identifying and implementing risk reduction measures for a specific risk.
- Related organizational or local policies and management protocols.
- Communicating with captors.
- How to communicate with and support families.
- Managing the aftermath of an incident.
- Preparing and training staff on awareness, prevention and surviving a capture situation.

III.39 Cash Security

How to manage security issues arising from handling large quantities of cash.

Key points include but are not limited to:

- Specific threats related to cash.
- Cash management considerations, including storage and transportation.
- Protecting valuables in the organization’s offices, warehouses and accommodations.
- How to manage payment procedures.
- Security and petty cash.
- Dealing with corruption concerns and how to mitigate fraud.

III.40 Managing Situation-Specific Threats and Incidents

How to manage context-specific security threats such as arrest and detention.

Key points include but are not limited to:

- Handling context-specific considerations in managing specific threats.
- Assessing internal capacity to manage the incident locally, including resources, staff and expertise.
- How to identify stakeholders and networks that can provide support in managing incidents.
- When to request support from regional offices and/or headquarters.
- Documenting specific threats and incidents.

III.41 Integrating Safety and Security in Emergency Response

Understanding safety and security considerations during emergency response.

Key points include but are not limited to:

- Integrating security into emergency planning documents and protocols.
- Policy considerations.
- Procedural considerations for various scenarios.
- Security in programming: how to conduct an effective emergency assessment.

III.42 Hostile Observation Awareness

How to detect hostile observation activities, identify the risks of hostile observation, and develop preventive and responsive procedures.

Key points include but are not limited to:

- The difference between surveillance and hostile observation.
- How to recognize potential signs of hostile observation activities.
- How to prevent hostile observation and other unwanted surveillance (general and context-specific).
- How to safely signal the presence of hostile observation activities to the right channels.

III.43 Health and Wellness

Overview of key health and wellness considerations.

Key points include but are not limited to:

- Understanding the link between a staff member's health, wellness and security.
- Key health risks in regional and country office areas of operation.
- Identifying at-risk staff.
- Increasing staff awareness and good practice in keeping healthy and safe.
- Identifying appropriate clinics, insurance considerations and medical emergency procedures.
- Other health and wellness considerations such as policies and prepositioning medical resources.

III.44 Operational Continuity

How operations will continue the event of an evacuation, hibernation, relocation or country office closing; how to conduct operational continuity planning and preparedness.

Key points include but are not limited to:

- Overview of operational continuity concepts and principles.
- Handling situations where operational continuity is possible and those where it is impossible.
- Planning for operational continuity, including addressing necessary functions and requirements.

III.45 Civil-Military Relations

Developing and implementing civil-military relations policies.

Key points include but are not limited to:

- Overview of various civil-military relations (cooperation versus coordination) and the impact on security.
- How to assess and minimize the impact on the organization, staff and security while working with the military and afterwards.
- Organizational considerations in civil-military policy development and in reviewing the organization's policy on interacting with militaries.
- UN frameworks and key guidance documents concerning civil-military relations.

III.46 Saving Lives Together

Understanding of Saving Lives Together (SLT), how it can be used and how to manage expectations.

Key points include but are not limited to:

- Overview of key principles of SLT.
- How SLT works in the field – pro and cons.
- Policy and field-specific SLT considerations.
- Existing SLT platforms.

Level IV Global Strategic

NGO Security Training Curriculum

Level IV - Global-Strategic Security

Level IV is primarily targeted for international headquarters staff with decision-making authority and responsibilities related to the organization's legal duty of care and/or its global operations. It provides participants with the key concepts and skills necessary to establish and maintain an organization-wide security vision, leadership, strategy and framework. This training is essential to foster and maintain an organization-wide security culture that treats the well-being of its personnel as paramount. Without healthy, safe and secure personnel, humanitarian and development programming cannot be achieved.

The training is divided into topics. After covering some general issues, this section provides a curriculum summary chart and then reviews each topic. It first summarizes the scope of the topic and then lists key content the organization can include in the training it designs. The list is not exclusive and the organization may choose to add other topics as well. Additional information on other aspects of course design can be found in the introduction to Section B above. This includes learning methodologies, creating a supportive environment, other learning opportunities, and monitoring and evaluation.

Target Audience

International headquarters staff with decision-making authority and responsibilities related to the organization's legal duty of care and/or its global operations. This may include individuals in:

- Corporate governance (e.g., board members, CEOs and presidents)
- Technical senior management at the headquarters level (e.g. security directors, human resources, operations, administration, finance, communications)

Complimentary Trainings

Training in the following matters may be useful to supplement the materials covered in this curriculum:

- Field strategic security management training (Level III)
- Personal safety and security training
- Leadership and management development
- Strategic planning

Learning Methodology

Level IV is best done on an organization-specific basis because it must meet the particular needs and culture of the organization. This also facilitates the handling of sensitive issues, decisions and policies.

Global-strategic security training needs to be realistic, concise and targeted based on a number of factors. These factors include organizational structure, size, capacity and operational profile (e.g., working exclusively through partners or serving as the implementing agency). It also must take into account the availability of people who should participate. Given schedule constraints, training may need to occur over a longer period of time instead of within a dedicated training course.

Because of the complexity of the audience and potentially the organization's size and capacity as well, the following should be considered:

- Presenting materials concisely with a focus on key information and concepts.
- Keeping sessions short and the content tightly focused.

- Transmitting materials during seminars, meetings and conferences convened to address other issues (see Supportive Environment below).
- Capitalizing on learning opportunities when relevant discussions arise elsewhere, sometimes in semi-formal situations.
- Weighing the appropriateness of individual versus group training.
- Subcategories within the group targeted in this training level may need different materials.

For crisis management training, the use of realistic simulations may be particularly useful.

Supportive Environment

As mentioned above, the effectiveness of the curriculum at this level also depends on integrating security into other trainings, seminars and meetings. For example, security can be included in such fora concerning:

- Strategic planning
- Risk management
- Human resources
- Policy development
- Project and program management
- Programming
- Communications, including media relations
- Advocacy

Topics

The following chart covers the goal, objectives and topics in Level IV. The topics reflect issues relevant to this level training. The amount of time it takes to cover different topics may vary significantly. For those familiar with the term "module" as used by the training community, keep in mind that topic as used in this document is not the same thing.

After the chart, the section turns to each topic in more detail. For each topic, it first summarizes the scope and then provides a list of key content the organization can include in the training it designs. The list is not exhaustive and the organization may choose to add other topics as well.

Level IV: Goal, Objectives and Topics

GOAL	Provide participants with the key concepts and skills necessary to establish and maintain an organization-wide security vision, leadership, strategy and framework.
KEY OBJECTIVES	1. Explain the importance of strategic and effective security management. 2. Equip participants to be able to develop a strategic vision for creating and maintaining an effective security culture. 3. Equip participants to develop organization's security risk management frameworks and comprehensive security management capacity. 4. Equip participants to be able to provide strategic level leadership, understanding, prioritization and governance of the organization's security management framework and systems to enable realization of the organization's objectives. 5. Equip participants to be able to deal with critical incidents – prevention, response and post-recovery.

CORE TOPICS	IV.1	Security Risk Management
	IV.2	Strategic Planning
	IV.3	Security Management Architecture and Capacity
	IV.4	Duty of Care
	IV.5	Security Policy, Principles, Standards and Guidance
	IV.6	Crisis Management
	IV.7	Risk Management and Operational Continuity
	IV.8	Programming and Security
	IV.9	Budgeting and Resources for Security
	IV.10	Human Resources and Security
	IV.11	Cultural, Gendered and Personal Considerations in Security
	IV.12	Communications and Information Management
	IV.13	Implementation and Compliance
	IV.14	Security Strategies
	IV.15	Dealing with Aggression
ELECTIVE TOPICS	IV.16	Stress Management in Traumatic or Critical Incidents
	IV.17	Security Implications of Working with Implementing Partners
	IV.18	Incident Reporting, Monitoring and Analysis
	IV.19	Security Planning
	IV.20	Security Networks
	IV.21	Civil-Military Relations
	IV.22	Using Armed Guards and Escorts
	IV.23	Saving Lives Together
	IV.24	Security Implications of Remote Management

Core Topics

IV.1 Security Risk Management

Overview of the most relevant framework(s) for integrating security risk management throughout organization's the culture and operations.

Key points include but are not limited to:

- Security risk management framework(s): key components and concepts.
- Security and the organization's mission.
- Effective security management: HQ level discussions and decision making.
- The organization's risk tolerance level.
- Accountability: who is accountable for what and to whom.
- Donor relations and security requirements.
- How to mainstream security including in organizational culture, budgets and programming.
- Measuring success in the organization's safety and security management.

IV.2 Strategic Planning

How to develop and integrate the organization's strategic planning processes, its overall mission and security-related goals.

Key points include but are not limited to:

- Strategic governance commitment to purpose and success in security – setting the direction.
- Overview of relevant international humanitarian law (IHL) and human rights law and situations in which they apply, including how humanitarian and development NGO workers are covered under IHL.
- Options available to NGOs in deciding what role to play in responding to humanitarian needs and human rights abuses (in light of relevant IHL), and the accompanying security considerations.
- Integrating security in the organization's mission, vision (desired outcome and success), values, goals, strategies, tactics, and performance measurement plan and evaluation.
- Implementation of strategic planning by executives and senior managers.

IV.3 Security Management Architecture and Capacity

Review of security management options an organization can use to clarify its existing security management architecture, roles, responsibilities and reporting lines.

Key points include but are not limited to:

- Overview of the organization's existing security management system and capacity:
  - where is security housed at headquarters (and at the field and regional levels);
  - roles and responsibilities at the HQ, regional and field levels;
  - issues between HQ and field offices that can hinder good security practices;
  - defining the organization's lines of authority, responsibility and decision making as they pertain to security; and
  - reporting and communications lines.
- The importance and key components of effective leadership and management.
- Other security management options the organization can use to clarify and strengthen the existing architecture.
- Issues, solutions, and considerations in centralized and decentralized security management styles.

IV.4 *Duty of Care*

Understanding and addressing the increasing probability and potential impact of legal actions on the organization. This includes good practice for demonstrating due diligence in meeting duty of care standards to reduce litigious activities.

Key points include but are not limited to:

- Defining legal liability and duty of care in jurisdictions where the organization operates.
- Overview of the key liability concerns for NGOs.
- In-depth review of core values and the concept of duty of care and how it applies to security and the organization.
- Review of situations that commonly result in legal liability.
- Insurance.
- How to assess context-specific cultural attitudes and tendencies concerning legal liability.
  - Handling legal claims.

IV.5 ***Security Policy, Principles, Standards and Guidance***

How to develop, revise and implement an organization's security policy, standards or other related security principles.

Key points include but are not limited to:

- Content considerations for security policy, principles, standards and guidance.
- Integration of security into other policies, standards and guidance.
- Who should write or be consulted concerning the policy.
- How to implement security policy.
- How to revise and evaluate security policy.

IV.6 ***Crisis Management***

How to coordinate a response that will mitigate physical and reputational damage to staff and assets.

Key points include but are not limited to:

- Decision-making authority.
- Composition of a headquarters-level crisis management team (CMT).
- CMT roles and responsibilities.
- Crisis management plans and protocols.
- Types of potential crises.
- Types of potential impact on the organization such as security, reputational and financial.
- How the organization's structure affects crisis response (i.e., federation, decentralized or centralized structure).
- Coordinating responses with field-level incident management teams (IMTs).
- Initial critical response to an incident.
- Developing protocols for crisis management.
- Negotiation strategies.
- How to communicate with and support families.
- Insurance considerations and options.
- Crisis communications, including internal, external and media.
- Coordinating and liaising with other key stakeholders such as governments, other organizations, private security providers and insurance companies.

IV.7 ***Risk Management and Operational Continuity***

How to conduct comprehensive risk management and ensure operational continuity.

Key points include but are not limited to:

- Defining risk management and its interdependent components (financial, reputational, programmatic and security).
- Security within a comprehensive risk management strategy.
- Donor-driven risk management requirements and how to demonstrate due diligence in risk management.
- Operational continuity concepts and principles for higher-level preparedness through policy development and use of resources.
- Planning for operational continuity.
- Examining different scenarios where program continuity are possible or impossible

IV.8 ***Programming and Security***

Strengthening the link between security and programming, with particular attention to the impact of program design and decisions on security.

Key points include but are not limited to:

- How to plan for and address changing operating conditions.
- How to increase and secure access.
- Donor requirements.
- Financing security and safety.
- Analyzing the impact of programming on security.
- Viewing security as enabling programming.

IV.9 ***Budgeting and Resources for Security***

How to accurately determine risk management expenditures, and how to justify these costs when presenting project proposals and budgets to donors.

Key points include but are not limited to:

- The importance of introducing safety and security risk management costs in the early stages and making them an integral part of program design, sustainability and success.
- Assessing global security resource needs and expenses (human resources, time and financial).
- Understanding donor attitudes, priorities and security requirements.
- Oversight of how the cost of risk management is built into project proposals and budgets.
- Staff development: training, capacity for security.
- Cost analysis methods, including cost benefit, true cost, cost effectiveness and value for money.
- Determining risk management costs and how to build them into project proposals and budgets.
- The cost of not spending on risk management.

IV.10 ***Human Resources and Security***

Review of the important links between certain HR issues and security.

Key points include but are not limited to:

- The importance of staff training for developing security competencies and awareness.
- Donor government antiterrorism legislation: impact and considerations.
- Security considerations in staff hiring, contracts and overall management (interviews, background checks, competencies, behavior and compliance).
- Safe working environment, staff care and wellness.
- Orientations, codes of conduct and communicating other HR policies.
- How to include culture, gender and other personal considerations when managing people.
- Insurance and benefits.
- Post-incident support mechanisms.
- How to strengthen communication and coordination between HR, administrative, legal and security personnel.
- Issues of high staff turnover and security.
- Dealing with corruption.
- Including security management responsibilities in job performance.
- Terminations: labor laws and good practices to avoid potential security incidents.

IV.11 ***Cultural, Gendered and Personal Considerations in Security***

Strengthened participant sensitivity to personal and societal factors that effect security realities for other staffers and how to address those realities in security efforts. These factors include gender, religion, sexual orientation, cultural and personal considerations such as disabilities.

Key points include but are not limited to:

- Cultivating a culture of security that integrates considerations of gender, religion, sexual orientation, cultural and other personal considerations – including use of policy to accomplish this goal.
- Principles for effective implementation of such approaches.
- Policy considerations.
- Cultural, religious, nationality, sexual orientation, gender-specific and other personal considerations concerning the security aspects of programming and operational situations.
- Overview of protection from sexual exploitation and abuse (PSEA) and gender-based violence (GBV): prevalence, policy and principles, reporting mechanisms and investigations.

IV.12 ***Communications and Information Management***

How to strategically communicate and manage information internally and externally. Managing and securing information is increasingly important in light of technological advances that facilitate widespread dissemination within an organization and externally. Awareness, discipline and transparency are key to how organizations and their personnel can better handle communicating information that is security- or programmatically sensitive.

Key points include but are not limited to:

- The importance of internal and external communications in various program and security scenarios.
- Examining internal and external spheres of communications:
  - how to explain the organization's activities, identity and other information under pressure;
  - the importance of and how to communicate with media;
  - how media can affect mission, reputation and security in crisis management situations; and
  - how communications affect an organization's profile, including advocacy initiatives and their impact on security.
- Information management and security:
  - assessing concerns and needs for information security within the organization at the headquarters and field levels;
  - overview of which mechanisms may be required to ensure discreteness in the organization's communications;
  - IT security considerations;
  - social media and security;
  - good practice in working with sensitive organizational, security, programming and operational information; and
  - how to identify and manage breaches in information security.

IV.13 ***Implementation and Compliance***

How to implement the organization's security policies and security measures, and ensure staff compliance. Implementation of security measures is often a significant gap in security management. Important issues also exist concerning compliance and staff acceptance.

Key points include but are not limited to:

- Overview of barriers and other issues that hinder implementation.
- Ways to overcome barriers and other issues.
- Tools and approaches for better implementation.
- Context and/or organization-specific compliance challenges.
- Tools for specific situations, staff and locations (e.g. processes, structures, roles and responsibilities, meetings, trainings, advisories and monitoring).
- Communicating plans – how to improve staff awareness of security planning.
- Other tools such as simulations and trainer of trainers.

IV.14 ***Security Strategies***

Overview of available security strategies and how to select the best one for a particular organization.

Key points include but are not limited to:

- Security strategies:
  - overview of current NGO strategies used to reduce security and safety risks: acceptance, protection, deterrence, transfer and avoidance;
  - detailed analysis of the pros and cons of each, how they fit with the organization's culture and capacity, and in which operational areas they may be appropriate based on threat and risk assessment;
  - overview of the resource requirements (cost, time, personnel);
- how to use risk assessment to select the best strategy: and
- acceptance: how to strategically conceptualize acceptance within an organization's policies, approaches, and how to access to tools and guidance to systematically cultivate and nurture acceptance in the field. (Active acceptance is increasingly relevant in operational situations.)

IV.15 ***Dealing with Aggression***

How to use interpersonal communications skills to defuse aggression in various situations.

Key points include but are not limited to:

- Principles of communication.
- Overview of different types of aggression and how to recognize their symptoms.
- Understanding the cultural dimension of aggression.
- Techniques for de-escalating aggression.

Elective Topics

IV.16 ***Stress Management in Traumatic or Critical Incidents***

How to use an evidence-based approach to strengthen the organization's culture and policies that support the psycho-social well-being of staff and teams; how to prepare for and respond to such needs in traumatic or critical incidents. It is proven that attending to and promoting staff health and wellness and resilience to stress, and building team cohesion optimizes professional performance.

Key points include but are not limited to:

- Overview of assumptions and evidence about stress and its impact on individuals, teams, organization and performance.
- Review of the organization's duty of care, leadership and management.

- Cohesion and how it can reduce adverse impacts of stress (both traumatic and cumulative).
- Review of policies and practices at the organizational level to foster culture of resilience.
- Overview of staff support issues and support outlets for managing traumatic or critical incidents.
- Communicating with and supporting families: considerations, strategies and other specific issues such as death notification.
- How to recognize when a staff member is suffering from trauma or acute stress.
- How to prepare for and respond to traumatic stress, including principles of psychological first aid and developing protocols.

IV.17 ***Security Implications of Working with Implementing Partners***

Understanding security implications associated with working with implementing partners, including possible moral and legal responsibilities related to transference of risk.

Key points include but are not limited to:

- Overview of different models of partnership between international NGOs and their implementing partners including contractors.
- The duty of care associated with each model of partnership (moral, ethical, legal).
- Overview of tools and options for supporting implementing partners.
- Considerations before deciding to implement it and its impact on program effectiveness.
- Implications including risk transfer, cost and effects on programming.
- Policy and procedural guidance for working with implementing partners.

IV.18 ***Incident Reporting, Monitoring and Analysis***

Review of good practice for incident reporting and the critical need for incident analysis at an organization-wide level.

Key points include but are not limited to:

- The importance incident reporting, monitoring and analysis for enhancing security management, due diligence concerning staff, meeting donor requirements and strengthening interagency collaboration.
- How to develop effective systems for incident reporting to encourage and facilitate reporting and capturing incidents.
- Review of types of information that incident reporting should capture such as trends, groups and individuals most at risk, and management issues.
- Linking incidents through incident pattern analysis and statistics.
- Incident analysis and decision making.
- Using post-incident analysis to strengthen institutional memory and inform effective operational and strategic changes.

IV.19 ***Security Planning***

Overview of security planning good practice for the organization.

Key points include but are not limited to:

- Overview of core global and country security documentation good practice.
- How to optimize security planning for mainstreaming security within the organization.

IV.20 ***Security Networks***

Overview of security information and coordination initiatives, and identifying headquarters-level security stakeholders.

Key points include but are not limited to:

- Overview of existing and relevant interagency security initiatives such as those through the European Interagency Security Forum, InterAction, the International NGO Safety and Security Association, and Saving Lives Together.
- Overview of other security coordination systems (country-specific security information coordination offices).
- The importance of identifying headquarters-level stakeholders such as governments and donors.
- Identifying how programming and presence affect different stakeholders and how they may react.

IV.21 ***Civil-Military Relations***

Key issues in developing and implementing civil-military relations policies.

Key points include but are not limited to:

- Overview of various civil-military relations (cooperation versus coordination) and the impact on security.
- How to assess and minimize the impact on the organization, staff and security both while working with the military and afterwards.
- Organizational considerations in civil-military policy development and in reviewing the organization's policy on interacting with militaries.
- UN frameworks and key guidance documents concerning civil-military relations.

IV.22 ***Using Armed Guards and Escorts***

Understanding considerations and issues that can inform decisions about using armed protection, and how to develop appropriate policies.

Key points include but are not limited to:

- Overview of types and sources of armed protection.
- Reasons for using armed protection.
- The implications of using armed protection, including negative impacts and ethical considerations.
- Criteria, decision making and procedures concerning the use of armed protection.
- If and when exceptions may be needed to the organization's general procedures for using armed protection.

IV.23 **Saving Lives Together**

Overview of the UN-NGO initiative Saving Lives Together.

Key points include but are not limited to:

- Overview of key principles of Saving Lives Together.

IV.24 ***Security Implications of Remote Management***

Understanding security implications associated with remote management of programs, including possible moral and legal responsibilities related to transference of risk.

Key points include but are not limited to:

- Definition of remote management.
- Considerations before deciding to implement it and its impact on program effectiveness.
- Implications of remote management including risk transfer, cost and effects on programming.
- How to improve remote management.
- Policy and procedural guidance for remote management.

SECTION C

Guidance Tools

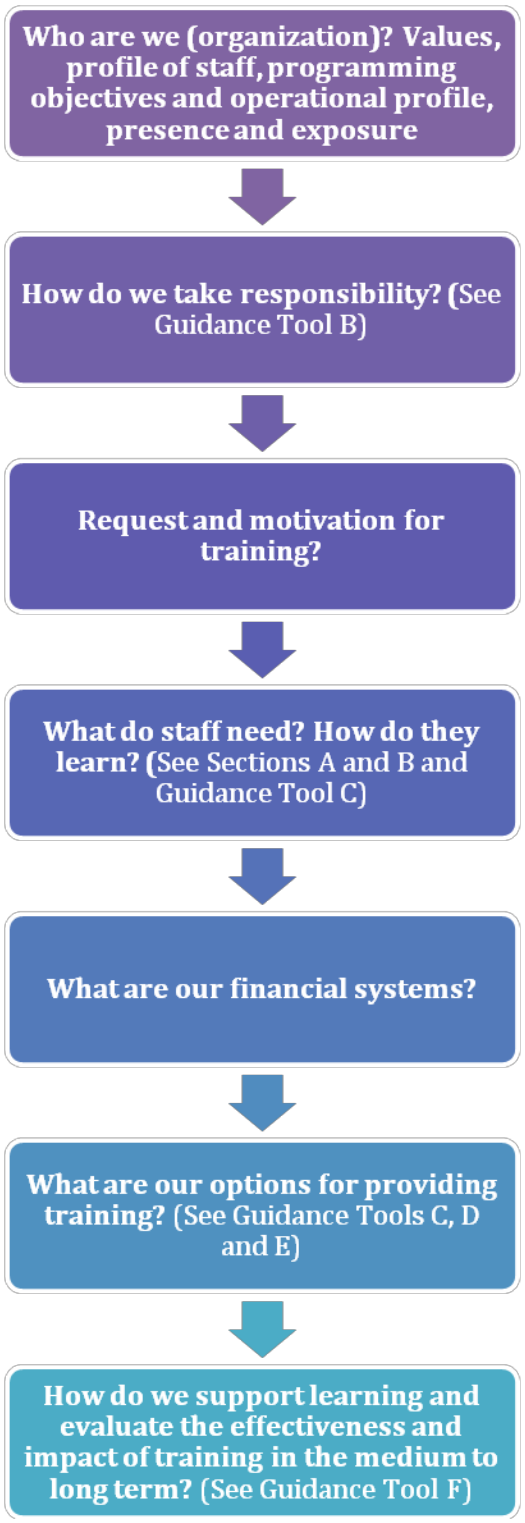
NGO Safety and Security Training Project

2014

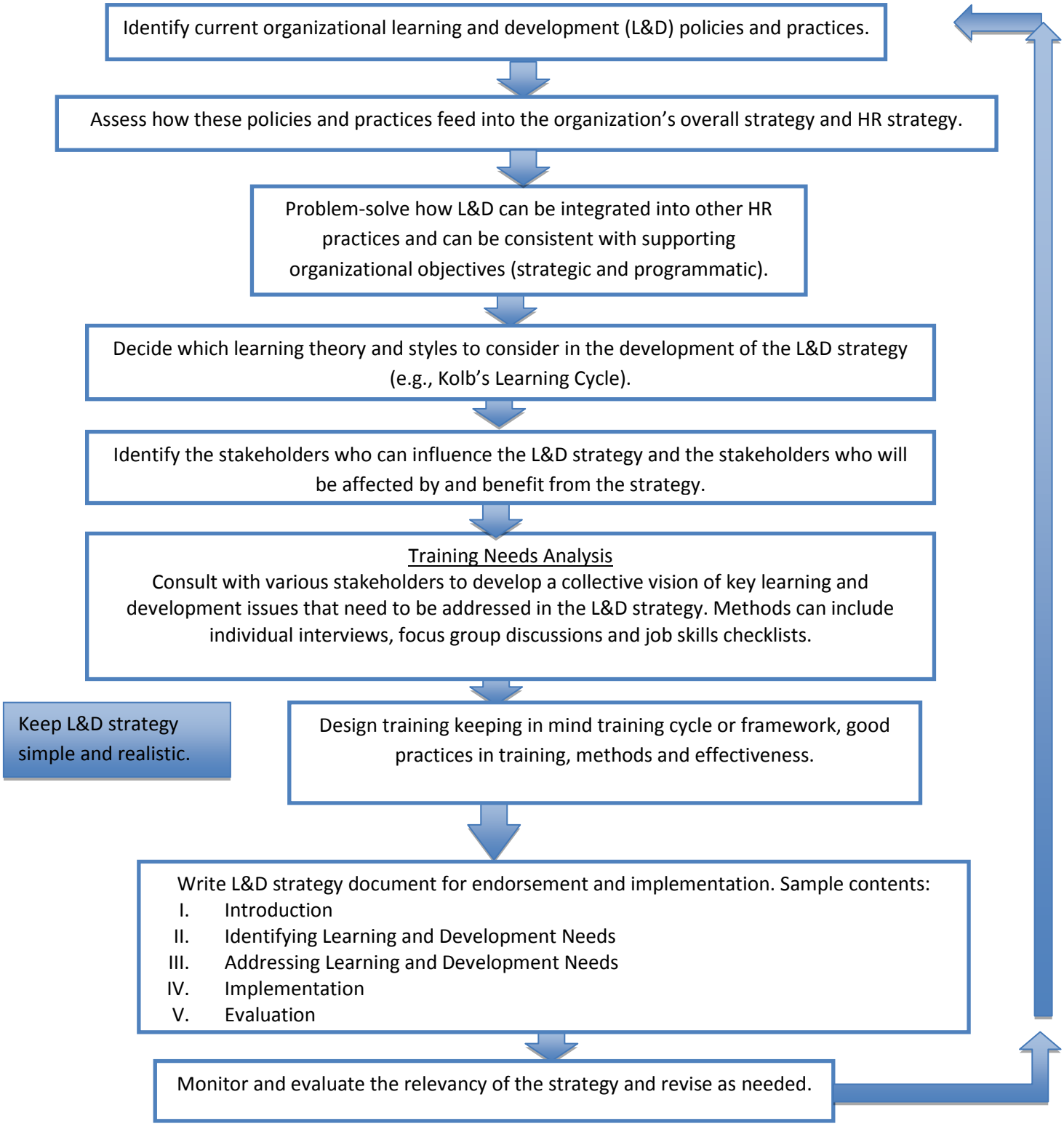
SECTION C - Guidance Tools

A. Organizational Assessment of Learning and Development Needs
B. Guidance on Learning and Development Strategies
C. Overview of Instructional and Learning Methods
D. Guidance on Selecting and Working with Training Providers
E. What to Expect from a Good Trainer
F. Monitoring and Evaluating Effectiveness and Impact of Training
G. NGO Security Training Planning Framework

GUIDANCE TOOL A
Organizational Assessment of Learning and Development Needs



GUIDANCE TOOL B
Guidance on Learning and Development Strategies

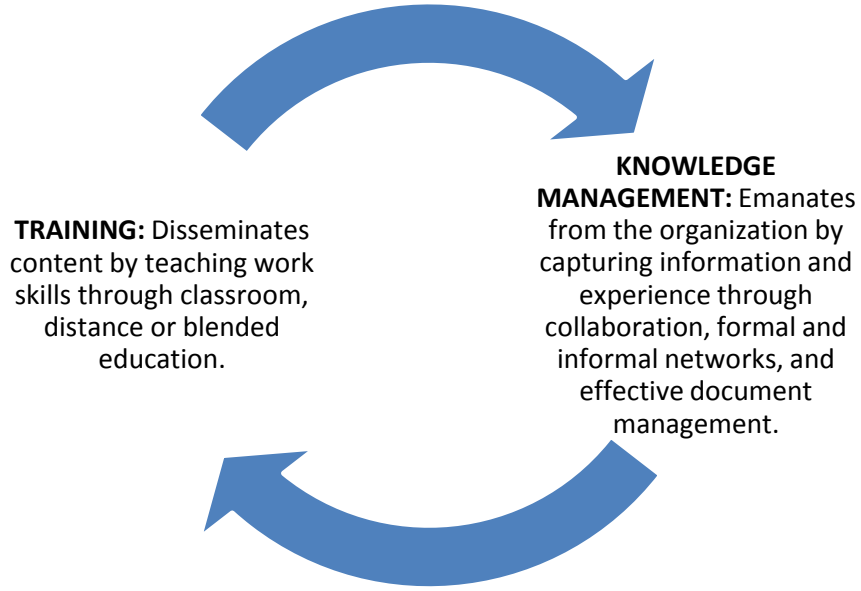


GUIDANCE TOOL C
Overview of Instructional and Learning Methods

Organizations need to know which instructional and learning methods are really available to them given the challenges NGOs face. These challenges include: the pressure to reach and train more people for less money; the tendency of responding to "just in time" learning requests; trying to address donor pressure for cost-efficiency; avoiding duplication of efforts; making resources easily accessible to staff; and the increasing calls to professionalize the sector through certification processes for key positions.

This figure[1] illustrates an integrated learning approach based on the notion that learning is a comprehensive process of informal and formal training methods and events.

INTEGRATED LEARNING



[1] CARE USA 2006

Instructional and Learning Methods

FACE-TO-FACE LEARNING

The following learning methods consist of instructional, on-the-job, self-managed and group learning that is interpersonal: either face-to-face classroom type workshops or use of practical workplace and team approaches and tasks for gaining knowledge and skill.

Method Description	Tools	Advantage	Disadvantage	Considerations
Classroom Theory – Facilitator Led These instructor/facilitator-led interventions support on-the-job learning and self-managed learning to increase performance and meet organizational objectives. The knowledge, skills and behaviors developed in classroom setting must be relevant to the realities of the workplace.	Training courses and workshops: The instructor imparts knowledge and demonstrates skills; participants work individually or in groups through facilitated learning. Case studies, table-top exercises, and open discussion: These provide important problem solving and reflection processes in a safe environment in which individuals can consider ways to respond to a critical incident. Seminars: In these sessions, subject matter experts deliver information by lecture and discussion (limited interaction with participants). Development programs: This is tutor-led classroom work through a variety of activities in the workplace such as self-managed learning assignments and mentoring.	Interaction between peers, team members and opportunities to discuss and process through decision making. Networking and interactions allow for learning between participants. Can provide "learning by doing" opportunities.	May be too didactic, causing excessive reliance on PowerPoint due to the theoretical nature of presentations.	Retention issues and need to design agenda to avoid "cramming" too much in too little time. Being aware of heavy PowerPoint, too much detail, not practical. Design should include mix of theory, didactic, discussion and problem-solving approaches using case studies and exercises; looking at critical thinking, decision-making, judgment and understanding consequences. Engaging facilitators who have good presentation and listening skills and can create positive learning environments.

Simulations – Facilitator Led These instructor/facilitator-led interventions support on-the-job learning and self-managed learning to increase performance and meet organizational objectives. They use active role playing and simulations to impart knowledge, skills and behaviors.	<u>Case studies, table-top exercises and open discussion:</u> These provide important problem-solving and reflection processes that help individuals consider ways to respond to a critical incident. <u>Active simulations and role play:</u> These active learning exercises use role play and simulating events to test reactions and promote understanding and learning through visceral and interactive experiences and scenarios.	Active simulation can be very effective: *"simulation was viewed to be more effective than written information or verbal warnings in preparing humanitarian and development workers to react more aptly to critical incidents and in increasing their sense of control..."*[2] Exposure to a certain amount of controlled anxiety can be very helpful in increasing self-awareness and preparing individuals for possible situations.	Active role play simulations may trigger unnecessary fear and/or may be traumatizing and retrigger PTSD in participants who have had PTSD before. Learning may be affected when people are terrified because fight-or-flight and freeze responses affect the absorption of information. May give a false sense of security because an actual security situation and incident can never be duplicated.	Being aware of distractions (the "fun and adventure" since it does not necessarily provide actual learning); need to be realistic in design and managing expectations. When designing scenarios and simulations, as the level of realism increases, more forethought and awareness should be given to potential negative impacts on the participants. Facilitators need to have important levels of experience to be aware of negative effects (use of violence, explicit and implicit aggression) and to create boundaries and assess the suitability of simulations. Facilitators need to factor flexibility into simulations and include time to debrief, set the stage, monitor and debrief again. They also need discernment to call off a simulation when they observe acute stress in individuals; this is important to prevent inflicting unnecessary harm on participants during training. Need safe psychological and emotional teaching spaces to avoid traumatization.

[2] Yin Wei Chong, "A Study on Factors Predicting Post Traumatic Stress Disorder amongst Humanitarian Workers." 2012

		Networking and interactions allow for learning between participants.	Participants, knowing it is a simulation, may react notably differently than they would in a real situation.	Pre-brief participants on possible reactions (previous and untreated trauma can re-surface in exercises). Have psycho-social and safe outlets available throughout. Allow participants to opt out if they wish. Give participants the opportunity to share openly during debriefing about how they felt during exercise. Ensure the health and physical safety: Avoid injuries No need to use live ammunition. Having clear and strict guidance, methods and debriefing considerations for trained actors in role play.
On-the-job learning On-the-job experience and learning opportunities that involve sharing knowledge and skills and learning from experience.	<u>Orientations</u>: Entering a new role is an optimal time to develop professional networks and a full understanding of expectations about job and role. Set up by managers, they can help new employees to learn the culture and become productive. <u>Observation, demonstration and practice:</u> Watching how tasks are performed, and capturing and re-using information based on what is heard and seen. <u>Delegation:</u> Process used by manager to assign tasks for other staff to complete.	Most job-specific knowledge and skills come from on-the-job learning; this makes these methods optimal for learning by doing. Cost effective. Opportunity for experienced staff to share knowledge.	Motivation and commitment of mentors and learners. Time- and effort-intensive.	Managers must provide time and flexibility for on-the-job learning and other mentoring and coaching activities. Workplace opportunities are a critical learning experiences that compliment other training methods. Formal and informal arrangements.

	Coaching: Involves creating ongoing learning opportunities and providing guidance, feedback at all stages of giving information, listening, demonstrating, encouraging, asking questions and observing someone while they take on new tasks. Mentoring: Process in which a person with more knowledge and experience supports someone with less experience in their career and professional development through informal, face to face communications usually and over a sustained period of time. Ex: Job rotations, shadowing and internships.			
Self-Managed Learning Self learning through reading, e-learning, attending events and pursuing learning outside working hours within the individual's control.	Reading and Development Guides: Reading is critical to development and can consist of job descriptions, work process maps, procedures, manuals, reports, policy, publications and periodicals accessed through sources such as the Internet, intranet and library files. E-learning: Use of any technology based electronic learning programs	Very effective. Cost-efficient. Allows learning about other approaches beyond immediate work sector.	Very dependent on the participant's self-discipline. Dependent on course design. Motivation and commitment of individual to take	Managers should provide flexibility and time for learner to pursue learning. Must have some incentives to encourage and achieve an acceptable level of participation and engagement.

	usually in the form of distance learning. (See below for more information.) Further education: Providing opportunities for learners to pursue outside of working hours and context (often refunded by the organization).		initiative and complete tasks.	
Group Learning - Peer learning and Mentoring This is a form of peer learning that provides practical structure for development.	Working with teams: Could be from other units with differing experience and skills to accomplish specific tasks or project. Networking and communities of practice: Practitioners from a particular specialty or work come together through a membership to network, share work related information, practices, and work on common objectives for improving collective expertise and knowledge. Action learning Form of learning by doing by bringing together an ad hoc group of peers with varying skills and experience for the purpose of analyzing work problems and generating solutions and developing action plans for implementation.	Very effective and low cost. Beneficial for team building, cohesion and performance. Approaches can facilitate dealing with complex issues, problem solving and mainstreaming good practice. Opportunity for experienced staff to share knowledge.	Time and process commitment by several individuals. Reliance on other groups members. Manager commitment for initiating, supervising and evaluating.	Importance of leadership and management in facilitating group processes. Participants can determine what they want to explore, or managers can provide some structure. Smaller groups are better. Learning groups can be set up within a functional areas or department or across the organization. Techniques include presentation on specific topics, case studies, reading groups, problem solving discussions.

Deployment Strategic use of HR options on a case-by-case basis, placing staff who need technical and other skill development into other areas.	Mobility: Movement of staff from one position to another. Secondment: Temporary movement or "loan" of an employee to another department or organization. Temporary assignments and special projects: Flexible, short-term approaches to skill development through an individual performing temporary duties.	Can address gaps and provide technical learning opportunities. Strategic options for HR.	Possibility that skills gained in one area may cause a skill deficit in another and risk of dilution of overall skill base.	Options should be on a case-by-case basis. Formal policies and arrangements for job movements.

HYBRID/BLENDED LEARNING

Considered very effective, hybrid learning (also known as blended learning) methods combine face-to-face training and interactions with electronic distance learning techniques resulting in the blending of technology based asynchronous teaching methods with traditional teaching methods.

Method Description	Tools	Advantage	Disadvantage	Considerations
Blended Learning (also known as hybrid learning) is considered very effective. Methods combine face-to-face training and interactions with electronic distance learning techniques, resulting in the blending of technology based asynchronous teaching methods with traditional teaching methods.	Blended= + instructor led + e-learning courses +/or workbooks and tools +/or workplace assignments	Very efficient and effective learning method.	Time and effort commitment. Relies on self-motivation. Requires a broader strategic approach to learning and development.	Participant time. Transfer of learning. Development timeframes. Cost. Commitment from line managers. Availability of generic materials. Return of investment.

E-LEARNING

E-learning is the use of technology for training, teaching, education and learning purposes. It is an umbrella term for methods such as electronic multimedia learning, computer-based learning, online education, Web-based training and virtual learning. It includes the use of various media (text, audio, video, applications, Internet) as delivery methods for educational approaches and as a medium to communicate knowledge. It can also be an administrative tool. E-learning may be asynchronous or synchronous.

Asynchronous: Self-paced learning that allows learners to exchange ideas and information outside of set times and events. It uses technologies such as email, blogs, wikis and discussion boards, as well as web textbooks, hypertext documents, video and some social networking.

Synchronous: Real-time learning with all learners interacting at the same time within a specific technological platform. It can include discussions, online real-time teacher instruction and feedback, Skype conversations, chat rooms or virtual classrooms with everyone online together and working collaboratively.

Method Description	Tools	Advantage	Disadvantage	Considerations
Virtual Classrooms Virtual classrooms use a mix of communication technologies. Instructors and learners can communicate and interact using microphones, webcams and real-time chatting as a group (e.g., Adobe Connect) or as web conferences, meetings. Learners can write on a shared whiteboard when allowed by instructor.	**Chat Rooms** Virtual rooms in which individuals correspond with other participants. Chat rooms are often used as virtual classrooms enabling distance learners to communicate with their instructor and peers. **E-mail** Can be used as an asynchronous distance communication platform between learners, instructors and peers carrying messages and files to facilitate learning. **GoToMeeting, webinars, online training and workshops** Real-time, point-to-point Web and video conferencing and	Convenience for learners. Provides flexibility and freedom to learn when and where the learner prefers and at their own pace. Increases access to learning opportunities.	Production costs can be exorbitant, especially when "shelf life" of a training product is not considered (e.g., development to delivery ratios of computer-based and any training incorporating multimedia learning).	Technology need to be seen as a training tool rather than an end unto itself. **Be sure to consider privacy and security issues associated with Internet discussions.** E-learning requires motivation, because it is not tactile. To be effective, it needs to be facilitated to garner motivation, because people generally need physical interaction and need process. Internet connectivity and bandwidth can limit video streaming, screencasts and the like; bandwidth for field offices needs to be assessed before considering these options. Optimal e-learning development requires good graphics design sense (e.g., typeface selection, images, formatting). While content may be good, if the manner in which it is presented and the user interface

Other technology include text notes, microphone rights, and breakout sessions in which learners can work collaboratively in small groups to accomplish a task and instructors can have private conversations with learners. Participants can receive direct instruction from instructor. Structured, scheduled classes can be recorded and stored on a server, which helps with reviewing materials for exams. This provides a social learning environment.	communications that allow meetings, lectures, presentations or training applications to share and interact with attendees in remote locations via the Internet. **Discussion boards** Internet- or intranet-based forums where both instructors and learners can post assignments, questions, case studies or messages that can be read and responded to by all other participants. **Audio** Use of audio (recorded or streamed via internet through webcasts, podcasts). **Video** Optimal for visual learners; can be sourced by DVD, streaming or downloading from internet, YouTube, messaging or interacting with guest speakers such as through Skype, Adobe connect or web cams and interactive video games. Some believe retention is higher when video is used in lessons.	E-learning requires motivation, because it is not tactile. Supervision and constant feedback needed. Need for technology equipment and knowledge of how to use computers. Concern over the use of public social media tools by employees – impact on the organization and perception of social media as trivial or a distraction.	are substandard, retention and engagement can be greatly diminished. Chat rooms, forums and e-mail lists all need moderators for maximum effectiveness. Moderators steer conversations, engage participants and police discussions. Chat rooms and instant messaging favor learners who have strong written skills and can type fast. Verbally strong learners are often at a disadvantage in this context. Participants with mixed primary native languages can have difficulties participating. If English is used with multicultural audiences, ensure terms and concepts are kept simple. Depends on creating a positive environment where participants are involved with others and the facilitator(s); should include assistance, encouragement, collaborative peer interaction, sense of community and course work at every step. Provide interactive multimedia exercises to develop problem-solving skills. Must have access to technology and computer skills. Provide clear staff guidance on the use of social media for learning within organization.

Computers, tablets, smart phones, and e-book readers
Devices that allow to access websites or other programs such as images, PDF, sharing by email, sharing resources on specific websites and/or intranets, documents or may support mobile-learning (m-learning).

Social Media
Allows people to share through discussion and conversation (experiences or resources), learn from each other and/or collaborate. Examples include blogs, social bookmarking, discussions, wikis and file sharing.

Blogging
Space for instructors and learners to post thoughts, ideas, comments on a website can foster interactive learning.

Webcams
Video cameras that allow participants to be seen and see others on the Internet so they can engage visually with others.

	Whiteboards Interactive learning and engaging through whiteboards or smart boards that allow instructors and learners to write on a touch screen. **Screencasting** Recent trend in e-learning where screens can be shared directly from a browser and which makes video available online for immediate streaming. This gives presenters another way to present ideas and share flow of thoughts; allows learners to pause and rewind.			
Linear Learning Computer-based and web-based training consisting of self-paced learning platforms via a computer or handheld device such as a tablet or smartphone. Contents are delivered by CD-ROM or a web browser and include video and animation to enhance learning. Usually includes multiple choice, drag and drop, radio button, simulation or other interactive activities.		Convenient for learners. Provides flexibility and freedom to learn when and where the learner prefers and at his/her own pace. User friendly with individual learning preferences. Stimulating through use of media (video and animation).	Creating web- or computer-based trainings requires significant resources. Software for developing such training is very complex. Lack of human interaction can limit content that can be presented.	Use smaller web/computer-based learning activities as part of a broader learning program that includes other online discussions and interactive activities.

			Need for technical equipment and knowledge of how to use the technology.
Collaborative Learning Uses instructional methods designed for students to work together on learning tasks (e.g., E-learning 2.0); instructor does not serve as the main source of knowledge and skills.	Blogs, wikis and cloud-based docs portals (e.g., Google docs and Dropbox) podcasts and virtual worlds. E-Learning 2.0: Instead of solely using and evaluating assignments, the focus is on social learning and use of social software.	Social and community aspect; can tap into potential benefits of the adage that one of the best ways to learn is by teaching others.	Requires instruction on how to use technology.
Administrative Tools Software used for delivering, tracking and managing trainings and education.	**Learning Management Systems:** Delivery, tracking and managing trainings by tracking attendance, time spent and progress of learner. Post announcements, grade assignments, check course activity, participate in discussions. Work can be submitted, read and responded to, quizzes (e.g., Blackboard Inc. and Moodle). **Electronic Performance support systems (EPSS):** computer based system that improves worker productivity by providing on the job access to integrated information advice and learning	Creation and maintenance requires significant initial and ongoing investment.	

	experience.

GUIDANCE TOOL D
Guidance on Selecting and Working with Training Providers
PART I - Selecting Training Provider

Security training needs are identified through a training needs analysis and/or are included in a learning and development strategy.

How can training needs be best addressed?
(method, capacity, expertise, resources, timing, location)

Internal training
Existing, updated and relevant curriculum, trainers, resources or capacity to develop and deliver training courses or e-learning or ability to implement self-managed training

External training
Decision-making processes and policy regarding use of external training providers

LOWER COST DOES NOT MEAN BETTER OPTION

Sample criteria for selecting external training provider

- What is their profile? Values, motivation, ethics, culture and gender sensitivity, and how does this fit with your organization and staff (individuals and teams)?
- What is their reputation? Capacity for providing training and expertise (references, vetted, credible testimonials), and how does this affect the organization's image?
- What is the cost? Preparation, travel, delivery pre- and post-event work, and are they reasonable for what you are requesting (value for money and comparatively to other providers; exorbitant versus undermining others)?
- Who are their trainers or associate trainers? Skills, knowledge, experience, teaching ability, gender.
- Can you request specific trainers specifically?
- What is their availability, proximity and deployability? Do they have presence in the location where training is needed?
- What are the training content, approach and methods? Do they correspond to your needs and community practices?

What type of training is needed or best-suited?

Open courses or generic

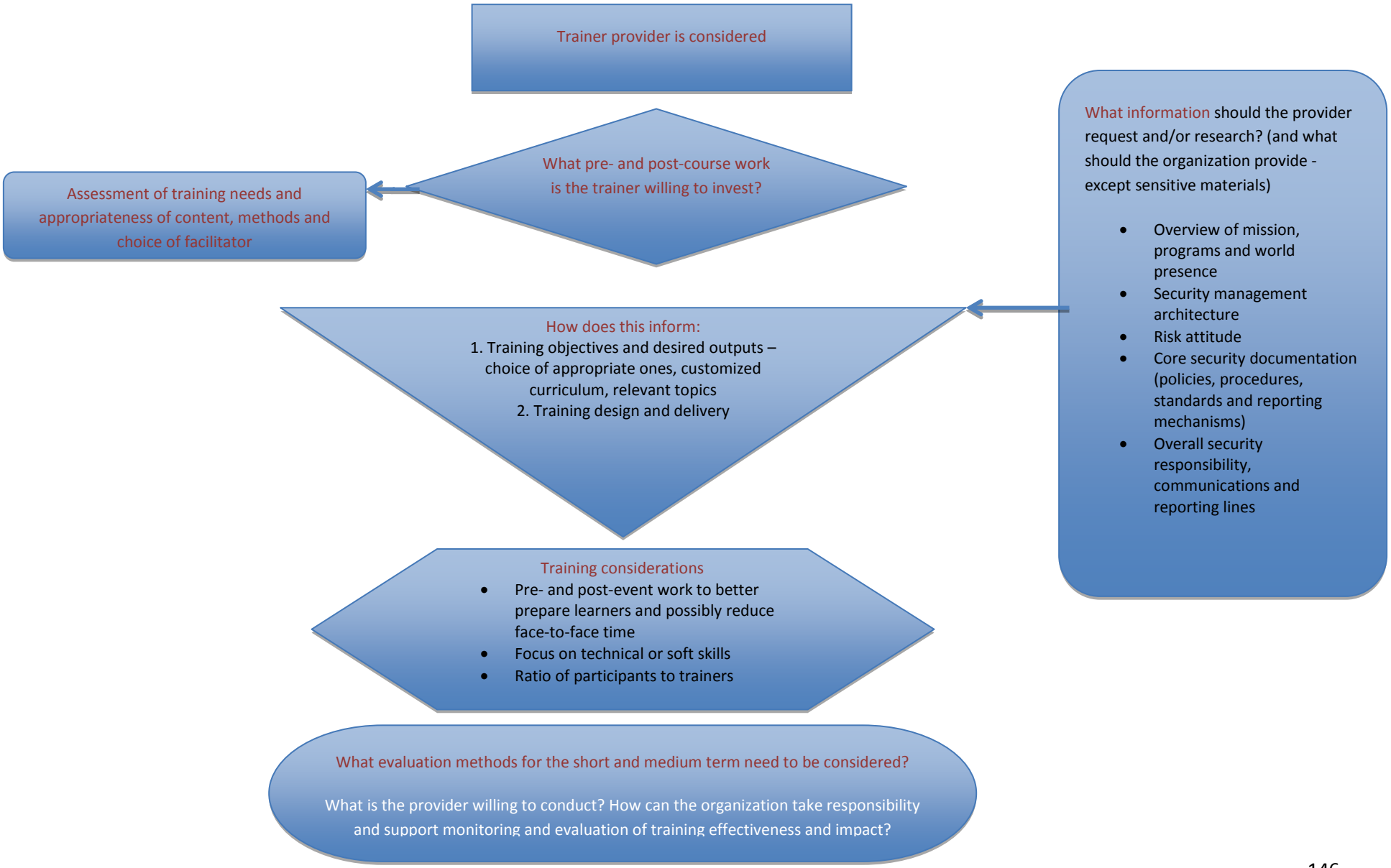
Organization/office-specific

See next page – working with providers

What are your choices of external providers?

- Nonprofit (NGOs, organizations, private)
- Private security providers (for-profit)
- Individual consultants
- Other organizations
- UN

PART II - Working with External Training Providers



GUIDANCE TOOL E
What to Expect from a Good Trainer (checklist)[3]

Humanitarian and Development Assistance: experience and knowledge

- ☐ Has credible experience working for an NGO in a security risk environment.
- ☐ Understands programming and operational realities and sensitivity.
- ☐ Ideally has worked in programming, emergencies and management.
- ☐ Keeps up to date on emerging humanitarian and development issues, evolving approaches and initiatives within the humanitarian and development sectors.

Safety and Security: experience and knowledge

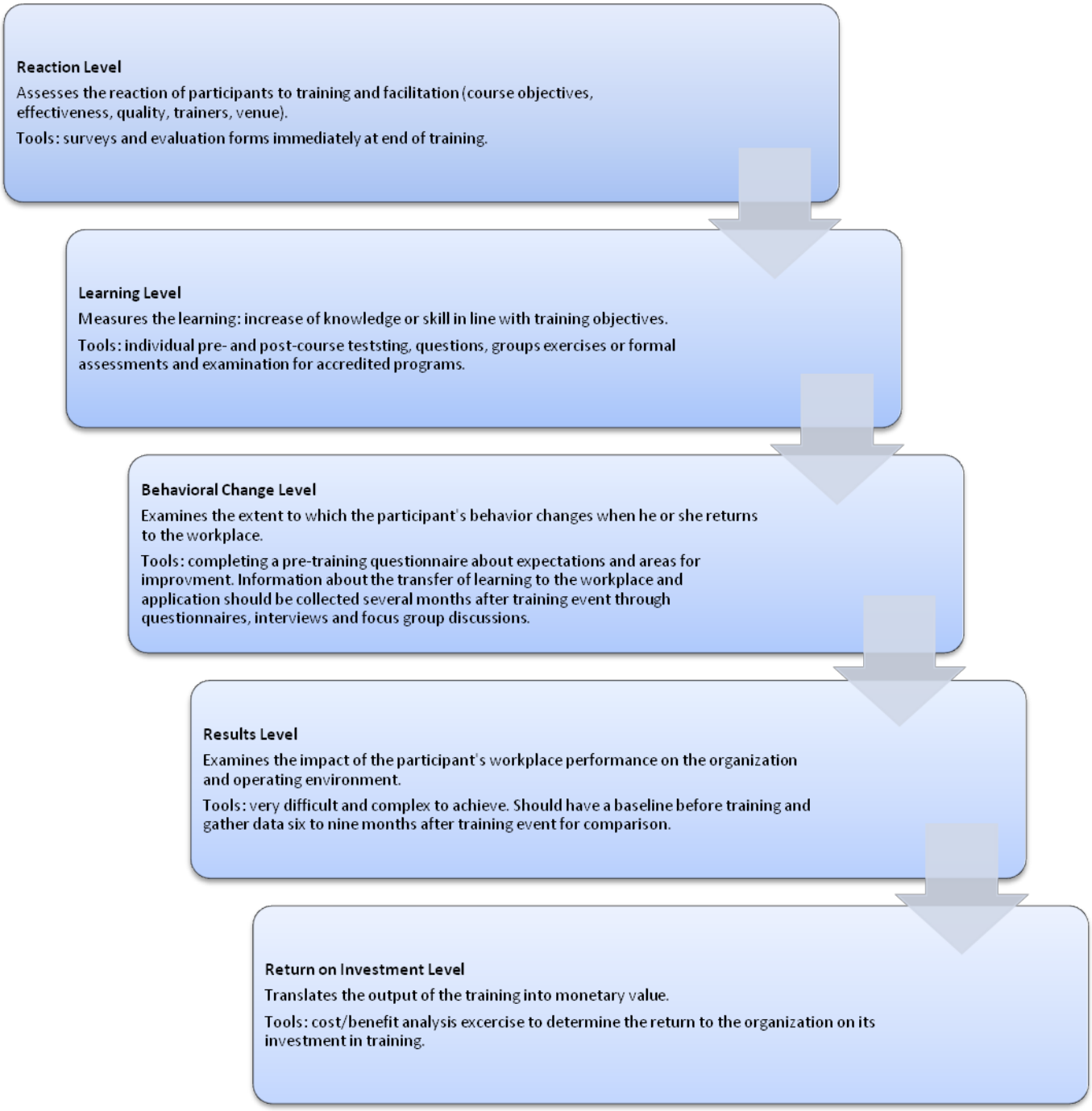
- ☐ Familiar with NGO security management and personal security approaches and practices.
- ☐ Familiar with relevant safety and security resources.
- ☐ Keeps current and active in NGO security management developments, forums and initiatives.
- ☐ Stays current on changes that occur over time in security management and personal security including evolving issues, approaches and resources.

Teaching Competencies

- ☐ Familiar with different and evolving security training curricula.
- ☐ Understands and can develop and use lesson plans.
- ☐ Clear understanding of goals and learning objectives for every course they teach.
- ☐ Thoroughly familiar with the subject matter and teaching materials.
- ☐ Able to differentiate between need to know and good to know information for each topic and course.
- ☐ Familiar with NGO security and other related resources relevant to each training they provide.
- ☐ Engaging presentation style and aware of teaching methods (lecture and non-lecture) and how to use them effectively.
- ☐ Good listening skills and able to foster positive learning environments.
- ☐ Able to effectively manage the time and flow of classroom activities.
- ☐ Skilled at facilitating exercises and evaluating the performance of participants.
- ☐ Able to demonstrate skills and knowledge.
- ☐ Skilled in providing positive and constructive feedback based on objective criteria and in providing space for learners to complete tasks.
- ☐ Able to create, present and debrief scenarios appropriate to the course objectives and participant abilities.

[3] Inspired from Wilderness Medical Associates Canada checklist for Trainers

GUIDANCE TOOL F
Monitoring and Evaluating Effectiveness and Impact of Training



GUIDANCE TOOL G
NGO Security Training Planning Framework

The following charts covers the goal, objectives, learning outcomes and topics for each level or sublevel. The topics reflect issues relevant to the particular level or sublevel. The amount of time it takes to cover different topics may vary significantly. For those familiar with the term "module" as used by the training community, keep in mind that "topic" as used in this document is not the same thing.

LEVEL I - SUMMARY CHART OF OBJECTIVES, LEARNING OUTCOMES AND TOPICS

This chart summarizes the objectives for each sublevel of Level I. For each objective, it also lists core and elective topics to help achieve that objective. The chart is a roadmap, summarizing each objective, its learning outcomes and topics.

Level IA – Basic Personal Security Level IA provides an introduction to personal security and how one's behavior affects safety and security by teaching participants about self-awareness, relevant security matters and how to respond to security risks in low-risk environments.			
Key Objectives	**Key Learning Outcomes**	**Core Topics**	**Elective Topics**
1. Encourage self-reflection about personal vulnerabilities, limits, strengths, resilience, emotional intelligence and other key objectives.	Participants understand their personal vulnerabilities, limits, strengths, resilience, emotional intelligence and other key objectives.	IA.2 Personal Awareness and Behavior IA.4 Awareness of Gendered, Cultural and Personal Considerations IA.7 Resiliency and Stress Management IA.8 Crime Awareness and Prevention IA.12 Dealing with Aggression	

2. Explain the operating environment and cultural, gender and personal considerations as they relate to security.	Participants understand their operating environments and cultural, gender and personal considerations as they relate to security.	IA.3 Situational Awareness IA.4 Awareness of Gendered, Cultural and Personal Considerations IA.7 Resiliency and Stress Management	
3. Present security concepts and how they relate to security strategies and programming.	Participants understand security concepts, how to apply them to the organization's security strategies and program goals, and understand the interaction between security and programming.	IA.1 NGO Security Concepts IA.5 Personal Risk Assessment and Risk Reduction IA.6 Travel Safety IA.10 Acceptance IA.13 Programming and Security	
4. Explain common threats and present information on good practice in personal security prevention and response.	Participants understand common threats, and know how to assess, reduce and respond to the security and safety risks they may face in a low-risk security context.	IA.8 Crime Awareness and Prevention IA.9 Gender-Based Violence (GBV) IA.12 Dealing with Aggression IA.14 Hostile Observation Awareness IA.15 Information Security	

5. Explain how to develop a personal safety and security strategy and set a personal risk threshold.	Participants know how to conduct a personal risk assessment and use it to develop a personal safety and security strategy and set a personal risk threshold.	IA.5 Personal Risk Assessment and Risk Reduction IA.11 Incident Reporting	

Level IB – Advanced Personal Security Levels IB develops self and team awareness for higher security risk environments by teaching participants security management and good practices in prevention and response to security situations.			
Key Objectives	**Key Learning Outcomes**	**Core Topics**	**Elective Topics**
1. Explain how to recognize and analyze security risks in medium- to high-risk working environments.	Participants know how to recognize and analyze security risks in medium- to high-risk working environments.	***All material covered in Basic Personal Security (IA) plus:*** I.B.2 Situational Analysis I.B.3 Risk Assessment	
2. Provide general awareness of security management concepts, good practice and strategies.	Participants understand security management concepts, good practice and strategies.	***All material covered in Basic Personal Security (IA) plus:*** I.B.1 Security Framework I.B.4 Risk Reduction Strategies I.B.5 Acceptance I.B.10 Security Stakeholders I.B.4 Security Strategies	
3. Prepare participants to assess and handle situation-specific security and safety risks.	Participants know how to assess and manage situation-specific security and safety risks.	***All material covered in Basic Personal Security (IA) plus:*** I.B.4 Risk Reduction Strategies I.B.7 Residential and Office Security I.B.11 Safety Threats	

4. Prepare participants to identify, mitigate and respond to security threats.	Participants know how to identify, mitigate and respond to security threats and have used simulations to practices these skills.	***All material covered in Basic Personal Security (IA) plus:*** I.B.6 Travel Safety and Security I.B.9 Field Communications I.B.12 Evacuation, Hibernation, Relocation I.B.13 Grab Bags	
5. Encourage additional self-assessment to help participants' refine their personal thresholds of acceptable risk.	Participants know how to use self-awareness to understand and set their personal risk thresholds; participants also understand and can support individual and team resilience.	***All material covered in Basic Personal Security (IA) plus:*** I.B.8 Personal and Team Resilience	

Level IC – Personal Security in Violent Environments Level IC teaches participants the contextualized security awareness and skills (prevention and response) they need for specific security threats in severe security risk environments.			
Key Objectives	**Key Learning Outcomes**	**Core Topics**	**Elective Topics**
1. Teach participants about threats and risk in their working environments and their and their organization's vulnerability to these threats.	Participants understand the specific security risks (including incident patterns and threats) in their operating environments. They also understand their vulnerability and the organization's vulnerability in their operating environments.	***All material covered in Basic and Advanced Personal Security (IA and IB) plus choice of elective topics based on context and security risk.***	I.C.1 Terrorism I.C.2 Improvised Explosive Devices and Bombs I.C.3 Landmines and Explosive Remnants of War (Unexploded Ordinance) I.C.4 Indirect and Direct Fire, Shelling and Weapons I.C.5 Crowds, Mobs and Demonstrations I.C.6 Kidnapping, Abduction and Hostage Taking I.C.7 Advanced Hostile Observation Awareness I.C.8 Hostile Checkpoints I.C.9 Helicopter Landing Procedures I.C.10 Convoy Travel I.C.11 Protective Equipment I.C.12 Acceptance
2. Provide guidance on how to prevent and respond to specific threats.	Participants know how to prevent and respond to specific threats.		
3. Explain risk mitigation and teach participants how to use mitigation tools.	Participants are able to effectively use risk mitigation tools in different situations; simulation exercises have been used to help participants practice and to test participant mastery of those skills and their skills for identifying and responding to security risks.		

LEVEL II - SUMMARY CHART OF OBJECTIVES, LEARNING OUTCOMES AND TOPICS

This chart summarizes key competencies for participants to master in Level II. For each objective, it also lists core and elective topics to help achieve that objective. The chart is a roadmap, summarizing each competency, its learning outcomes and topics.

Level IIA – Field Security Focal Points Level IIA provides necessary training to staff responsible for establishing, implementing, running and/or managing the organization's field security systems.			
Key Objectives	**Key Learning Outcomes**	**Core Topics**	**Elective Topics**
1. Teach participants how the organization's security framework works and review the participants' security responsibilities within that framework.	Participants understand security, risk management frameworks, and how the organization's security framework policies and mechanisms work. Participants understand their security responsibilities and those of other management staff. Participants understand the difference between safety and security, and when each applies to their responsibilities.	II.A.1 Humanitarian Principles and International Humanitarian Law II.A.2 Roles and Responsibilities II.A.3 Security Risk Management Framework II.A.4 Programming, Policy, Operations and Security	

2. Teach participants the skills necessary to meet the office's day-to-day security needs.	Participants can conduct risk assessments and develop risk reduction measures as needed. Participants can develop and help implement security planning and security measures as needed. Participants can conduct technical security tasks such as security orientations and site assessments. Participants are able to monitor changing risks in the working environment and develop corresponding scenarios. Participants can update security planning and measures.	II.A.5 Situational Analysis - Using Security Tools II.A.6 Risk Assessments II.A.7 Risk Reduction Strategies II.A.8 Standard Operating Procedures and Contingency Planning II.A.16 Managing Guards and Drivers II.A.17 Travel Safety and Security II.A.18 Travel and Movement Tracking II.A.19 Site Security II.A.22 Health and Safety II.A.26 Practical Issues in Building Acceptance II.A.27 Dealing with Aggression	II.A.28 Working with Armed Protection and Private Security Companies II.A.29 Civil-Military Relations at the Operational Level II.A.30 Hostile Observation Awareness

3. Teach participants how to communicate effectively with staff, security coordination platforms, authorities, the local community and beneficiaries.	Participants can develop and use the various communication tools needed to communicate security-related information. Participants can identify and engage with internal and external security stakeholders. Participants are better equipped to network and engage in security consultation processes.	II.A.10 Incident Reporting and Analysis II.A.12 Security Stakeholders II.A.13 Consultative Processes II.A.14 Cultural, Gendered and Personal Considerations II.A.15 Leadership and Management II.A.16 Managing Guards and Drivers	II.A.32 Saving Lives Together
4. Teach participants how to execute crisis management responsibilities.	Participants can manage and/or support incident response as appropriate (depending on severity). Participants understand the organization's incident reporting, tracking and analysis mechanisms and practices.	II.A.9 Supporting Incident and Crisis Management II.A.11 Stress Management	

5. Teach participants how to monitor and communicate changes to operating environment and revise field office protocols as necessary.	Participants know how to request and access internal and external support to fulfill their responsibilities. Participants can identify local resources for security management.	II.A.20 Information Security and Management II.A.21 Security Briefings and Orientation II.A.23 Practical Issues in Implementing Security II.A.24 Monitoring Security on a Daily Basis II.A.25 Practical Issues in Updating Security Information and Planning	II.A.31 Communicating and Working with Senior Management

Level IIB – Drivers Level IIB is drivers and other staff who drive vehicles in the course of their work and/or are responsible for the movements of personnel and assets. It teaches participants safe and evasive driving techniques and other good practice in vehicle and travel safety and security.			
Key Objectives	**Key Learning Outcomes**	**Core Topics**	**Elective Topics**
1. Explain the organization's vehicle and travel security policies and procedures.	Participants understand the organization's vehicle and travel policies and procedures.	II.B.3 Vehicle and Fleet Safety and Security Standards	
2.Review the roles and responsibilities of a driver.	Participants are clear about their specific responsibilities and duties and understand their ambassadorial role.	II.B.15 Field Communications II.B.16 Dealing with Aggression II.B.18 Vehicle Travel Security II.B.19 Health and Safety	
3. Provide technical guidance on safe travel, vehicles, routines, planning and rules.	Participants are equipped to assess, reduce and react in specific safety and security situations. Participants are equipped with technical and soft skills necessary to fulfill their responsibilities.	II.B.1 Mission, Policies, Procedures, Programs and Culture II.B.2 Roles and Responsibilities II.B.3 Vehicle and Fleet Safety and Security Standards II.B.4 Risk Assessments II.B.5 Vehicle Inspections, Maintenance and Basic Repairs II.B.6 Preparation and Route Planning II.B.7 Vehicle Handling, Defensive Driving and Evasive Driving II.B.8 Driving at Night, in Poor Visibility and Poor Weather II.B.9 Local Laws and Other Road Signs and Signals II.B.10 Passenger Safety II.B.11 Cargo Safety II.B.12 Accident Procedures and Reporting II.B.13 First Aid Kits	II.B.20 Hostile Observation Awareness II.B.21 Convoys II.B.22 Checkpoints II.B. 23 Driving with Armed Protection and Escorts

4. Teach other necessary interpersonal communications skills.	Participants are able to enforce safety and security measures regarding the organization's vehicles and during travel. Participants are able to build discipline around good practice concerning vehicle and vehicle travel requirements.	II.B.14 Practical Issues in Building Acceptance II.B.17 Cultural, Gendered and Personal Considerations	

Level IIC – Guards Level IIC teaches guards how to effectively perform their security management responsibilities.			
Key Objectives	**Key Learning Outcomes**	**Core Topics**	**Elective Topics**
1. Explain the organization's office and premises security policies and procedures.	Participants understand the organization's office and premises security policies.	IIC.1 Mission, Policies, Procedures and Culture II.C.3 Local laws	
2. Review the roles and responsibilities of a guard.	Participants are clear about their specific responsibilities and duties and understand their ambassadorial role.	II.C.2 Roles and Responsibilities	
3. Teach participants concrete technical skills regarding procedures and dealing with specific situations.	Participants know how to assess, reduce and react in specific safety and security situations. Participants are equipped with the technical and soft skills necessary to fulfill their responsibilities.	IIC.4 Patrolling IIC.5 Risk Assessments IIC.6 Health and Safety IIC.7 Fire Safety IIC.8 Emergency Response Procedures IIC.9 Evacuation Drills IIC.12 Field Communications IIC.13 Visitor Access IIC.14 First Aid Kits	IIC.16 Hostile observation awareness
4. Teach participants other necessary interpersonal communications skills.	Participants are able to enforce safety and security measures in the facilities they are guarding. Participants are able to adopt good practice in meeting facility security requirements.	IIC.10 Dealing with Aggression IIC.11 Cultural, Gendered and Personal Considerations IIC.15 Practical Issues in Building Acceptance	

LEVEL III – SUMMARY CHART OF TOPICS AND OBJECTIVES

This chart summarizes key objectives for Level III. For each objective, it also lists core and elective topics to help achieve that objective. The chart is a roadmap, summarizing each objective, its learning outcomes and topics.

Level III targets staff responsible for developing, managing, reviewing and advising on security issues, teaching them the soft and hard skills they need to ensure programs are implemented within an acceptable level of security risk.			
Key Objectives	**Key Learning Outcomes**	**Core Topics**	**Elective Topics**
1. Provide an overview of all components of security risk management.	Participants understand that security must be a constant priority throughout the organization, reflected in policies, planning, budgeting and overall management in field offices and operations. Participants understand security, risk management frameworks, and organizational security management mechanisms and policy. Participants are equipped to mainstream effective security management throughout the organization's policies and programs.	III.1 Security Risk Management Frameworks III.6 Security Planning – Development and Review III.12 Budgeting and Resources for Security III.16 Site Selection and Security III.20 Security and Training III.21 Programming and Security III.28 International Legal Frameworks	
2. Explain the relationship between security and duty of care and the participant's related responsibilities.	Participants understand their security roles and responsibilities and those of others as well.	III.14 Security Stakeholders III.17 The Organization's Security Management Architecture, Policies and Standards	III.30 Security Networks III.31 Engaging Private Security Providers III.32 Negotiating Access

	Participants understand duty of care.	III.18 Accountability Frameworks III.19 Duty of Care and Legal Liability	III.33 Working with Armed Protection and Private Security Companies III.34 Working with Implementing Partners: Security Considerations III.35 Security Implications of Remote Management of Programs III.45 Civil-Military Relations III.46 Saving Lives Together
3. Teach participants how to use information to improve the organization's security culture.	Participants understand the organization's information security and management policies and practices. Participants are able to develop and enforce protocols for managing, securing and analyzing information.	III.13 Information Management and Security III.15 Field Security Assessments, Advisory and Monitoring Activities III.22 Incident Reporting, Monitoring and Analysis III.24 Security Self Assessments and Audits	III.34 Media Training III.39 Cash Security
4. Teach participants how to manage security risk management processes and training, and how to supervise others with security support responsibilities.	Participants understand their leadership role in security management, security training and meeting related support needs of their staff.	III.2 Context Assessment and Situational Analysis III.3 Risk Assessments and Understanding Risk Thresholds III.4 Risk Reduction Strategies III.5 Acceptance	III.41 Integrating Safety and Security in Emergency Response III.42 Hostile Observation Awareness III.43 Health and Wellness

	Participants are equipped to enable effective security management through technical and management skills.	III.7 Implementation and Compliance III.9 Leadership and Management at the Country and Regional Levels III.10 HR and Security III.11 Cultural, Gendered and Personal Considerations in Security III.16 Site Selection and Security III.20 Security and Training III.25 Managing Guards and Drivers	
5. Equip senior managers to effectively handle incidents.	Participants understand the organization's crisis and incident management structures, decision-making authority, policies and protocols. Participants know how to deal with security incidents and their impact.	III.8 Stress Management In Traumatic or Critical Incidents III.23 Managing the Full Spectrum of Incidents and Post-Incident Recovery III.26 Crisis Management III.27 Evacuation, Hibernation, Relocation and Suspension III.29 Dealing with Aggression	III.33 Gender-Based Violence (GBV) – Prevention and Case Management III.38 Kidnapping, Abduction and Hostage Taking III.40 Managing Situation-Specific Threats and Incidents III.44 Operational Continuity

LEVEL IV - Summary Chart of Topics and Objectives

This chart summarizes key objectives for Level IV. For each objective, it also lists core and elective topics to help achieve that objective. The chart is a roadmap, summarizing each objective, its learning outcomes and topics.

Because of the complexity of this level's targeted audience, the topics are further divided under these groups:

1. Corporate governance (e.g., board members, CEOs and presidents)
2. Technical senior management at the headquarters level (e.g. security directors, human resources, operations, administration, finance, communications)

Level IV present participants with the key concepts and skills necessary to establish and maintain an organization-wide security vision, leadership, strategy and framework.			
Key Objectives	**Key Learning Outcomes**	**Core Topics**	**Elective Topics**
Explain the importance of strategic and effective security management.	Participants understand that security must be an ongoing priority throughout the organization, reflected in policies, planning, budgeting and global management. Participants understand security, risk management frameworks, and organizational security management mechanisms and policy. Participants understand duty of care (moral, ethical and legal).	Corporate Governance IV.4 Duty of Care Senior Management IV.4 Duty of Care IV.7 Risk Management and Operational Continuity IV.11 Cultural, Gendered and Personal Considerations in Security	

Equip participants to be able to develop a strategic vision for creating and maintaining a security culture.	Participants are able to build security into the organization's global and strategic vision. Participants are able to create a sustainable security culture mainstreamed throughout the organization.	<u>Corporate Governance and Senior Management</u> IV.2 Strategic Planning <u>Senior Management</u> IV.5 Security Policy, Principles, Standards and Guidance IV.9 Budgeting and Resources for Security IV.13 Implementation and Compliance IV.14 Security Strategies	
Equip participants to develop organization's security risk management frameworks and comprehensive security management capacity.	Participants are familiar with key components and issues to address in a security framework, and know how to develop a framework to meet the needs of their organization. Participants develop the skills to construct and oversee a comprehensive security management capacity for the organization.	<u>Corporate Governance and Senior Management</u> IV.1 Security Risk Management IV.3 Security Management Architecture and Capacity	
Equip participants to be able to ensure strategic level leadership, understanding, prioritization and governance of the organization's security management framework and systems to enable realization of organization objectives.	Participants develop the leadership and strategic conceptual skills needed to mainstream effective security management throughout the organization's policies and programs. Participants understand their role in security management, security training and meeting related support needs of their staff and programs.	<u>Corporate Governance and Senior Management</u> IV.2 Strategic Planning <u>Senior Management</u> IV.1 Security Risk Management IV.2 Strategic Planning IV.8 Programming and Security IV.10 Human Resources and Security IV.12 Communications and Information Management	<u>Senior Management</u> IV.17 Security Implications of Working with Implementing Partners IV.19 Security Planning IV.21 Civil-Military Relations IV.22 Using Armed Guards and Escorts IV.24 Security implications of Remote Management

Equip participants to be able to deal with critical incidents – prevention, response and post-recovery.	Participants understand the components and resources necessary to deal with critical security incidents and their impact.	<u>Corporate Governance and Senior Management</u> IV.6 Crisis Management IV.7 Risk Management and Operational Continuity <u>Senior Management</u> IV.12 Communications and Information Management IV.15 Dealing with Aggression	<u>Senior Management</u> IV.16 Stress Management in Traumatic or Critical Incidents IV.18 Incident Reporting, Monitoring and Analysis

Annexes

NGO Safety and Security Training Project

2014

ANNEX 1: Glossary of NGO Safety and Security Training Terminology

Awareness: knowledge or perception of a situation or fact: there is a lack of awareness of the risks; concern about and well-informed interest in a particular situation or development.

Curriculum: a set of courses constituting an area of specialization; the subjects comprising a course of study.

Core Curriculum: set of courses that are considered essential (or required) for specific acquisition of skills and knowledge.

Elective Curriculum: set of courses that are optional and selected for interests, specialization or other reasons.

Executive: a person with senior managerial responsibility in an organization.

Evaluation: the making of a judgment about the amount, number or value of something; assessment.

Facilitator: a person who helps to bring about an outcome (learning, productivity, or communication) by providing indirect or unobtrusive assistance, guidance or supervision.

Gendered: specific to an individual and informed by their sex and gender.

Goal: the object of a person's ambition or effort; an aim or desired result.

Hard Skills: specific, teachable abilities that may be required in a given context, such as a job.

Hostile Environment Training: one of several types of training that comes predominantly from a military approach and terminology for personal security training for severe security risk situations survival and hard technical avoidance.

Knowledge: facts, information and skills acquired through experience or education; the theoretical or practical understanding of a subject.

Learning: the acquisition of knowledge or skills through study, experience, or being taught.

Topics: each of a set of standardized parts or independent units that can be used to construct a more complex structure.

Module: set of independent units of study or training that can be combined in a number of ways to form an educational course.

Monitoring: observe and check the progress or quality of (something) over a period of time; keep under systematic review; maintain regular surveillance.

Objective: thing aimed at or sought; a goal.

Operational: of, or relating to, the routine functioning and activities of a business or organization.

Performance: the action or process of performing a task or function; a task or operation seen in terms of how successfully it is performed.

Safety: a freedom from risk or harm as a result of unintentional acts (accidents, natural phenomenon or illness).

Security: a freedom from risk or harm resulting from violence or other intentional acts.

Sessions: [*often with modifier*] a period devoted to a particular activity.

Soft Skills: personal attributes that enable someone to interact effectively and harmoniously with other people; subjective talents people possess in a job, including good listening and speaking capabilities, pleasant manner, positive attitude, integrity and social skills.

Skills: the ability to do something well; expertise.

Strategic: relating to the identification of long-term or overall aims and interests and the means of achieving them: "strategic planning"; carefully designed or planned to serve a particular purpose or advantage.

Syllabus: an outline or a summary of the main points of a text, lecture, or course of study.

Trainer: a person who trains or teaches (a person or animal) a particular skill or type of behavior through sustained practice and instruction.

Transference: the act of transferring something or the process of being transferred: "education involves the transference of knowledge".

Personal Security: building deeper awareness and abilities for individuals to better assess and guide their prevention and response strategies depending on the fluidity of possible security scenarios in violent and complex security risk environments.

ANNEX 2: REFERENCES

Barry, Jane. *Integrated Security: The Manual*. Kvinna till Kvinna, 2011.

Bickley, Shaun. *Safety First: A Field Security Handbook for NGO Staff*. Save the Children UK, second revised edition, 2010.

Bouchet-Sauliner, Francoise. *The Practical Guide to Humanitarian Law*. Medcins Sans Frontieres, 2002.

"Can You Get Sued? Legal Liability of International Humanitarian Aid Agencies Towards Their Staff," Security Management Initiative, 2011.

Chong, Yin Wei "A Study on Factors Predicting Post-Traumatic Stress Disorder Amongst Humanitarian Workers," 2012. (research paper available online)

"Critical Incident Protocol: Your Guide to Managing Critical Incidents," CARE USA, 2009.

Donini, Antonio, Larry Minear, Iam Smillie, Ted van Baarda and Anthony C. Welsh. "Mapping the Security Environment: Understanding the Perceptions of Local Communities, Peace Support Operations and Assistance Agencies," Feinstein International Famine Center, 2005.

ECHO Security Review, 2004, Generic Security Guide; Security Training Directory; Security Report.

"ECHO Security Training Manual: Trainers' Guide,"European Community Humanitarian Office,2006

Egeland, Jan, Adele Harmer and Abby Stoddard. "To Stay and Deliver: Good Practice for Humanitarians in Complex Security Environments," Office for the Coordination of Humanitarian Affairs, 2011.

Eguren, Enrique. *Protection Manual for Human Rights' Defenders*. Peace Brigades International and Front Line Defenders,2005

Fast, L., Finucane, C.. Freeman, F., O'Neill, M., and E. Rowley. "The Acceptance Toolkit," Save the Children Federation, Inc., 2011.

Fast, L., Rowley, E., O'Neill, M. and F. Freeman. "The Promise of Acceptance," Save the Children Federation, Inc., 2002.

Finucane, Christopher. "Humanitarian Safety and Security: Obligations and Responsibilities Towards Local Implementing Partners,"
Church World Service Afghanistan/Pakistan,2011.

"First Aid in Armed Conflict and Other Situations of Violence,"
International Committee of the Red Cross,2006.

Gent, Mike. "Weighing Up the Risks in Aid Work," *Humanitarian Exchange Magazine*, issue 21, July 2002.

"Good Practice Review: Operational Security Management in Violent Environments," (2010 Edition). Humanitarian Practice Network, Overseas Development Institute, 2010.

Griffoli-Mancini, Deborah and Andre Picot. *Humanitarian Negotiation: A Handbook for Securing Access, Assistance and Protection for Civilians in Armed Conflict*. Geneva: Centre for Humanitarian Dialogue, 2004.

"Guard Management and Training for NGOs in Afghanistan,"
RedR/ANSO Regional Security Learning Initiative,
2005.

"Guide to preparing a Learning and Development Strategy," Civil Service Training and Development Centre, 2011.

"Humanitarian Action and Armed Conflict: Coping with Stress," International Committee of the Red Cross, 2001.

InterAction Security Modules. 1998.

"Personal Security: Staying Safe in the Field - World Vision's Guide to Personal Security," World Vision International, 2012.

Roberts, David Lloyd. *Staying Alive: Safety and Security Guidelines for Humanitarian Volunteers in Conflict Areas.* International Committee of the Red Cross, 1999 (revised in 2005).

"Report of the Working Group on NGO Security Training Curriculum," NGO Security Working Group, 1997.

"Save the Children Global Safety and Security Learning and Development Strategy." Department of Global Safety and Security, Save the Children International, 2012.

"Stay Safe: The International Federation's Guide to a Safer Mission," International Federation of Red Cross and Red Crescent Societies, 2007.

"Stay Safe: The International Federation's Guide for Security Managers," International Federation of Red Cross and Red Crescent Societies, 2007.

"Security Collaboration: Best Practice Guide," InterAction, 2009.

"Security Risk Management NGO Approach," InterAction Security Unit.

Stoddard, Abby, Harmer, Adele and Katherine Haver. "Providing Aid in Insecure Environments: Trends in Policy and Operations" (HPG Report 23), Overseas Development Institute and the Center on International Cooperation, 2006.

"UNICEF Security Report: Analysis of Security incidents in 2011 and future outlook," UNICEF 2011.

Van Brabant, Koenraad. “Good Practice Review 8: Operational Security Management in Violent Environments,” Humanitarian Practice Network, Overseas Development Institute. 2000.

Van Brabant, Koenraad. “HPG Report 9: Mainstreaming the Organisational Management of Safety and Security,” Humanitarian Policy Group, Overseas Development Institute, 2001.

Walker, Peter and Catherine Russ. “Professionalising the Humanitarian Sector,” ELRHA (Enhancing Learning & Research for Humanitarian Assistance), 2010.

“Wilderness First Aid Curriculum Guide,” Wilderness Medical Associates, 2010.

EISF Publications

“Abduction Management,” EISF,2010.

“Crisis Management of Critical Incidents,” EISF,2010.

“Engaging Private Security Providers: A Guideline for Non-governmental Organisations,” EISF,2011

“Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management,” EISF,2012

“Incident Statistics in Aid Worker Safety and Security Management,” EISF,2012

“Joint NGO Safety and Security Training,” EISF,2010.

“Managing Aid Agency Security in an Evolving World,” EISF2010.

“Risk Thresholds in Humanitarian Assistance,” EISF, 2010.

“Security Management and Capacity Development: International Agencies Working with Local Partners,” EISF,2012.

“The Cost of Security Risk Management for NGOs,” EISF, 2012.

“The Information Management Challenge: a Briefing on Information Security for Humanitarian NGOs in the Field,” EISF,2010.

Websites:

http://www.cipd.co.uk/hr-resources/factsheets/learning-talent-development-strategy.aspx