Smart Practices Review for Implementing Security Risk Management in International Development Organizations

Christie Ulicny, MACD candidate
School of Public Administration
University of Victoria
July 2017

Client:	Tom Tunney, Senior Manager, University and College Programming & Barb Hogan, Operations Manager, World University Service of Canada
Supervisor:	Dr. Kimberly Speers, Assistant Teaching Professor School of Public Administration, University of Victoria
Second Reader:	Dr. Thea Vakil, Associate Professor and Associate Director School of Public Administration, University of Victoria
Chair:	Dr. Lynne Siemens, Associate Professor and Graduate Advisor School of Public Administration, University of Victoria

Acknowledgements

I would like to thank my friends and family who have been incredibly supportive throughout the MACD program. I have been grateful for your guidance, cheerleading, and laughter, which has carried me through this process.

Thank you to Dr. Kimberly Speers for your guidance throughout the Masters Project, and to Tom Tunney and Barb Hogan at WUSC for taking on this initiative and offering integral input into the shaping of the project. Of course, thank you to the interview participants who offered their precious time to share their knowledge and help complete this research.

Executive Summary

Project Objective

The primary purpose of this project is to provide a report on effective smart practices in security risk management protocols to World University Service of Canada (WUSC), the project client, by providing recommendations that will support improvements to their security risk management plan. Secondarily, this project is intended to help build knowledge for other international development organizations seeking to improve upon or develop a security risk management plan or system. Through the assessment of both academic and grey literature, as well as the collection of information from staff at a number of international development organizations, this project summarizes common frameworks and tools, examines environmental context, shared challenges, and opportunities for the international development field.

The project aimed to answer the following questions:

Primary research question

- What are smart practices for effective security risk management in an international development organization?

Secondary research questions

- How is security risk management best resourced and managed in an international development or volunteer cooperation agency working within different regions and country contexts?
- What are common challenges to implementing security risk management plans in international development and volunteer cooperation agencies?

This project defines security risk management as coordinated activities to protect an organization, its staff, and volunteers from threats to safety, acts of violence, harm and loss (Connors, 2012, p. 305; The Charity Commission, 2013, Protect your charity's staff and beneficiaries).

Methodology and Methods

The main methodology for this project is a smart practices review of security risk management protocols, conducted through a literature and organizational document review, as well as interviews with key international development organization staff. Drawing from adaptable frameworks summarized in the literature review, as well as sector specific material, the smart practices collected create what Vesely describes as a set of exemplars that can be utilized across diverse contexts (2011, p. 99).

Primary Research Methods

Phone interviews with key informants were employed to collect information from parties in different global locations to gain insight into current practices. Semi-structured interviews of eight participants, seven from international development and volunteer cooperation organizations and one from a security network, were completed. Organizations were selected based on their significant history working in international development and security. They varied in size, reach and budget (from approximately $15 million to $380 million), which allowed for a comparison of both challenges and practices employed. The purpose of this approach was to understand whether smart practices differ based on access to resources or the increased complexity of operating in more countries with a larger staff/volunteer base.

Findings and Analysis

The findings from the literature review and the primary research conducted for this report demonstrated a great deal of convergence. The literature review provided an overview of risk management frameworks, tools, and protocols, as well as the global context in which international development organizations operate. It also discussed the environment necessary for successful security risk management as well as common challenges. The findings from the primary research reflected and complemented the literature review and in addition, offered dialogue around typical contextual and internal challenges faced by organizations operating internationally.

This provided unique perspectives from those with experience working in diverse humanitarian and international development settings. Some key findings from the primary research included: 1) the relevance of security risk philosophy and value of developing a

culture of security; 2)the need for more consistent training for all staff; 3) the importance of senior level engagement in the development of security risk policies; 4) issues of traffic accidents and sexual assault as the most commonly faced risks across global sites, and; 5) the relevance of utilizing an anti-oppressive lens to review organizational practices around security risk management.

Important themes and questions offering valuable insights for WUSCs security risk implementation plan were posed throughout the discussion and analysis section. The discussion began with a macro level analysis related to risk philosophy and culture and its relationship with the risk context. Nested within this philosophy and culture, specific approaches and practices were presented and common challenges discussed to offer key lessons that could elicit organizational analysis and awareness. The findings were utilized to create the options and recommendations presented to WUSC.

It is important to note that while this research provides an overview of smart practices and approaches considered valuable by organizations and individuals, these smart practices they do not represent a fulsome approach to security risk management for all international development organizations.

Recommendations

Four recommendations were developed to support WUSC in the implementation of their renewed security risk management plan. The following recommendations offer short, medium and long term actions that will provide direction in achieving these objectives. The recommendations are:

1. **Communicate new risk philosophy and utilize this philosophy to foster a positive, inclusive, and active security risk organizational culture and the associated implementation strategy.** This includes:
    - Creating and executing a security risk philosophy communications plan;
    - allocating messaging dissemination duties;
    - developing and reinforcing behavioural expectations around processes, and ;
    - distributing organizational charts and process flow charts.

2. **Systematize processes while maintaining responsiveness and reactivity to context and risks.** This includes:
    - Articulating security risk thresholds and their relationship with protocols;
    - developing and communicating systems and schedules for security risk management processes;
    - assessing policies;
    - ensuring data management system is effective;
    - integrating systematic processes into practice, and;
    - maintaining a contingency fund.
3. **Examine whether security risk management processes and protocols are applied equitably.** This includes:
    - Requiring staff individual vulnerability self-assessments;
    - assessing training practices;
    - determining equity of capacity building for national and international staff;
    - assessing policies – how they are applied and through what lens;
    - determine best way to provide training and developing a baseline for global briefing and training policies.
4. **Develop a coordinated resource allocation and fundraising approach for programs.** This includes:
    - Using risk level and context to inform project selection, funding requirements, contingency fund allocation and proposal inclusions;
    - determine need for regional or local security advisors, and;
    - determine the type of training required for each location.

Table of Contents

Conceptualization of Terms

This section provides definitions of important terms used throughout the report.

Danger habituation – unconscious adjustment to a higher risk threshold due to consistent exposure to threats (HPN, 2010, p. 113).

Disaster – an event that causes widespread loss that is beyond the capacity of a community to cope using its own resources (United Nations Environment Programme, 2011, p. 6).

Duty of Care – a legal and ethical obligation for organizations (and individuals) to provide a reasonable level of protection and care for all those involved with an organization (Volunteer Canada, 2012, p. 12).

Due Diligence – to act reasonably and in good faith regarding the interests of an organization and those who interact with it (Volunteer Canada, 2012, p. 60).

Liability – the duties and responsibilities of an individual or organization as outlined by law (Volunteer Canada, 2012, p. 60).

Mitigation – actions taken to reduce a threat, exposure to a threat, and/or impact if a threat is encountered (HPN, 2010, p. 28).

Negligence – when an individual "is harmed as a result of the action or inaction of another person (organization)" (Volunteer Canada, 2012, p. 13).

Risk – vulnerability to threats and the potential impact of encountering a threat (HPN, 2010, p. 28).

Risk Management – a systematic approach to addressing uncertainty through the identification, assessment, mitigation and communication of risks (Berg, 2010, p. 81).

Risk Threshold – "the point beyond which the risk is considered too high to continue operating; influenced by the probability that an incident will occur, and the seriousness of the impact if it occurs" (HPN, 2010, xix).

Security Focal Point – in-country staff who are given security risk management duties along with their regular role (often managers or coordinators) (HPN, 2010, p. 11).

Security Risk Philosophy – a verbalized or written strategy that articulates a statement of accountability and outlines the risk tolerance of an organization in relation to its mandate (Desilets, 2016, p. 12).

Security Risk Management – coordinated activities to protect an organization, its staff and volunteers from threats to safety, acts of violence, harm and loss (Connors, 2012, p. 305; The Charity Commission, 2013, Protect your charity's staff and beneficiaries).

Threat – any factor that could cause harm, loss, or damage (HPN, 2010, p. 28; InterAction Security Unit, n.d., p. 6).

Vulnerability – the likelihood of encountering a threat and the impact of encountering that threat (HPN, 2010, p. 28).

1.0 Introduction

The purpose of this report is to provide information on smart practices in security risk management to WUSC, to help them improve their security risk management system. This report is also intended to help build knowledge on the topic in the field of international development. This chapter will outline the background of risk management and give an overview of WUSC and the challenges faced by the organization in relation to security risk management. Additionally, it will outline the project objectives, the layout of the report and provide key terms utilized throughout the report.

1.1 Background and Problem Definition

Security risk management for international development organizations is complex. Work completed by organizations operating in marginalized communities with vulnerable populations can carry with it unavoidable risks (Ministry of Citizenship and Immigration, 2009, p. 4). For international development organizations, managing risks is integral for the safety and security of staff, volunteers, and local community partners, as well as for satisfying their moral, legal, and ethical responsibilities to all stakeholders (Griffin, 2013, p 11; Humanitarian Practice Network, 2010, p. 7). By following smart practices in risk management, an organization can demonstrate due diligence and also protect their intangible assets such as reputation, staff/volunteer experience, global partnerships and community impact (Agard, 2011, p. 9; The Charity Commission, 2011, p. 1; HPN, 2010, p. 7).

The sector has faced a number of challenges catalyzing an interest in creating more robust security management systems for international development organizations. According to the Ontario Ministry of Citizenship and Immigration (2010, p. 4), interest in risk management in the non-profit sector has been growing in recent years due to a range of factors including high profile lawsuits and associated organizational costs. With increasing concern for evolving economic, environmental, health, safety, geopolitical, and technological risks, addressing the complex issue of managing security risks has become a priority for many international development organizations (Humanitarian Outcomes, n.d., p. 1; Neuman & Weissman, n.d., para. 3; T. Tunney, Personal Communication, July 29, 2016; World Economic Forum, 2016, p. 6-7). According to the Humanitarian Practices Network (HPN) (2010, p. 1) these contextual

issues have “generated a deeper awareness of the security challenges faced by operational agencies” and led many international development organizations to reconfigure, reinforce and adapt their strategies for security risk management and interagency collaboration.

Significant security related events have created a sense of urgency for many organizations to improve their current security risk management systems. World University Service of Canada (WUSC), a Canadian international development organization operating in 25 countries globally, has been working to strengthen their security risk management practices (T. Tunney, Personal Communication, October 26, 2016). In 2015, a terrorist attack on a hotel in Burkina Faso that resulted in the tragic death of six Canadians, catalyzed the review of safety and security protocols within a number of international development organizations, including WUSC (CBC News, 2016; Desilets, 2016, p. 4; T. Tunney, Personal Communication, October 26, 2016). Recently, WUSC hired a consultant to undertake an audit of their security management practices (Desilets, 2016, p. 4). The audit exposed some gaps in WUSC’s security management practices, which the organization is now responding to by developing a more robust implementation plan based on the recommendations they received (Desilets, 2016, p. 4). The following report will provide WUSC with smart practices in security risk management to help inform their new plan.

1.2 Project Client

World University Service of Canada (WUSC) is a Canadian international development organization dedicated to building a more equitable world (WUSC, 2015). The organization operates in 25 countries and employs over 300 staff (Desilets, 2016, p. 4; T. Tunney, Personal Communication, January 2017). Their vision is “to create a world where all young people can grow up in safe, secure and supportive environments, where they can learn, work and play a vital role in their country’s development” (WUSC, 2015, Our Vision). WUSC’s focus is in a number of areas including education, health, gender equality, livelihoods and supporting youth (WUSC, 2015, Our Work).

A component of WUSC’s work includes partnership with Centre for International Studies and Cooperation (CECI) to implement the Uniterra program, a program funded by Global Affairs Canada that places approximately 600 volunteers (85% Canadian) each year in 14

countries around the world to contribute their time and skills to support lasting change (B. Hogan, Personal Communication, May 29, 2017; Uniterra, 2016, About Us, para. 1). The program is focused on mobilizing volunteers and international partnerships to increase inclusive economic opportunities and empowerment for women and youth (Uniterra, 2016, Towards a More Equitable World section, para. 1). This program is a great collaborative opportunity that demonstrates the value of sharing efforts and resources. It also adds a layer of complexity to the work that is done by WUSC as they work collaboratively with CECI to implement programming that aligns with both organization's policies and procedures in diverse international contexts.

Tom Tunney, Senior Manager, University and College Programming and Barb Hogan, Operations Manager at WUSC, are the project client contacts for this research report.

1.3 Project Objectives and Research Questions

The primary objective of this project is to provide a report on effective smart practices in security risk management protocols to WUSC, the project client, by providing recommendations that will support their development of a new security risk management implementation plan to build upon their current practices. Secondarily, this project will help to build knowledge in the field for other international development agencies seeking to improve upon or develop a security risk management plan or system. Through the assessment of both academic and grey literature, as well as the collection of information from international development agency staff, this project summarizes common frameworks and tools, examines context, shared challenges, as well as opportunities for the international development field. This is important work because strong risk and security management protocols within an organization are credited with increasing accountability, protecting assets, ensuring legal compliance as well as creating "maximum benefit and minimum harm, and…increas[ing] opportunities for effective and innovative work" (Gaskin, n.d., p. 4).

Collecting insights from eight staff members at international development and volunteer cooperation agencies as well as one security network; undertaking a review of risk management plans, frameworks and tools, as well as completing a literature review has informed recommendations for WUSC's security risk management practices.

The primary research question explored was:

- What are smart practices for effective security risk management in an international development organization?

The secondary questions explored were:

- How is security risk management best resourced and managed in an international development or volunteer cooperation agency working within different regions and country contexts?
- What are common challenges to implementing security risk management plans in international development and volunteer cooperation agencies?

In this report, effective is defined as practices that have been tested and proven successful in achieving their task.

1.4 Organization of Report

This reports aim is to explore smart practices in security risk management for international development organizations. The literature review begins with an overview of risk management approaches, frameworks, and an explanation of duty of care to clarify the overarching system that lays the foundation for security risk management. This is followed by commonly used risk management tools and protocols, as well as resource allocation strategies for security risk management, to provide an overview of practical information for implementation. An overview of common global risks examining the general context in which international development organizations are operating is presented. This leads into an exploration of the parameters for creating an environment for effective security risk management implementation, as well as common challenges. These topics are explored again in the primary research findings collected through the interview of staff from eight international development agencies. The project concludes with security risk smart practices recommendations for WUSC, the project client, and other international development organizations developing or modifying their security risk management plan.

2.0 Literature Review

2.1 Overview

The following literature review was completed to gather scholarly and non-academic research on smart practices in security and risk management. This review aimed to: 1) define risk management and related frameworks from which security risk management implementation plans are built; 2) identify common tools and protocols for security risk management; 3) provide methods for creating a successful security risk management environment; and 4) discuss challenges for implementation.

This research was completed based on scholarly and grey sources. The research revealed an abundance of academic literature in the area of risk management frameworks and approaches for diverse sectors as well as grey literature related to security risk management practices in international development. A non-exhaustive search of the PAIS International, Web of Science, Political Science Abstracts, JSTOR, EBSCO, Google Scholar, and Proquest databases for scholarly sources of literature on the topic of security risk management practices and common security issues for international development agencies, provided limited resources. Further research overturned an abundance of grey literature created by diverse global organizations such as the Humanitarian Practice Network, United Nations, government bodies, and other international non-profit organizations in the area of global risk and security issues. The search terms used to identify sources were the following:

- Risk management
- Risk management frameworks
- Security management
- Security risk management for international development
- International development safety and security
- Humanitarian safety and security

2.2 Risk Management Overview

Risk management is deemed to be a logical approach to assessing systems and addressing uncertainty (Berg, 2010, p. 81; Mitchell & Harris, 2012, p. 2-3). It is built on a set of principles and guidelines to address complex issues within diverse contexts (ISO, 2009, p. v; Lalonde & Boiral, 2012, p. 282; The Association of Insurance and Risk Managers, Alarm & The Institute of Risk Management, n.d., p. 3). This section of the literature review provides an overview of the research conducted on risk management, the legal responsibility of organizations, and introduces two frameworks relevant to international development.

According to various authors, risk management should be approached holistically focusing on risk assessment, mitigation, monitoring, communication, and resource allocation (Berg, 2010, p. 79 & 81; ISO, 2009, p. 10; The Association of Insurance and Risk Managers et al., n.d., p. 3). Researchers and experts in the field state that risks must be assessed for both probability and severity of impact, which informs an organization of the level of risk associated with undertaking activities to achieve its objectives (Berg, 2010, p. 79; The Association of Insurance and Risk Managers et al., n.d., p. 2). As stated frequently in the literature, risk management should be dynamic and responsive to changing threats and contexts (Lalonde & Boiral, 2012, p. 277; The Association of Insurance and Risk Managers et al., n.d., p. 3). When effectively implemented and sustained, risk management is touted for improving governance, stakeholder relations, organizational resilience, the achievement of organizational objectives, and increasing alignment with regulatory requirements (ISO, 2009, p. v).

2.2.1 Legal 'Duty of Care'

Duty of care is defined as the legal and ethical obligation that organizations have to provide a reasonable level of protection and care for all those involved with an organization in order to avoid negligence (Volunteer Canada, 2012, p. 12). According to Volunteer Canada, organizations can be deemed liable when an individual "is harmed as a result of the action or inaction of another person (organization)" (2012, p. 13). They further state that duty of care is relative and measured against the actions a prudent person/organization would have undertaken in a similar circumstance (Volunteer Canada, 2012, p. 13). Standards are even higher if clients/staff are part of a vulnerable population (i.e. children, the elderly, people with disabilities) (Volunteer Canada, 2012, p. 11). A number of charitable governance organizations state that

managing risk is an important means for an organization to perform their due diligence (The Charity Commission, 2011, p. 1; Volunteer Canada, 2012, p. 12). It helps organizations protect their 'intangible assets', such as reputation, client experience, global partnerships and community impact (Agard, 2011, p. 9 & 10; The Charity Commission, 2010, Annex 2).

2.2.2 Risk Management Frameworks

Although there are a number of risk management frameworks, two were frequently referred to in international development organization risk management planning documents. The first, developed in 2004, is Enterprise Risk Management (ERM) and the second developed in 2009, is ISO 31000 (Lalonde & Boiral, 2012, p. 272; Norwegian Refugee Council, 2015, p. 16). ERM outlines a process built on the premise that organizations exist to create value for their stakeholders and thus must focus on the relative impact of risks on organizational objectives (Committee of Sponsoring Organizations of the Treadway Commission, 2004, p. 3; Norwegian Refugee Council, 2015, p. 16). ISO 31000 was developed as a generic logic-based universal risk management framework designed to help organizations in any sector integrate risk management into their operations (Berg, 2010, p. 80; Lalonde & Boiral, 2012, p. 272 & 274). Both offer guidelines for enhancing organizational performance, safety and controls (ISO, 2009, p. vi). This project refers to the ISO 31000 framework as well as other tools and systems developed specifically for, or by, international development organizations.

ISO 31000 Overview

As an international standard, ISO 31000 (2009, p. vii) offers generic principles, a process overview, and framework for effective risk management. Although it provides guidelines, it was not created as a prescriptive system framework but rather one adaptable to diverse settings and needs (ISO, 2009, p. 9). Figure 1 presents each of the ISO 31000 components and demonstrates how these principles and processes fit together within the framework.

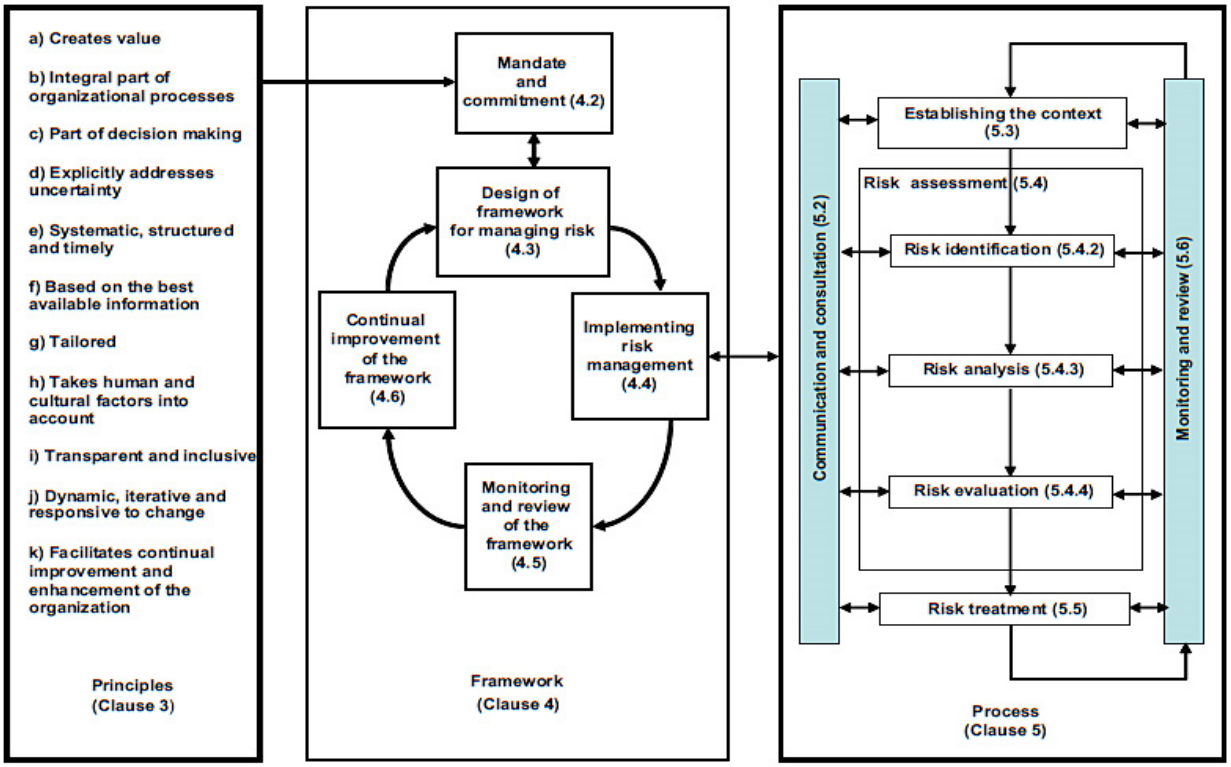


Figure 1 – ISO risk management principles, framework and process (2009, p. vii).

According to ISO (2009, p. 7), the principles listed in Figure 1 are the foundation for an organizational risk management commitment, policy, and culture. The framework is in place to guide decision-making, governance activities, and organizational accountability around risks (ISO, 2009, p. 8). The process offers a flow chart on actions that must be undertaken such as: establishing context, identifying and analyzing risk, defining mitigation measures, monitoring the process and communicating with stakeholders (Berg, 2010, p. 80 & 81; ISO, 2009, p. 14). As mentioned, this generic system has been created to adapt to any sector and to create continuity across borders by standardizing language and process (ISO, 2009, p. 9). Although, according to Leitch (2010, p. 888), the terminology in ISO 31000 is not well defined which can create confusion in the application of the framework.

Humanitarian Practice Network - Good Practice Review 8 Overview

In 2000, a sector specific security risk management framework was created for international development by the Humanitarian Practice Network (HPN) – a forum for those working in the humanitarian sector to share knowledge and smart practice (HPN, 2010, ix & p. 9; HPN, 2017, About HPN). This framework (Figure 2) has been developed as part of a good

practice review by a collaborative team of experts in the field of operational security and revised multiple times since its inception (HPN, 2010, p. ix). It provides practical steps, with aligning questions that organizations can complete/ask to assess operational feasibility of implementing or operating programs in a given location (HPN, 2010, p. 8 & p. 9). It also acknowledges the challenges and dilemmas faced in international development related to the risks and rewards inherent in such work (HPN, 2010, p. 8 & p. 9).

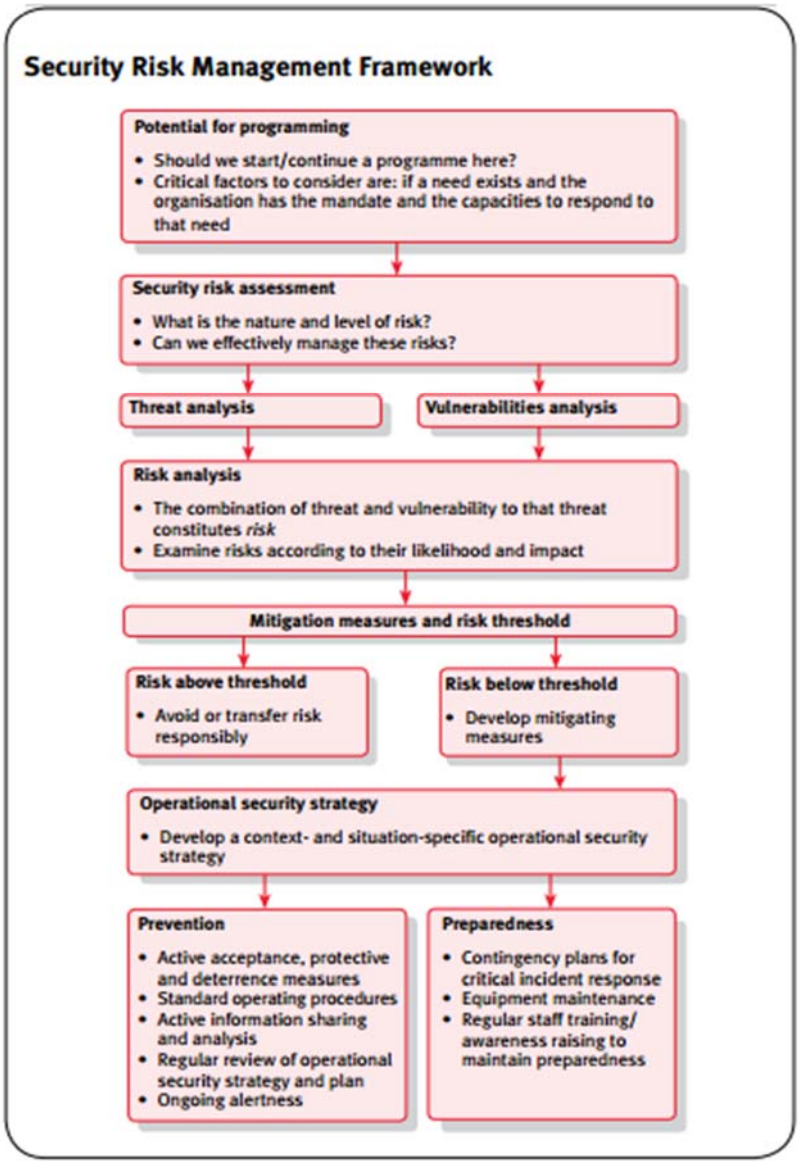


Figure 2 – HPN's (2010, p. 9) Security Risk Management Framework.

Many steps in HPN's framework include processes to guide organizations in risk management implementation. The framework aligns with ISO 31000 in requiring risk

assessment, analysis, mitigation, and review for the relevant context (HPN, 2010, p 8). HPN (2010, p 8) also recommends an organizational capacity review to determine capabilities to manage risk. It states that an organization should decide on an acceptable risk threshold and a set of guiding questions based on organizational mandate as well as the benefit or detriment of operating or removing a program in any given community (HPN, 2010, p. 8).

In order to be well prepared for risks, HPN states that there must be "ongoing assessment of security conditions to determine whether the security strategy remains appropriate to the threats in that environment, and whether the risks remain acceptable" (2010, p. 10). According to HPN (2010, p. 8), for risks below an organization's defined threshold, a "situation-specific" strategy should be developed. In the case of risks that exceed the threshold, HPN (2010, p. 8) recommends not starting, stopping, or transferring the risk of programming to another organization. The transfer of risk can prove controversial as it can create greater risk for a local/partner agency and their staff (HPN, 2010, p. 96). HPN states that there can be cultural or economic reasons why an organization would take on transferred and often greater risk (HPN, 2010, p. 22). HPN (2010, p. 22) recommends joint risk assessment and capacity assessment of the partner agency, which may be difficult in emergency situations.

HPN (2010, p. 8-10) posits that effective security risk management requires both prevention and the capacity to manage crisis and the aftermath of incidents. They state that procedures must include both mitigation measures and critical incident response including policies to guide post-incident practices (i.e. immediate and longer-term survivor support, evacuation etc.) and review (HPN, 2010, p. 9). Review of practices are cited as essential for both ISO and HPN's frameworks, as they ensure organizational effectiveness and efficiency in risk management and encourage learning from events, identifying trends and emerging risks (ISO, 2009, p. 20).

2.3 Risk Management Tools and Protocols

This section of the chapter provides a collection of commonly used risk management protocols and tools outlining the major steps to implementing risk management processes as found in the literature.

2.3.1 Assessing External Risk Context

According to the ISO (2009, p. 15), the context and parameters in which risk management will be implemented should be established when designing a risk management system. HPN agrees, stating that "a solid understanding of the local environment and of the role – both actual and perceived – that aid agencies play in it" is necessary (2010, p. 30). Understanding contextual knowledge is an ongoing process as the context is always evolving (HPN, 2010, p. 30). A PESTLE analysis (appendix 1) is a common framework used for assessing external risk factors when working internationally (The Charity Commission, 2011, Tool 3: Risk Management).

PESTLE is an acronym for political, economic, social, technological, legal and environmental factors that influence risk (Law, 2016, PESTLE Analysis). Assessing and charting the risks existing in each new community an organization operates in, can help to clarify the political stability, country infrastructure, cultural practices, health and safety issues, human rights concerns, technological limitations and environmental hazards that will require navigation (The Charity Commission, 2011, Tool 3: Risk Management). Gaining a holistic picture of the environment in which these programs will be undertaken is integral to safe and effective operations (The Charity Commission, 2013, Pestle analysis: compliance toolkit link). As these risks are outside of the control of the agency, they must be monitored regularly to ensure responsiveness (The Charity Commission, 2011, Tool 5: Risk Management, p. 3).

The Community Toolbox (2016, section 5) recommends contacting local agencies, NGOs, and embassies, as well as speaking to local people, undertaking media analysis, reviewing legislation, police records and international reports to gain insights into context. HPN (2010, p. 30) also recommends including research of the history of the country and its political legacies, transnational relationships, government-community relations, identity groups, religious, social and political ideologies, social structures and social norms. According to HPN,

good context analysis includes assessing social divisions where issues may not yet be visible but may arise, as well as how the organization completing the risk assessment is perceived in its operating environment (HPN, 2010, p. 30-31).

2.3.2 Assessing Internal Risk Context

Berg (2010, p. 82) states that understanding the internal risk context requires a review of organizational objectives, policies, strategic plans, stakeholder interests, as well as operational constraints and opportunities. The organizational culture and messaging about risk and security must also be reviewed (Berg, 2010, p. 82). Berg (2010, p. 83) posits that developing risk criteria while reviewing internal context can help align the risk management process with organizational ideologies. Undertaking site specific program analysis, including interviews with staff and activity observation to understand the goals, resources, and capacity of both the local site and overall organization, helps to create further cohesion (European Commission, 2004, p. 66; HPN, 2010, p. 29).

2.3.3 Security Risk Assessment and Analysis

According to the HPN (2010, p 27), a security risk assessment allows an organization to perform a risk-benefit analysis to justify the start-up of a new program or the continued operation of a current program. Various field experts agree that risk assessments need to be revisited with changes to the external environment or with programmatic changes (HPN, 2010, p. 27; Interaction Security Unit, n.d., p. 8). This allows an organization to systematically review the threats in an environment, vulnerabilities that may exist for them, and consider whether the current mitigation measures in place will be sufficient to reduce the threat or vulnerability (HPN, 2010, p. 37-38). According to Berg (2010, p. 84), an organization should identify the potential impact of a risk by clarifying why an event is a risk, what will happen if the risk occurs, as well as what effect this will have on organizational objectives and program outcomes. A risk assessment cycle (Figure 5) demonstrates the constant iterative process of risk assessment and provides rules for organizations to follow (The Charity Commission, 2011, p. 1).

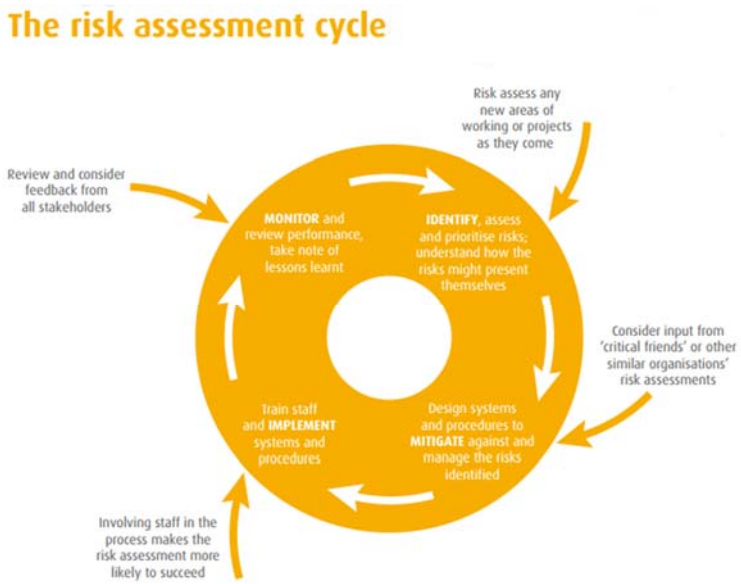


Figure 3 – Risk Assessment Cycle (The Charity Commission, 2011, p. 1).

Both the field experts and academics recommend scenario planning, process mapping, reviewing relevant audit reports, policies, program evaluations, and research reports to collect both internal and external risk information (Berg, 2010, p. 84; HPN, 2010, p. 15; Interaction Security Unit, n.d., p. 13-14). For human imposed threats field experts also note an organization should gain an understanding of the "history, intention and capabilities" of a threat occurring and the threat agent's ability to undertake such an attack (HPN, 2010, p. 40; Interaction Security Unit, n.d., p. 14). For more global risks such as environmental or health based threats, monitoring of global alert systems is essential for preparedness (Stanganelli, 2008, p. 93). The inclusion of diverse and knowledgeable staff in the assessment process also impacts organizational preparedness through the collection of essential information (Berg, 2010, p. 84).

2.3.4 Risk Register and Risk Matrix

Once collected, identified risks can be inserted into a risk register (appendix 2) and analyzed. A risk register is a tool that acts as a repository for risks (Humanitarian Outcomes, n.d., Tools). It outlines the type of risk, severity, mitigation measures, and those responsible for the risk (Humanitarian Outcomes, n.d., Tools). A customizable risk register template is offered on the Humanitarian Outcomes (n.d.) website in their tools section. It prompts organizations to develop customized risk impact criteria and ratings, as well as provides a risk matrix analysis

table (appendix 4) which colour codes the significance of rated risks (Humanitarian Outcomes, n.d., Tools). A checklist for developing a risk register is included in appendix 3.

A risk matrix analysis table can help an organization define which risks fall within their risk threshold. Berg (2010, p 86) states that acceptable levels of risk include: 1) a low level of risk that does not require mitigation; 2) a risk that cannot be mitigated and must be accepted or avoided, and; 3) benefits/objectives that outweigh the level of threat. Program criticality, sustainability, as well as risk to the safety and security of staff and volunteers must be considered in this process (InterAction Security Unit, n.d., p. 8). InterAction Security Unit (n.d., p. 9) provides the following guiding questions:

1) Is the program so significant that the NGO would be willing to accept high or very high risk to staff/volunteer lives?
2) Have all alternative options for achieving program objectives been explored?
3) Have all actions to reduce current risk levels to medium or lower been taken?
4) Can the residual risk be managed with the current system?

According to InterAction Security Unit (n.d., p. 9), senior management must be able to answer "yes" to all of these questions to safely go ahead with programming.

A risk matrix analysis table provides an overview of the level of severity of risk based on a cross-section of the likelihood and impact. An organization is responsible for defining the impact of each risk or event. The United Nations security risk impact matrix example has been included in appendix 5.

2.3.5 Organizational Process for Security Risk Assessment and Analysis

According to InterAction Security Unit (n.d., p. 9) a security risk assessment should be developed by the Security Focal Point with the in-country team, which is then reviewed by the security management team and regional director who provide feedback and adjustments. HPN clarifies that although "many organizations devolve decision-making authority [to in-country staff, the] ultimate responsibility…lies with the Executive Director, or in some cases the Board of Trustees" (2010, p. 11). Higher levels of approval should be required for significant decisions such as downgrading risk ratings of a country or the use of armed guards for protection (HPN, 2010, p. 11).

2.3.6 Risk Mitigation Measures

Once analyzed and an acceptable risk threshold defined, an organization can decide how they will approach these risks. InterAction Security Unit (n.d., p. 20), points out that mitigation measures should focus on factors that can be controlled by the organization - program elements or organizational vulnerabilities. Both academic and field experts posit that organizations can approach risk by: 1) reducing its likelihood by working to avoid triggering risk; 2) reducing threat impact through strategic procedures; 3) reducing exposure through avoidance or risk transfer to another agency, and; 4) accepting the risk as it is (Berg, 2010, p. 86; HPN, 2010, p. 50; InterAction Security Unit, n.d., p. 21). Berg (2010, p. 86) cautions that accepting risk requires a significant amount of resources. InterAction Security Unit (n.d., p. 20) states that the successfully implementation of mitigation measures to reduce a risk to an acceptable level for an organization should be the goal.

Each organization is responsible for creating guidelines for how to treat risks with varying levels of severity, based on their mandate and risk philosophies (United Nations Somalia, n.d., p. 21). Figure 4 provides the United Nations Somalia's (n.d., p. 21) example of internal risk treatment and review processes based on risk level categories.

Risk Level	Treatment Guidelines	Escalation And Retention Guidelines
Extreme	Immediate action required to actively manage risk and limit exposure	Escalate to the Board, risks generally not accepted or retained
High	Cost/benefit analysis required to assess extent to which risk should be treated - monitor to ensure risk does not adversely change over time	Escalate to Head of Agency, risks generally not accepted or retained
Medium	Constant/regular monitoring required to ensure risk exposure is managed effectively, disruptions minimised and outcomes monitored	Escalate to relevant senior officer or senior management level, specify risk management actions, risks may generally be retained and managed at operational level
Low	Effectively manage through routine procedures and appropriate internal controls	Monitor and manage at the relevant officer, or operational level, risks generally retained

Figure 4 - Escalation and Retention Guidelines (United Nations Somalia, n.d., p. 21).

2.3.7 Risk Management Monitoring

As an iterative process, risks, policy, assessment criteria, mitigation measures and implementation processes should be monitored annually to ensure the risk management system is

effective and continues to align with organizational objectives and context (United Nations Somalia, n.d., p. 26; HPN, 2010, p. 40). Berg explains the importance of developing "benchmarks for success or warning signs for failure" in this process (2010, p. 81). United Nations Somalia (n.d., p. 26) recommends reviewing risks and mitigation plans monthly and reporting on the risk register and mitigation plans at monthly or quarterly Board meetings. They also provide a reminder that both the process and framework can be adapted as changes occur and gaps are found, so improvements can be made (United Nations Somalia, n.d., p. 27).

2.4 Organizational Resource Allocation for Risk Management

According to Project Management Institute (2013, p. 95), resource prioritization is essential for the effective use of limited resources across a program or organization. This section provides a brief explanation of how decisions are made regarding resource allocation in the risk management process. This helps to ensure ample resources are in place for effective system implementation and incident preparedness.

Mitchell & Harris (2012, p. 4) recommend utilizing risk assessment information and forecasts for risk, organizational capacity, cost-benefit analysis, and cultural acceptance of risk as guiding factors for resource allocation. The Project Management Institute (2013, p. 97) posits that activities to manage risks should be proportionate to the level of risk and a program's significance to the organization. When outlining mitigation measures, the resources required for these measures should be defined and agreed upon (Project Management Institute, 2013, p. 97). Contingency or unrestricted funds are a common mitigation measure that allows an organization to adapt to new contexts and to address the impact of risk events (Watt, 2014 Contingency Plan) According to Watt (2014, Contingency Plan) contingency budgets are also proportionate to the level of risk and are often managed at the project level to allow for urgent access.

Staffing

According to HPN (2010, p. 11), global security advisers who oversee all security programs are increasingly becoming common in international development. For high-risk areas, regional security advisors may be appropriate as they can provide more concentrated support for in-country projects (HPN, 2010, p. 11). For many organizations the country director is responsible for adherence to risk management procedures in international settings, however a

security advisor or security focal point (often a manager or coordinator with additional duties) may be delegated some of these responsibilities (HPN, 2010, p. 11). Organizations are advised to utilize the location's risk rating, the workload associated with mitigation requirements, along with financial feasibility to take appropriate staffing measures (HPN, 2010, p. 11).

2.5 Global Security Risks in International Development

The state of the global risk landscape is ever changing, which impacts the approach and objectives of international development organizations. The following section provides an overview of global risks and therefore, the context in which international development organizations are operating. Although risks can be classified a number of ways, for the purpose of this paper, this section will outline the following security risk categories: geopolitical, health, safety, and environmental. It is important to note that risks do not operate in insolation and can interact with and impact one another, increasing the complexity of working in these environments (Stoddard, Haver & Czwarno, 2016, p. 8).

According to studies completed by the World Economic Forum (WEF) (2016, p. 11 & p. 88), ten years ago the most significant global risks in terms of likelihood and impact were economic. WEF's (2016, p. 11) research from 2016 highlights environmental and conflict based risks as the most significant at present. This aligns with organizational rhetoric about changes in the security environment (HPN, 2010, p. 1). HPN (2010, p. 1) cites violence as increasing against aid workers, they mention kidnappings, criminality and more lethal and politically motivated attacks as concerns for international development organizations. Figure 5 provides an overview of changes in the likelihood and impact of global risks as defined by experts in the field through a research study completed by the WEF (2016, p. 11) from 2007- 2016.

Source: World Economic Forum 2007–2016, *Global Risks Reports*.

Figure 5 – Global Risk Landscape (World Economic Forum, 2016, p. 11).

2.5.1 Geopolitical Risks

Stoddard, Harmer, Haver, Taylor, and Harvey (2015, p. 32) highlight conflict as a root cause for the increase in aid required globally. They state that "chronic complex emergencies – characterized by long-standing conflicts, weak governance and severe poverty – create conditions where people need outside help to meet their most basic needs year after year, with no foreseeable 'normal' to get back to" (Stoddard et al., 2015, p. 33). This scenario draws support from international development organizations into regions with diverse challenges. From a security risk perspective, this type of political instability often removes the rule of law and the protection of civilians, including non-profit staff (Gaul et al., 2006, p. 8). According to Gaul et al. (2006, p. 9) research shows that 90% of fatalities in modern wars are civilians, contrasting with historic wars such as WWII where most casualties were soldiers. Additionally, in conflict,

aid organizations are often targets for attacks, as these acts create terror with little risk for retaliation (Gaul et al., 2006, p. 9).

In 2015, 287 aid workers were victims of violent attacks (Humanitarian Outcomes, 2016, Figures at a glance). Of those 287 victims, 109 were killed, 110 were wounded and 79 were kidnapped - with 68 surviving these events (Humanitarian Outcomes, 2016, Figures at a glance). These victim rates represent 148 incidents as reported from 25 countries (Humanitarian Outcomes, 2016, Figures at a glance). Although this is a reduction in both attacks and victims from the previous year, historical data demonstrates that 10 years ago, the total number of incidents (74) was 50% less than of the number of attacks that occurred in 2015 (Humanitarian Outcomes, 2014, p. 1). Stoddard et al. (2016, p. 9 & 10) attribute the increase in incidents to a small number of highly violent areas experiencing conflict such as Syria, Afghanistan, Somalia, South Sudan, Yemen, and the Central African Republic.

This aligns with research from the Institute for Economics and Peace (IEP) (2014, p. 43), who found that from 2007 to 2014 global peace has deteriorated with violent demonstrations, increasing homicide rates, perceptions of criminality and terrorism as the most significant causes. They highlight terrorist activity as a main driver of this increase, citing the number of deaths from terrorism as having increased from 3,800 in 2002 to approximately 17,800 in 2013 (Institute for Economics and Peace, 2014, p. 42). They also note that terrorism has become active in 59 countries, an increase from 28 countries affected in 2002. Since 2007, homicide rates have also increased in low income regions, notably Sub-Saharan Africa, Latin America and Southern Asia for a number of contextual reasons (IEP, 2014, p. 42). IEP explains that while better methods of data collection locally could contribute to this increase, “rural to urban migration, the role of international criminal networks, and the ongoing legacy of political violence” are also key factors (2014, p. 42).

According to De Cordier (2009, p. 664), the politicization of development work increases security challenges. Many international development organizations are Western aligned, which often injects Western political values and agendas into areas where aid is focused and influences how it is distributed (De Cordier, 2009, p. 664). Additionally, military groups take on humanitarian projects in different regions which removes the neutrality that is the goal of aid work (Gaul et al., 2006, p. 9; HPN, 2010, p. 30). De Cordier (2009, p. 667) points out that

development organizations often spread values and norms that may contrast or be incompatible with local custom. This can "fuel negative perceptions and misperceptions" creating polarization and increasing the likelihood of an organization becoming a target (De Cordier, 2009, p. 667).

2.5.2 Health Risks

According to the World Health Organization (WHO), (2015, as cited in World Economic Forum, 2016, p. 59) the resurgence of endemic infectious diseases continues to be a global issue. Cases such as the Ebola crisis, SARS, and Zika demonstrate how the movement of people and animals across countries increase the transmission of infectious diseases (World Health Organization, 2015, as cited in World Economic Forum, 2016, p. 59). WHO (2017, Global infectious disease surveillance) cites plague, cholera and yellow fever as diseases of international importance while The Global Fund (2016, The opportunity, para. 2) acknowledges tuberculosis, HIV, and malaria as accounting for one third of the global disease burden.

As organizations who move personnel throughout global regions, international development agencies staff and volunteers are particularly affected by global health issues. The Centre for Disease Control and Prevention (2017, Humanitarian Aid Workers), posits that aid workers may be exposed to greater risk than a regular tourist due to interaction with poor sanitation, disease (depending on project and role) and high levels of stress. For locales with poor hygiene and sanitation, and where access to clean water and medical services may be low, risk to health can be a significant consideration and organizational mitigation measures will need to reflect that (WHO, 2012, p. 2).

2.5.3 Safety Risks

Although there are a number of safety risks posed to international development organizations, two common risks frequently mentioned in the literature that are addressed here are motor vehicle accidents and sexual assault.

Motor Vehicle Accidents

One of the most significant safety risks worldwide is motor vehicle related death (WHO, 2017, Top 10 causes of death). In 2015, 1.3 million people were killed by motor vehicle accidents (WHO, 2017, Top 10 causes of death). Although this is common across countries of all levels of income, low-income countries had a 10% higher rate of death from traffic accidents

(WHO, 2017, Top 10 causes of death). This is a significant consideration for international development organizations, as it tends to be a difficult risk to avoid or mitigate. Figure 6 demonstrates the WHO's regional road traffic mortality rate from 2013.

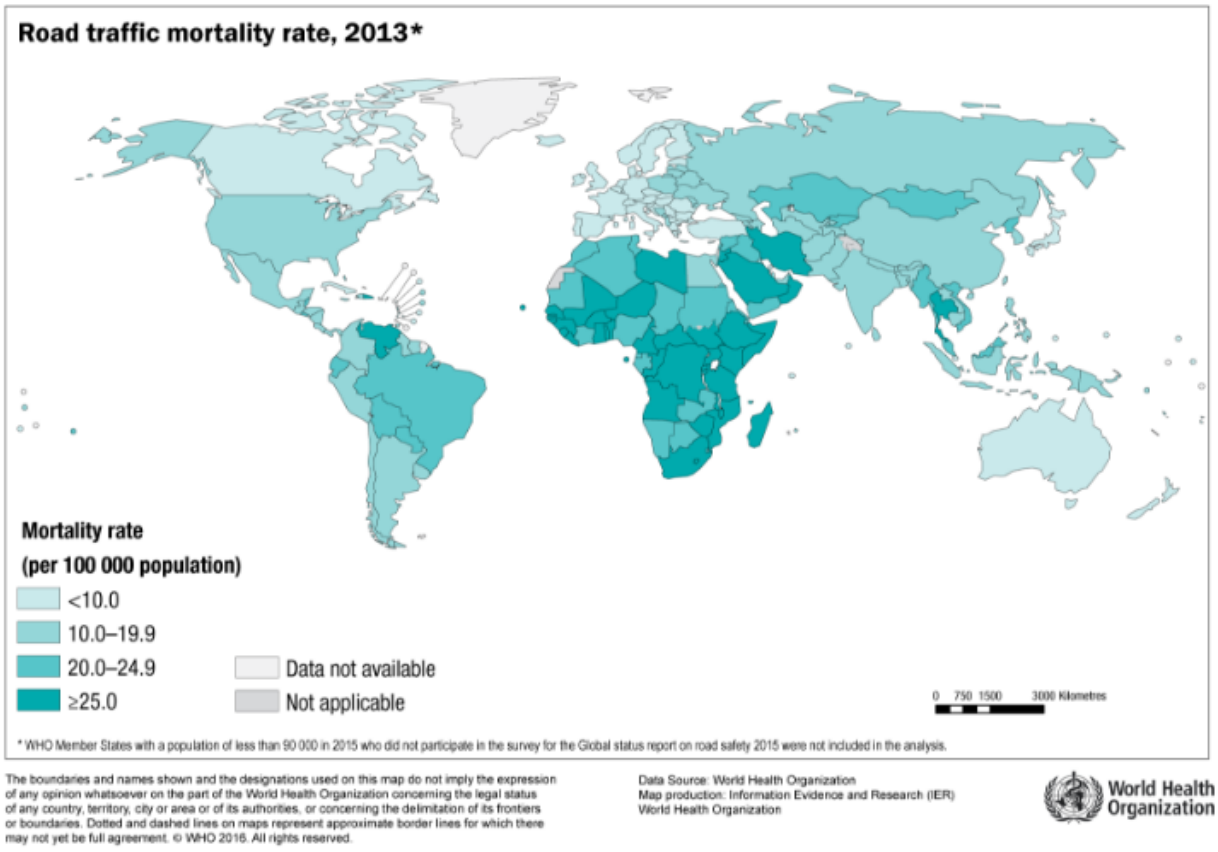


Figure 6 – Global road traffic mortality rate, 2013 (WHO, 2013).

Sexual Violence

According to the HPN, sexual assault is a distinct category of threat and should be treated with specific "prevention, mitigation, crisis management and after-care" (2010, p. 209). Sexual aggression can be motivated by a number of factors including the desire to gain power, humiliate others, and for sex (HPN, 2010, p. 209). They cite working in conflict or unstable regions, regions where women are expected to be subservient and are subjected to other local cultural or political beliefs, as factors that increase the risk (HPN, 2010, p. 209). Beliefs associated with sexual violence include: 1) the perspective that certain types of women are unworthy of respect and therefore sexual objects; 2) that feelings of power can be acquired through the domination of others, and that this power can elevate the social group the rapist belongs to; 3) that participation

in gang rape can increase group cohesion and bonding within a group; 4) that rape can be used as a tactic in war to demoralize the enemy, weaken social bonds and humiliate the opposing group by degrading local women; 5) that rape can also be used politically as a terror tactic to intimidate those intervening in a territory or community (HPN, 2010, p. 209). Clarity on the motivation behind such sexual violence should influence prevention and mitigation measures in order to best protect staff, volunteers and clients (HPN, 2010, p. 210). HPN (2010, p. 210), highlights sexual assault and rape as a security risk that requires more attention in security policies and protocols.

2.5.4 Environmental Risks

Experts conclude "that environmental degradation, poverty and disaster risk share common causes as well as common consequences for human security and well-being" (United Nations Environment Programme, 2011, p. 4). Environmental risk often overlaps with other risk factors such as health, safety and food insecurity.

Natural Disasters

According to Stoddard et al. (2015, p. 32) the Centre for Research on the Epidemiology of Disasters reported 350 natural disasters in 2013. They note that environmental risks such as natural disasters can have sudden-onset which usually cause acute crisis followed by emergency response and recovery (Stoddard et al., 2015, p. 33). Having effective emergency response protocols in place is an important element for international development organizations responsible for staff and volunteers working in regions where natural disasters may strike. This is especially important in regions where infrastructure and the capacity to respond to disasters may not be in place (Stoddard et al., 2015, p. 34).

Climate Change

According to the WEF, "climate change is expected to amplify existing security problems and create new ones" (2016, p. 30). Extreme weather events are anticipated to become more frequent and intense which will have increasingly more severe impacts on impoverished countries with high levels of instability (WEF, 2016, p. 30). Experts are aligning predicted water and food shortages with the impacts of climate change. Presently, over a billion people lack access to clean water and 2.7 billion people experience water shortages for at least one month each year (WEF, 2016, p. 12). As "wells dry up, crops and fisheries fail, and people lose their

livelihoods, simmering tensions between social groups are more likely to boil over into community violence" (WEF, 2016, p. 30). This also swells the ranks of terrorist and guerilla groups who may be able to find new recruits amongst the despair and frustration (WEF, 2016, p 30). These challenges may pose a number of issues for international development organizations. Experts suggest that "early warning systems, risk assessment and the use of sustainable natural resources, are – in practice – disaster risk reduction activities" (United Nations Environment Programme, 2011, p. 8).

2.5.6 Global Risk Overview

Figure 7 offers WEF's (2016, p. 3) overview of the most likely global risks based on regions. This provides international development organizations a sense of contextual challenges existing in the regions.

Figure 7 - Most likely global risks 2016, based on regions (WEF, 2016, p. 3).

2.6 Creating an Environment for Effective Security Risk Management

Effective risk and security management requires a culture of consciousness and action. There are a number of factors that create an environment for successful security risk management. This section of the report provides an overview of the acceptance approach to security risk management, the development of a security risk culture and communications strategies.

2.6.1 Acceptance Approach to Security Risk Management

Throughout the literature, the 'acceptance approach' is commonly cited as a cornerstone to successful security risk mitigation for international development organizations (HPN, 2010, p. XV; NRC, 2015, p. 15). This approach to security risk management is built on the premise that threats can be reduced by developing community relations and gaining local acceptance for organizational operations in the region (HPN, 2010, p. XV). It is thought that a community is more likely to protect an organization and its staff and volunteers if there is an appreciation for, and understanding of, their work (Childs, 2013, p. 64; HPN, 2010, p. XV).

Childs (2013, p. 65), posits that with the increase in violent incidents against international aid workers, this passive approach is proving insufficient. He notes that international development organizations rely on doing good to generate acceptance. He points out that the "level of acceptance…generated is dependent upon three factors – the quantity and quality of the aid provided (and secondary benefits such as employment or business), the degree to which a potential attacker values aid and the social distance between the potential attacker and the person(s) benefiting from the aid" (Childs, 2013, p. 65). Of those, only the quantity and quality of aid can be controlled by any organization (Childs, 2013, p. 65). Childs (2013, p. 65) argues that attackers are often healthy and not the typical recipients of aid, meaning they may not have strong ties with the aid an organization provides. Additionally, as the provision of aid can cause anger and resentment, it is important to assess the level of organizational acceptance from both the community and specific risk sources (Childs, 2013, p. 65). Childs posits that "the risk of a targeted attack is inversely proportional" to the strength of the threat group and that the application of this knowledge can help international development organizations assess and mitigate targeted attacks more effectively (2013, p. 65).

2.6.2 Developing a Risk Management Culture

In order to effectively implement risk management, an organizational culture that reflects a balance between the mission of an organization and program criticality, must be developed (Berg, 2010, p. 81; InterAction Security Unit, n.d., p. 8). Berg (2010, p. 81) posits that this culture outlines expectations around risk practices as well as organizational limits. By creating an inclusive system that engages staff, a common understanding of threats and shared responsibility for following protocol is created (HPN, 2010, p. 28).

Creating a culture of risk awareness and the space for related dialogue allows for more insight into risks, their root cause and potential impact (Berg, 2010, p. 81). It can also increase communication, foster inter-departmental relations and create proactive action around managing risk (Berg, 2010, p. 81). This is thought to increase the notion of risk management as a benefit rather than a roadblock in meeting objectives (Pironti, 2012, para. 1). Lalonde and Boiral (2012, p. 278), highlight the importance of providing staff training and creating a reward system for staff who detect and report risks. This positive reinforcement creates cultural acceptance related to security risk management.

2.6.3 Risk Management Communications

According to Berg (2010, p. 88), clear communication is an integral element of an effective risk management process. Developing policies, handbooks, reporting standards and submission procedures helps to systematize processes and increases the likelihood of the protocols being completed correctly (Berg, 2010, p. 88). Although organizations usually have a critical incident management team (CIMT) who are trained and responsible for crisis response, it is important that all team members be well versed on the risk management process (HPN, 2010, p. 236). This furthers the risk management culture and encourages every staff member to view the work of the organization through a risk management lens.

Incident Communications

During an incident, information must flow quickly and effectively to actors and managers (HPN, 2010, p. 106). It is a common practice to have designated staff communicate via a communications tree to a set number of others who are then responsible for passing that information along to a set number of recipients by phone, SMS or radio (HPN, 2010, p. 106). A

secondary source of contact (such as a SAT phone) should be established since in country networks can fail during conflict or environmental disasters (HPN, 2010, p. 106).

2.7 Challenges to Implementing a Security Risk Management Plan in International Development Settings

According to Lalonde and Boiral (2012, p. 286), challenges with risk management can arise when organizations: 1) create a false sense of security by developing inadequate risk management systems; 2) are ineffective at implementing these systems; 3) lack the necessary resources; 4) do not integrate risk management into their processes; 5) do not train their staff or adequately support them. Other challenges include staff turnover, inconsistent training or training that is not in line with the threats in that region (HPN, 2010, p. 30). This section of the report provides an overview of common challenges to implementing security risk management and considerations for international development organizations.

2.7.1 Risk Perception

According to Lalonde and Boiral (2012, pp 282 & 272), risk has an element of social construction where individual perception influences attitudes toward risk. Additionally, unconscious adjustment to a higher risk threshold due to consistent exposure to threats may cause a differential between the perceptions of risk for local staff versus international staff (HPN, 2010, p. 113). This adjustment, called danger habituation, is aligned with the reduction of objective risk assessment and increased risk-taking behaviour (HPN, 2010, p. xvi).

2.7.2 Vulnerability Based on Identity

In security risk, threats may differ for international and local staff as well as staff of differing genders, ethnicity, sexual orientation or religion (Gaul et al, 2006, p. 11). Implementing risk management without sensitivity to the vulnerabilities that exist for different staff and volunteers can be short sighted. According to Gaul et al (2006, p. 11), national staff can be at greater risk than international staff due to negative associations with working for Western organizations, perceived wealth, and ease of abduction with lesser risk of retaliation than if done to international staff. Gaul et al (2006, p. 11) explains that it is often assumed that national staff are at less risk because they are thought to understand local context and language. For this reason, nationals are often left out of security trainings (Gaul et al, 2006, p. 11).

Gender Risks

According to Persaud, gender is an important element to consider in order to create a "human-centred [security risk] approach" (2012, p. 10). Persaud (2012, p. 10) states that both male and females have distinct vulnerabilities and that culture and religion influence the understanding and importance of gender in a society. Concerns about violating social norms by addressing gender issues can be considered one of the reasons some organizations have not integrated gender into their approaches (Persaud, 2012, p. 14). Other internal organizational challenges to integrating gender into security management include: 1) the biases of staff and stakeholders; 2) difficulty gaining buy-in regarding gender sensitivity; 3) predominately men managing security, and; 4) lack of consultation with relevant groups of staff (Persaud, 2012, p. 15). Persaud notes that "the implementation of gender-specific security measures (or procedures) should not compromise gender equality" (2012, p. 14).

Persaud (2012, p. 17) recommends examining if and how gender is integrated into organizational security policy. She recommends that organizations review: 1) gender equality and empowerment in programming; 2) using a gender lens in policy frameworks; 3) gender distribution and employment equity; 4) how process and procedures respect gender (Persaud, 2012, p. 18). New policies should be developed where gaps are found. Recommendations for implementing gender-sensitive security includes relevant training and onboarding, standardized policies and procedural documents, as well as security plans (Persaud, 2012, p. 29).

2.7.3 Inappropriate Motives

According to HPN, many international development organizations begin programs "in high risk environments without the money and competencies they need" often to meet an important need in a community or because of the financial incentive (2010, p. 38). As well, those with the resources can be distracted from security risk management by other organizational priorities (HPN, 2010, p. 38). HPN (2010, p. 38) recommends reviewing organizational motive for beginning programs by reviewing the influence of donors and financial incentives.

2.7.4 Considerations for Security Risk Management Approach

The international development world is interdependent in many ways and one organization's approach to security management can impact other organizations in the same

region (Gaul, 2006, p. 10). For instance, having armed guards on site is one protective strategy for security management (HPN 2010, p. 1). However, according to Gaul et al. (2006, p. 10), an organization may endanger other organizations by hiring armed guards, inadvertently exposing those without guards as easy targets. One's approach should be considered for impact to other stakeholders.

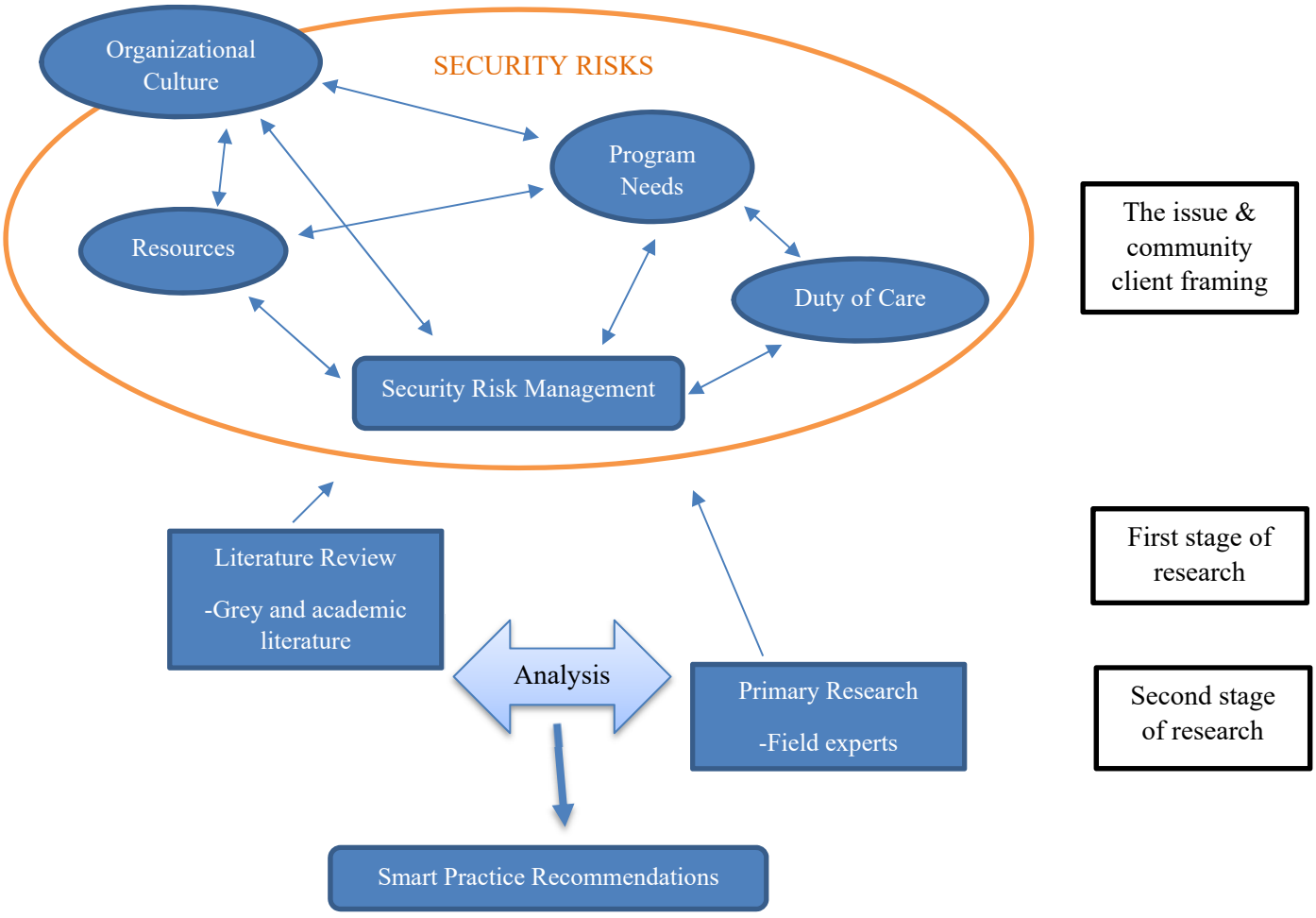
2.8 Summary

Reports on security risk management protocols from organizations operating in various countries were utilized to gain an understanding of current smart practices, as well as implementation strategies and challenges. International network's and agencies' reports were reviewed for common strategies employed in-country, conditions under which those strategies were employed, and the global context in which international development organizations operate. The requirements for creating an environment for successful security risk management, as well the challenges to implementing a security risk management plan were addressed. The literature was drawn from a host of sources including academia, business, government, non-governmental organizations, associations and networks in the area of both risk management and security risk management. While a number of academic sources could be found for risk management practices from many fields, most of the security risk management literature was sourced from security risk networks or organizations operating in diverse international contexts. In order to create a full picture of global risks, information was compiled from global reports from authorities, security risk databases and scholarly research in diverse fields. Literature on risk management and security management protocols were compiled to give a more fulsome description of practices.

2.9 Conceptual Framework

The conceptual framework for this project focuses on examining smart practices as a means to elicit insights into more effective security risk management plan development and implementation. The conceptual framework was based on the notion that security risks are an unavoidable part of international development work, as is the complexity created in regard to the development of programs, distribution of resources, and actions around duty of care. The literature review and primary research took a holistic view of the context and other influencers to

provide smart practice recommendations. Smart practices were defined as protocols/actions mentioned by more than one interviewee as well as unique practices that evolved from practice-based iterations or in response to changing risks.



3.0 Methodology and Methods

This section provides an overview of the qualitative methodology and methods used to collect the primary research.

3.1 Methodology

The methodology for this research involved a smart practice review of security risk management protocols through interviews with key international development, volunteer cooperation, and security network agency staff, as well as a literature and organizational document review. Conducting a smart practices review helped provide clarity on practices that have been tested and proven successful in similar organizations (Bardach, 2012, p. 109; Vesely, 2011, p. 99). The smart practices outlined in this report are what Bardach (2012, p. 116) would describe as flexible and not overly prescriptive allowing them to be applied to varied settings. Those selected were referred to as effectively accomplishing their required task and demonstrating their organizational value by a number of organizations and researchers (Bardach, 2012, p. 115 & p. 121). The smart practices collected create what Vesely (2011, p. 99) describes as a set of exemplars that can be utilized across diverse contexts. Phone interviews with key informants were employed to collect information from parties in different global locations to gain insight into current practices. This allowed for practices to be compared and analyzed, and for the complex phenomenon that enabled them to be successful to be understood (Vesely, 2011, p. 103 & p. 107). This is important, as the smart practices ideology outlines the importance of assessing the context for the application of these practices (Bardach, 2012, p. 120-121).

3.2 Methods

The literature review was completed to compile relevant research on the topic and interviews that were undertaken with key informants to gain knowledge on current security risk management practices in diverse international contexts. Important documents were provided by informants as exemplars. All of the compiled research was then utilized to identify common smart practice.

3.2.1 *Key Informants*

Security risk management smart practices were gathered through semi-structured interviews with eight participants; seven from international development and volunteer cooperation agencies and one from a security network. As well, a review of procedural documents was completed. Organizations were selected based on their significant histories working in international development, humanitarian contexts and with security strategies in complex regions. They varied in size, reach and budget (from approximately $15 million to $380 million) which allowed for the comparison of diverse challenges and practices employed. The purpose of this was to understand whether smart practices differ based on access to resources or the increased complexity of operating in more countries with a larger staff/volunteer base. This information will be useful for WUSC and other development agencies as they look toward expansion.

3.2.2 *Interview Process*

The semi-structured interviews included planned questions but allowed the interview to take a conversational form so that the interviewees could discuss and explore issues of importance (Longhurst, 2016, p. 143). This format of interview allowed the interviewer to build rapport with the interviewees, which is known to increase information sharing thereby providing the space to learn more about specific ideologies behind organizational practices (Longhurst, 2016, p. 147 & p. 153). By utilizing semi-structured interviews, discussions were directed yet broad, which allowed interviewees to provide detailed and revealing insight into unique organizational phenomenon and context (Chadwick, Gill, Stewart & Treasure, 2008, p. 291). Additionally, questions were designed to gain information on specific protocols and practices that have been effective for organizations when implementing security risk management plans. Challenges and organizational gaps in these processes were also requested. Eight interviews were completed by phone and one by Skype. Interviews were 45 minutes to one hour in length.

3.3 Data Analysis

Data was systematically analyzed within this project. Each interview was recorded and notated. Afterwards, interviews were transcribed from the recordings and thematic coding was undertaken from these transcripts. Primary themes and associated concepts were captured in a

spreadsheet with the following categories: 1) security risk philosophy; 2) frameworks and tools; 3) risk categorization; 4) global risks; 5) creating an environment for security risk management; 6) resource allocation; 7) media influence; 8) applying a gender lens, and; 9) challenges to security risk management implementation. Concepts that were recurring amongst the interviewees, as well as unique yet effective practices were considered the primary themes. These themes demonstrated the key concepts relevant to answering the research questions. While some participants provided relevant organizational documents, the findings were primarily based on interview results.

3.4 Project Limitations and Delimitations

This section outlines the limitations and strengths of this primary research, to frame it within the existing body of research and research that will come after.

Limitations

This project collected information from staff at eight international organizations with six residing in Canada and two in the United Kingdom. It did not gain the perspective of national staff in the various regions these organizations operate. Not all organizations provided policy or procedural documents for review.

Delimitation

This project includes in-depth semi-structured interviews with staff from international development and volunteer cooperation organizations as well as a security network. These interviews elicited information on effective risk management practices within diverse organizations working in the field and provided insight into the elements that impact security risk management successes or failures. This structured process of knowledge gathering allowed for in-depth discussions and the exploration of diverse topics, as well as an organic discussion of unique and successful practices in security risk management. In a predominately male dominated field, all but one of the interviewees were women.

4.0 Findings

This section provides a summary of the major themes collected in the primary research. The information collected through interviews with staff at relevant organizations offers practical answers to the research questions posed.

4.1 Introduction

In order to gain practical knowledge from the field, interviews with eight staff from seven international development and volunteer cooperation organizations, as well as one security network were undertaken to learn about effective smart practices for security risk management. Although from diverse positions in a variety of organizations, staff interviewed all had shared experience working in security, program, project or volunteer management positions internationally. Many had undertaken humanitarian work in-country and seven of the eight staff had worked as country, regional or international directors which gave them a holistic perspective of how security risk management functions within their organizations. Two staff interviewed were located in the UK, while the rest were located in Canada. Seven of the eight interviewees were women.

The research findings present major themes discovered in the interview process in the following areas: 1) creating an environment for successful security risk management; 2) security risk frameworks, tools, training and policies; 3) risk categorization and global risks; and 4) challenges to implementing a security risk management plan in international development. Smart practices were selected based on consistency between interviewees as well as unique procedures noted as effective. This research is presented in a way that preserves the confidentiality of the interviewee and their associated organizations.

4.2 Creating an Environment for Effective Security Risk Management

Creating the right environment for security risk management is helpful for allowing the successful implementation of such a system. This section of the report provides an overview of the factors many organizations employ to create an environment for successful security risk management.

4.2.1 *Security Risk Philosophy*

Although organizational security risk philosophy was not clearly articulated by approximately 50% of the interviewees, throughout the interviews it became clear that for many organizations, security and risk management ideologies were embedded in their day-to-day work. Many participants noted that security risk management was an important element in the planning of programs and that significant organizational awareness existed. Three interviewees stated that the security triangle - which outlines the ideologies of acceptance, protection and deterrence, formed the basis of their security risk philosophies (HPN, 2010, p. 55). A 'safety first' approach and the idea of balancing organizational mandate with risks, which allowed an organization to "work in difficult contexts but with a safe work environment", were also mentioned. Those who had experience working in conflict zones noted the importance of having a security philosophy based not only on protecting staff but enabling important programming.

A common theme throughout the philosophy discussions was centered on the importance of having adaptive programs and mitigation measures based on context and risk, as well as clarity on field based applications of risk thresholds. Participants mentioned that contexts were constantly changing in international development and thus, reactivity was an integral element of effective organizations. The monitoring of issues, observation of trends, and adjustment of programs and training activities were described as positive elements of various organizational security risk management programs. The security risk philosophies were thought to influence those actions.

4.2.2 *Culture of Security*

According to a number of interviewees, everyone is interdependent when it comes to security. This heightens the importance of communicating this joint responsibility. The value of openness and transparency in building a security risk culture was mentioned by two interviewees. Dialogue around smart practices for upcoming tasks was said to make for better executed projects in-country. Interviewees stated that gaining the trust and buy-in of staff regarding security risk management required inclusiveness and clarity. One interviewee explained that when directives were given without an explanation, resentment was often generated creating a volatile working environment. They suggested that gaining acceptance on

rules or protocols required negotiation and depth of context, and that dialogue was necessary to foster that understanding.

Open dialogue was also said to increase the safety of staff and volunteers by providing the level of personal information sharing required of security programs. They explained that asking certain personal details such as ethnicity, sexual orientation, or religion during the hiring process violates anti-discrimination policies in many Western countries; but that knowing those details are essential for providing effective mitigation measures and safety. They stated "[the security plan] will not say you cannot send ethnicity A into area B and vice versa. If you're not open about individual vulnerabilities the plans can be unworkable because they do not go down to the level of detail required". Fostering a sense of comradery, respect and responsibility toward one another, helps build a culture of security.

The role of the Board of Directors and the senior management was also thought to shape the culture of security, as a number of interviewees described it as "starting at the top". Board of Directors were said to create more staff accountability by requiring senior management to take security seriously. The security risk attitude of leadership was thought to then have a trickle-down effect to middle management and front line staff. Additionally, two interviewees felt having a clearly controlled hierarchy making calculated decisions was required, especially in higher risk areas.

Rules and procedural reporting were also noted as essential elements to shaping this culture of security. These were thought to create consistency, help clarify expectations and capture relevant information that form institutional knowledge. For one organization, reporting expectations were also placed on volunteers requiring that they report near misses and incidents while on overseas placements. This was thought to engage volunteers in the security risk culture and also ensured they were aware of their personal responsibility for their safety and the safety of those around them. Most interviewees stated that security risk management responsibilities were distributed across roles in their organizations. This was seen as both a positive – everyone shared the responsibilities and contributed to creating a safe environment; as well as a negative – responsibilities were scattered and no one person held the responsibility for ensuring systematic or consistent approaches. One participant noted that their organization operated under a

committee setting which helped with security risk information and data sharing across departments.

4.2.3 *Responding to Changes in Security Status*

Researching contexts, understanding the complexity of regions and being vigilant to monitor subtle changes in context was noted as an important part of predicting deterioration in security status in regions. Flexible and reactive security risk management systems were noted to pick up these contextual changes. Updating risk assessments in order to inform escalation measures was mentioned by almost all interviewees. This was also said to inform an organization as to when they have met their risk threshold and whether they need to "stand down" or evacuate a location. Measures such as check-in systems, restriction of movement, and curfews were examples of systems put in place in response to heightened risks. Increased training for staff and volunteers in specific areas was another mitigation measure discussed to help increase awareness of heightened risks and increase confidence in security risk response.

4.2.4 *Communications*

One organization required that senior management update board members on security risk management plans and global risks quarterly. This meant that information had to be shared between departments and reported from countries of operation semi-regularly. Regional meetings were also mentioned as an arena to discuss security, mitigation and protocols, as well as to share upcoming concerns. One unique approach described by one of the interviewees was the notion of organizational jurisdictions. Each jurisdiction was under the leadership of a CEO who was responsible for anyone who entered their jurisdiction. As a result, CEOs were kept informed of staff movement and communicated with other CEOs to provide details on staff travel to their region. This was considered important for evacuations or other emergencies.

Emergency Communication

Many interviewees stated that emergency communications were approached in a systematic way. Clear reporting structure for incidents with accessible and appropriate contacts (i.e. medical contacts, insurance, legal contacts etc.) in the case of emergencies was mentioned by all interviewees. Clearly documented emergency communication processes were thought to bring clarity and integration into roles and ensure that new staff or volunteers were clear on

actions to take for a diverse set of emergencies. Additionally, clear emergency communication processes were noted to increase due diligence and reduce the likelihood of error. Secondary plans or delegation of authority was also noted as important in emergencies. As one interviewee aptly stated “clarity on what to do, when, especially in a time of crisis can mean life or death.”

4.2.5 *Acceptance*

Several interviewees noted the value of stakeholder relationships and the strength of the safety net created by community acceptance and partnerships. Local knowledge was viewed by all interviewees as integral for understanding contexts, nuances, and complexity, especially in insecure environments. The connection with local community was also said to increase organizational ability to react quickly in incidences. One interviewee explained the importance of working to build community relations rather than creating a false sense of security by thinking that “doing good” builds acceptance. They stated “I think there’s a traditional idea that if we’re doing lovely things, no one will hurt us; and that doesn’t work as a security strategy. But building up acceptance and working with, not only direct beneficiaries and other stakeholders, communities - places where we have compounds, places that we have an impact on, and really understanding the context and actors where you’re working, you can build up, to a certain extent, security through acceptance”.

4.2.6 *Resource allocation*

One organization undertook research on smart practices in security risk resourcing and found that there was “no best practice”. By their calculations, budgetary allocation for security risk management ranged from 3 to 30% on different projects. Six of eight interviewees stated that their organizations had security budgets allocated in their programs or that funding allocation was at the discretion of the country director. Interviewees highlighted the importance of having sufficient resources to respond to incidents and contextual changes, to properly and systematically train staff and perform in-depth risk assessments regionally and internationally.

One interviewee felt that a smart practice for budgetary allocation for security risk management included approaching security as a direct cost, rather than overhead. This practice was thought to enable programming and ensure that security risk practices were effectively implemented without being discounted.

Staffing

The vast majority of interviewees noted that the country director was responsible for the overall security risk management in each country. A number of interviewees noted that security advisors were often hired for high risk countries and that allocation was based on the volume of work in the country. One interviewee expressed that their organization hired approximately 98% national staff in each location which they felt provided more stability to the programs and better understanding of local contexts. Additionally, another interviewee noted that increasingly organizations are "recognizing the importance of having data analysts to really understand the context and the programs that they're implementing…how the context is impacting on their ability to undertake programs".

4.3 Security Risk Frameworks, Tools, Training and Policies

This section provides an overview of the frameworks, tools, training styles and policies currently in practice in diverse international contexts.

4.3.1 *Overview of Security Risk Frameworks and Tools*

Interviewees reported that their organizations followed diverse security risk frameworks ranging from those independently developed, those based on the ISO 31000, the Security Triangle, and Canada's Global Affairs Result-Based Management protocols. The majority of participants demonstrated an understanding of the practical tools contained within the frameworks rather than stating which specific framework was being followed. Interviewees highlighted the importance of understanding and assessing the context in which they were operating. This information was collected from partners, local staff, embassies, high commissions, donors, media and context specific research. Similarly, risk assessments were shaped by information collected from trusted stakeholders, local media reviews and interactions with volunteers/staff who had returned from in-country placements. In all cases, risk assessment and analysis was completed at a regional and local level by in-country staff.

One unique approach to risk analysis was expressed by an interviewee employed by a security network. It included an 18 question discussion list rather than a checklist. This was thought to lead a team to appropriate actions, empowering staff through active problem solving.

The interviewee noted the importance of confidence in decision making, as well as a strategy for creating consistency across regions in the application of this approach

Risk Matrix and Register

Almost all interviewees cited the risk register and risk matrix as integral parts of their security risk management tools. One interviewee from a mid-sized agency shared a colour-coded risk tolerance guide (based on a risk matrix) that their organization created outlining the specific issues they see regularly. They utilized this in country as a frame of reference for how each risk might appear at different levels of severity - low was colour-coded green up to a critical risk which was colour-coded black. The guide was thought to systematize and simplify the risk assessment process across global programs. An additional systematization technique mentioned by another interviewee was creating a global schedule for updating risk registers across all sites. This was thought to keep information up to date and keep teams accountable. Many also expressed the value of their organization participating in security networks and forums to share information on challenges and learn more about effective tools and smart practice from a host of similar organizations.

Most organizations were said to rank, prioritize, and assess the degree to which security risk mitigation could occur. This was done in accordance with their organizational risk threshold. For many, senior management and the Board of Directors were part of these processes quarterly, as the legal risk owners. Their inclusion was thought to increase the understanding of in-country risks at the senior level and the perceived importance of security risk management across the organization.

4.3.2 *Training*

All interviewees outlined the important role of training in their security risk management systems. It was expressed that staff must be aware of the risk context in which they work, as well as mitigation measures and emergency protocols in place to ensure organizations are meeting their duty of care. A number of interviewees mentioned a need for consistency in on-boarding and security training even though nearly all interviewees witnessed inconsistency in frequency, type and who was invited to participate in trainings. The only consistent training noted by all interviewees was that of in-country briefings for visiting staff/volunteers and pre-departure training for volunteers by volunteer cooperation organizations.

Many organizations hired local agencies such as police or high commissions for in-country training, whereas other organizations hired private security agencies to provide more extensive training or had staff participate in network trainings. The appropriateness of some of the private security training was questioned by one interviewee. They debated which approach - realistic simulation (i.e. bagging and tying participants to simulate a kidnapping) or practical discussions, were more appropriate to train for preparedness and information retention. Concerns about a lack of affordable and appropriate security solutions in different regions was mentioned. Cost related to training meant that some organizations did not consistently provide personal security training to national staff in-country.

Mental health training to support staff and volunteers working in stressful environments and a global earthquake scenario exercise were two unique training offerings presented. Earthquake training aligned with the regions they worked in and was a way to demonstrate the importance the organization placed on addressing this environmental risk while ensuring training was cohesive.

4.3.3 *Policies*

Discussion centered on the way policy was created and applied by international development organizations. Similar to the risk threshold process, for most organizations, new policies required board level approval. The importance of senior level engagement in security risk policies that specifically addressed changing contexts, process, and procedures was mentioned by three interviewees as integral for providing clarity on field level actions. Inappropriate or out of date policy was thought to handcuff frontline staff while relevant policies could help provide continuity across global locations.

Consistency was defined as important for policies yet nearly all interviewees expressed the importance of allowing for flexibility in their application. The notion that some organizations became too practice oriented, developing policy and operating procedures that reduced problem solving and encouraged staff to check boxes was presented by one interviewee. This same interviewee stated “You cannot empower somebody with a checklist and expect them to create an understanding of the context you’re working [in]…[they need] an ability to be flexible and to make decisions”.

One interesting policy discussed in the interviews was one organization's environmental policy. The interviewee mentioned that environmental protection was at the core of their programs. In consultation with experts, the organization developed an environmental ranking system that each program was measured against. Interventions were then developed to both mitigate program related environmental impact and reduce environmental risks for each program.

4.4 Global Security Risks and Categorization

The way in which organizations categorize risk, as well as common global risks they face across sites provides insights into the context in which international development organizations operate. It also offers opportunities to assess organizational preparedness and provides areas of risk that may require focus or investment.

Categorization

According to one interviewee employed by a security network, broad categories as suggested by the United Nations such as crime, terrorism, natural disasters, civil unrest and armed conflict are generally accepted by many organizations. However, they also highlighted the importance of creating specific risk categories that represent the vulnerabilities of the individual organization. All interviewees noted that their organizations had a host of ways they categorized security risks including differentiating between "day-to-day risks" such as road traffic accidents and petty crime to large scale risks such as natural disasters or civil unrest, as they have varied levels of likelihood, impact and mitigation.

An interesting point was made by one security advisor regarding the categorization of risks. The participant noted that it is important to go beyond categorization and deeply analyze a risk to understand the intention behind it in order to effectively mitigate it. They mentioned that abduction, for example, is one category with different subsets provoked by diverse motives. Understanding the difference between express kidnappings, criminal kidnapping for quick cash, and politically charged kidnappings influenced mitigation and response. This also allows for proper data collection in the case of an incident to improve institutional knowledge.

Common Global Risks

Interviewees were asked to list the biggest risk and safety concerns they face across sites. The chart below represents their response as well as the number of organizations queried that noted that same concern.

Conflict related issues which could include outbreaks of gunfire, land mines, improvised explosive devices and other external threats related to conflict was the most mentioned risk throughout the interviews. Although these risks were not experienced consistently across sites, the general sense was that these threats were increasing globally and thus required more vigilance and organizational preparedness.

When asked directly about biggest risks faced across sites, traffic accidents were the most common concern for interviewees, with risks being higher in emerging countries with varied road condition and safety records. Interviewees expressed how getting into a motor vehicle was unavoidable in many locations and that mitigation was often not considered with the same vigilance as other risks. For organizations with volunteers, they could not ensure volunteers would not choose riskier travel options such as taking a motorbike taxi in a country with lax or weak traffic laws.

Sexual harassment and assault was the second most mentioned risk when asked directly. Issues of cultural norms, ideologies and expectations were discussed as some of the challenges with addressing these incidences. Three interviewees noted that the rates of reporting had increased, one noting specifically in Central and Latin America, but that there were still barriers to reporting (which will be discussed in further detail in the "Considering Gender in Security" section).

4.5 Challenges to Implementing a Security Risk Management Plan in International Development Settings

Challenges to implementing security risk management as expressed by actors in-country provide opportunities to gain relevant insights. Approaching security risk management implementation with these insights helps organizations avoid errors and improve success by knowing where to invest time, energy and mediate difficult circumstances. This section provides a number of challenges ranging from procedural to contextual.

4.5.1 *Variability in Security Risk Procedures and Processes*

Challenges to completing risk assessments, due to variability in risk tolerance for the individuals responsible, was mentioned by one interviewee. They posited that local country staff undertaking risk assessment did not always appropriately represent the risk status of their communities due to their own acclimatization to the circumstances. One example included organizational staff in Latin America mentioning that they did not feel the gang members visible in the streets were a risk if one was not participating in criminal activity themselves. The interviewee that shared this story noted that, as security advisor, they had to explain the relevance of this issue as a risk to foreign volunteers or staff, who may not know to follow social custom. This same security advisor expressed that she took security evaluation trips to various locations if the in-country risk assessments did not align with the information they collected from embassies, high commissions and local news.

The importance of a consistent and clearly communicated organizational risk threshold was conveyed by a number of interviewees. One interviewee shared the story of an organization member who stated that the possibility of death and abduction were not acceptable risks for their organization, but then stated that they planned to work in Syria. According to this interviewee

"those two statements are incompatible". The interviewee felt it important for organizations to create a risk threshold, then design and fund programs accordingly.

4.5.2 *Considering Gender in Security Risk Management*

Due to the varied status of women internationally, applying a gender lens is common in security risk management. All interviewees said their organization recognized gendered risks and two stated that they had gender advisors on staff to verify language, develop gender policies, and assess approaches for programming in more difficult cultural contexts for women (examples given included Iraq and Afghanistan). One interviewee spoke of the effort their organization put into gender-based programmatic analysis and mitigation policies related to the safety and security of participants. For example, they assessed female economic empowerment programs for their threat to safety due to the increased wealth for those who participated.

Additionally, two interviewees noted how organizations can inappropriately apply a gender lens creating gender bias instead. One such example was that of female staff having an earlier curfew than men. When further examined, the risks for men and women after a certain hour were the same. An additional example was a list of risks provided to female humanitarian staff arriving in Afghanistan. With the exception of a head scarf rule, every risk was related to respecting local culture and was equally relevant to both men and women. These examples demonstrate how biases can influence organizational culture and actions related to gender risk mitigation.

Sexual Assault/harassment

Assault and sexual harassment came up a number of times as something that required attention for both sexes but that was disproportional for women. Many discussed cultural gaps in what was considered sexually appropriate and suggested that teams needed in-country staff who could understand the complexity of the situations to assess them and define appropriate mitigation measures. They also touched on the lack of local resources common for follow-up and support for victims of sexual assault. One internal concern was the way reporting was often handled. In order to protect the victim, incident reports were collected in such a way that institutional knowledge was lost, creating a skewed picture of the severity of the issue.

Organizations took diverse approaches to finding means of addressing sexual violence including: 1) putting together a sexual violence task force; 2) providing sexual harassment and assault webinar training and tools for in-country offices; 3) senior management level discussions associated with gender-related security risk management issues, and; 4) an incidence reporting committee to keep anonymity of the victim. One interviewee noted that "[for] national staff, where there may be greater consequences for them reporting it than the incident itself, by using a committee which enables the information to be fed up into the system without it having a consequence on the individual."

A number of interviewees noted that a gender lens was too limiting and that focus should be on all forms of discrimination and oppression based on gender identity, sexual orientation, ethnicity, religion etc. One interviewee noted that their organization considered each volunteer and staff member holistically looking at the nuances of gender, age, ethnicity, and religion and how that might impact their experience and vulnerability in various locales.

4.5.3 *Staffing Issues*

One interviewee expressed the challenge with finding good staff. They felt that some organizations underpay their security positions and as a consequence, attract people who may not have the capacity to undertake the level of responsibility required of them. Others employ ex-military in-country who may have protective experience but may not have an understanding of the nuances of humanitarian action to appropriately undertake the role. Training for these roles is not always considered a priority when in competition for program funding. As a solution to the staffing challenges faced in-country, some organizations have taken to job sharing in high risk environments where staff work in 6 month shifts; others have taken to training program staff in security to encourage them to transfer to security roles within the organization.

Additional solutions to staffing challenges included the hiring of consultants and external firms. That was said to create situations where consultants facilitate a process and require already over exerted staff to write the associated reports; or the consultant writes a report for an organization that does not always gain traction with staff due to lack of internal ownership.

4.5.4 *Donors and Funding Related Issues*

According to a number of interviewees, there is often a discrepancy between the approach grant writers take and the practical requirements of programs in-country. There is a concern that security will be seen as a discretionary cost by donors and therefore rejected, so many grant writers will leave security out of their funding proposals. This may mean a program is expected to operate without adequate security funding.

Additionally, a number of interviewees discussed the challenges of mitigating changing security status of regions without the proper resources available to deal with those changes quickly. Most projects were described as having been funded based on budget forecasting. Two interviewees mentioned funding was unlikely to increase in regions appearing peaceful. Thus, organizations often had to be reactive rather than proactive. One interviewee noted that reports to donors, such as the Government of Canada's risk register, was not thought to provide a complete picture of the issues on the ground. This was expressed as a difficulty in conveying the reality of the risks or the nuances of the experiences of staff and volunteers to the donor. As a topic that arose organically in the interviews, further research would need to be completed to determine how this aligns with the literature.

4.5.5 *Media Influence*

Interviewees commented on the direct and indirect effect of the media on public perception. This was noted by various interviewees as something that required managing, for the sake of organizational reputation as well as influence on key stakeholders and donors. Some felt that media highlighted issues or events that could help their organizations reflect and measure against their current practices. While others felt media could cause problems for international development organizations by creating negative press and reducing communication acceptance. One example included the inflammatory media presentation of the Ebola crisis which made it difficult for some organizations to find volunteers for various regions in Africa.

Social media

Social media was approached with both appreciation and apprehension. The ease of contact by family members for staff and volunteers in times of emergencies was considered useful (i.e. crisis check in apps). On the other hand, while the speed of information sharing was

quite rapid, the quality of information was not always high. Additionally, “rate this organization sites” or the sharing of information such as organizational budgets without the proper context can create a loss of public support. One interviewee explained that many members of the public might reject supporting organizations with high administrative fees, however, organizations working in a high risk areas such as Syria, would be likely to have higher overhead.

4.6 Summary

The primary research provided a clear overview of current practices in security risk management. The semi-structured format of the interviews allowed for in-depth discussions of important issues, challenges and areas of opportunity for international development organizations. Methods for creating an organizational environment that fosters security risk management was discussed as a foundational element of effective system implementation. Built from that foundation, common practices - security risk frameworks, tools, policies and resourcing were also explored to learn more about approaches that were found to be beneficial. Common risks and risk categorization were discussed to provide a sense of the global contexts in which organizations are operating and to provide areas of focus for international development organizations. Common challenges to implementing security risk management in diverse settings were also shared in the findings, offering an opportunity to learn from practical experiences in-country.

5.0 Discussion and Analysis

This section provides an overview of the findings from both the literature review and primary research, and will discuss how those findings converge and diverge. Major themes related to the primary research question will be highlighted. The implications of these findings will also be examined and will inform the options provided to WUSC to support their security risk management implementation plan.

5.1 Smart Practices for Effective Security Risk Management

5.1.1 Risk Philosophy and Threshold

A risk management system sits within the greater organization as part of its strategic governance structure. As expressed in both the primary and secondary research, this system is influenced by organizational mission and vision. For that reason, it should be developed based on expressed risk philosophies and thresholds to create a cohesive approach. As security risk management systems need to be adaptive and reactive, yet maintain a balance between risk and mandate, the risk philosophy and thresholds provide parameters and guidance around operational practices.

In the primary research, security risk philosophy was not found to be clearly articulated by many of the staff interviewed, which could indicate poor internal communication of the philosophy or no clearly developed philosophy. Providing a clear philosophy can empower staff to think strategically when new risks arise and can reduce incongruent actions across sites. Additionally, clearly outlining organizational risk tolerance and thresholds clarifies limits around actions and can help define entrance and exit indicators for programming. Understanding the internal risk context, such as objectives, policies, strategic plans, as well as operational capacity helps inform thresholds (Berg, 2010, p. 82-83). Although program criticality may influence organizational action, risk thresholds and organizational capacity should inform programmatic decisions. Any adjustments to the thresholds should be thoroughly analyzed and discussed with the legal risk owner – Board of Directors, senior management, country directors etc., who are not often working directly in-country and according to one interviewee “should have as much information that they possibly can to make a right decision”. Duty of care must be considered when making such decisions.

5.1.2 Organizational Risk Culture

Equally as important as the risk philosophy and threshold, and also influenced by them, is the internal organizational security risk culture. Seventy-five percent of the interviewees ranked this element of security risk culture as the most integral component of their organization's security risk management practice. One security advisor's comment illustrates how their organization's efforts to change the attitude around security risk management impacted their security risk culture. "[Our organization] has been on a journey in the last five years to really see risk management, safety and security management as part of how we prepare. It's an enabler. It actually allows our programs to be effective and to be great. It allows our programs to be efficient and to use our money appropriately". This was in direct contrast to other's feelings that security risk practices were a roadblock or an additional hoop to jump through.

Aligning with the secondary research, they stated that creating an inclusive environment that engages all staff in a common understanding of the risks, as well as a shared responsibility for following protocol, is essential (HPN, 2010, p. 28). One interviewee mentioned the sense of contribution toward maintaining security, and understanding that each individual's actions can impact this system, as important for gaining buy-in. Clear, open communication and information sharing was said to be crucial to developing such a culture. One interviewee stated that for their organization "[there's] not a day that goes by in the field where you are not talking about how you are supposed to go about doing something and what the best way to do it is; the safest way to do it". Encouraging proactive action and presenting security risk management as a benefit can also create positive reinforcement for participating in this culture and present the idea that security risk management is an enabler (Pironti, 2012, para. 1; Lalonde & Boiral, 2012, p. 291).

5.1.3 *Risk Context*

Once organizational security risk philosophy and thresholds are defined, the external risk contexts must be assessed and understood. Both the primary and secondary research demonstrate the importance of holistic and in-depth contextual research to clarify social dynamics, structures, laws, politics, and environment in the regions organizations intend to work in order to prepare for and predict where issues may arise (HPN, 2010, p. 30-31). Additionally, HPN (2010, p.30) states that organizations should understand what role they will play in that context. Both the primary and secondary research recommend liaising with stakeholders, utilizing a host of

documents and resources to compile contextual information. Assessing risk context was described in both the primary and secondary research as an iterative process given the constantly changing contexts. One interviewee expressed evolving context as one of the most challenging aspects of security risk management. They felt it took a lot of effort to understand the complexity of contexts and how they are influenced and shaped. Employing data analysts was said to be increasingly more common in international development organizations as a method for consistent contextual assessment and analysis.

5.1.4 *Risk Frameworks*

With a clear understanding of the context in which the system will be implemented, as well as the risk philosophies and risk thresholds, a cohesive security risk framework can be developed (ISO, 2009, p 15). This framework helps organizations navigate security risk management complexities by standardizing processes in alignment with organizational mandate and mission (Berg, 2010, p. 83). Figure 1 (ISO, 2009, p. vii) in the literature review demonstrates the additional principles that should solidify the commitment of an organization around risk management; which becomes the basis for the design of a risk management system.

Both the literature review and research findings demonstrate that a number of frameworks can be applied to successfully implement an effective security risk management plan. With all frameworks comes the need to customize and select one that will meet organizational needs while taking a holistic perspective that includes all of the necessary processes (Berg, 2010, p. 79 & 81; ISO, 2009, p. 10; The Association of Insurance and Risk Managers et al., n.d., p. 3). This was reflected in the primary research by the number of diverse frameworks in practical use.

5.1.5 Systematization of Security Risk Processes

Frameworks provide standardized processes which help an organization create systematization. In order to meet duty of care requirements and to create consistency, continuity, and ensure effective data management across global sites, systematization is considered an important element of a security risk management system in both the primary and secondary research. Research also reflected the importance of a dynamic and responsive security risk management system. This adds a level of complexity to the management of a security risk

system that needs to be methodical and consistent but also flexible and reactive to changing contexts, programming, or dynamics.

5.1.6 *Commonly Used Tools and Protocols*

Although there are a number of tools available for security risk assessment and analysis, the most consistently mentioned tools, in both the primary and secondary research, were the risk register and risk matrix. These tools were said to be adaptable for context, easy to understand, and offered a visual that made clear whether or not risks fell within the risk threshold. They also help organizations create mitigation measures which are, again, said to be based on mandate, risk philosophy, and threshold (United Nations Somalia, n.d., p. 21). These tools provide a means to align mitigation measures with different risk levels, which can be shared across sites yet are flexible enough to allow for the addition of context specific risks or mitigation measures for each location.

Additionally, the risk register and matrix simplify security risk monitoring. As an iterative process, monitoring practices were expressed as important in both the primary and secondary research. Secondary research suggests reviewing risk and mitigation plans monthly and reporting on them quarterly to the Board of Directors (United Nations Somalia, n.d., p. 26). Interviewees stated that engaging the board and senior management in security risk management updates was thought to increase staff accountability and keep security at the forefront of organizational decisions. Both primary and secondary research outlined the importance of being reactive to contextual and programmatic changes in relation to the risk and mitigation plans. This highlights the importance of consistent monitoring practices. Additionally, monitoring may pick up complex information – changes in the environment or socio-political changes that can be difficult to detect without close inspection. Security networks were expressed in the primary research as important resources for the discussion of mitigation, challenges, and opportunities for improved actions, as well as shared environmental monitoring.

5.1.7 *Acceptance Approach*

Acceptance was often referred to as an important mitigation measure in international development in both the primary and secondary research. It is thought to reduce threat by gaining local acceptance for organizational operations and help root organizations within a community (HPN, 2010, p. XV). Although it was cited by nearly every interviewee as an integral part of

their operations, secondary research and one interviewee cautioned against the false sense of security that can arise from the notion that "doing good" generates sufficient community acceptance to protect staff and volunteers. Childs (2013, p. 65), notes that an increase in violent attacks on international aid workers demonstrates how acceptance – a passive approach, is proving insufficient. This revelation can be utilized as a lesson for international development organizations. Expecting acceptance to be an appropriate mitigation measure on its own can create more vulnerability, however, engaging with community and gaining acceptance is an important tool. According to the primary research, by developing strong relations with community, aid workers could learn more about context and complexity in the local environment. These relationships could also act as safeguards, improve program effectiveness, and support an organizations ability to react quickly to incidents.

5.1.8 *Applying a Gender Lens*

Both the literature review and primary research indicated that gender should be an important consideration when developing a security risk management system. While applying a gender lens can be misconstrued as a female approach, both male and females have distinct vulnerabilities (Persaud, 2012, p. 10). The primary research pointed out the importance of applying a gender lens appropriately to reduce employing a gender bias in process and procedures. Complexity around the cultural and religious influence on gender norms in a society, and concerns about violating these norms, were suggested as a barrier for integrating gender into security risk approaches (Persaud, 2012, p. 14). The literature encourages organizations to review their practices to assess and account for staff and stakeholders biases, buy-in to gender related policies, and gender balance in security roles.

In the primary research, many organizations employed gender advisors and had strong gender policies and approaches for programming. The literature suggested reviewing programming, policy frameworks, employment equity, and operational procedures for their application of a gender lens (Persaud, 2012, p. 18). Recommendations offered by Persaud (2012, p. 29) for implementing gender-sensitive security includes relevant training and onboarding, standardized policies and procedural documents, as well as inclusive security plans.

5.1.9 *Communications*

Communication was discussed as both a process vital to security risk management, as well as a means of "sense-making" for staff and volunteers in both the primary and secondary research. Communication was described in the primary research as an essential element in developing organizational security risk culture and gaining buy-in. Two interviewees noted the conflict often created by issuing security risk 'orders' rather than explaining the relevance and importance of required actions. Providing relevant context, especially in the field where some security rules could impact regular day-to-day life, was seen as a method for creating a more positive and cooperative atmosphere. Additionally, internal communication processes were discussed as essential to system cohesion and effectiveness. In the secondary research, communications products are described as important for systematizing processes. Clear communications policies, handbooks, procedures, and reporting templates or standards should be in place. According to the primary research, the benefits of this were trifold, as they helped create consistency for due diligence, reduced likelihood of error, but also created institutional knowledge influencing future decisions, actions, and iterations in the system.

5.1.10 *Resourcing*

According to the literature, resourcing should be based on risk assessment information, forecasting, cost-benefit analysis, organizational capacity, and cultural acceptance (Mitchell & Harris, 2012, p. 4). The primary research confirmed that there was no typical percentage of budget allocated to security risk management and that funding was generally proportionate to the level of risk associated with a region or project. Organizations commonly allocated funds to individual programs, while some had regional security risk budgets. There was some debate as to whether there should be a central budget for all projects to have minimum security funding. This might include resources such as satellite phones or flak jackets in conflict zones. It was felt by one interviewee that security risk should be considered a direct cost rather than overhead in order to create more consistency and capacity for organizations to implement security practices without skimping. They felt that challenges arose when internal fundraising teams removed security risk requests from funding proposals in order to make the proposal more palatable to donors. This action was said to put organizations in difficult positions as they received program funding, were accountable to donors, but then lacked the proper resources to undertake

appropriate security risk measures. According to the primary research, donors were not always amenable to these additions after the fact without a demonstrated change in the context or environment.

Contingency and unrestricted funds were mentioned in both primary and secondary research as a means of supporting programmatic or organizational adaptation to new context. This tended to be for emergencies and not allocated to programming preparation. In the secondary research, contingency fund budgeting was recommended to be proportionate to the risk and agreed upon prior to program start up.

Staffing

Staffing should be based on risk rating and workload for mitigation measures according to the primary and secondary research. In the literature, global security advisors were said to be becoming increasingly more common, as well as regional security advisors in high-risk areas. There was inconsistency in the primary research regarding the benefit of having a dedicated security advisor managing the system globally versus the shared responsibility created by distributing security responsibilities across roles. While some felt that security advisors might mean those in-country deferred too much to the advisor, others expressed the importance of the consistent oversight across programs that a security advisor could provide. Additionally, it was noted that responsibilities in-country would have to be delegated regardless. This could continue to foster the collective sense of responsibility that some felt might be removed with a security advisor.

In the primary research, many interviewees noted the employment of national staff in their global locations. While this was touted for creating added stability and local knowledge, concerns were brought up regarding a shortage of trained/experienced staff in various locations and the need to invest in capacity building. One interviewee felt national security staff were often hired without the skills required to fulfill important parts of their roles such as planning or budgeting. They stated the importance of providing relevant salaries to attract skilled people, as well as appropriate onboarding and training provisions. They also cautioned against the default hiring of ex-military who may have difficulty understanding the nuances required of an international development organization which should hold a non-politicized/neutral space in-country to effectively provide programming and maintain safety.

Training

Training was consistently mentioned in the primary and secondary research as crucial for successful security risk management systems. Training around how to effectively use risk tools, complete processes, undertake protocols, and understand context were discussed as essential in the primary research. The secondary research noted that training should be consistent, in line with the threats in that region, and sensitive to the vulnerabilities of the organizations and individual staff. The type of training offered by the organizations interviewed was diverse, ranging from onboarding and contextual reviews to practical scenarios. Practical exercises were thought to be helpful to keep skills relevant, increase staff and volunteer preparedness, and reduce the effects of danger habituation in-country. Discussion regarding how realistic simulation should be - as it can create undue stress in participants, was mentioned in the primary research. Stress reduction and mental health training was a unique program mentioned by one interviewee, as important for supporting the wellbeing of people working in complex and unstable environments.

5.2 Challenges to Implement a Security Risk Management Plan in International Development Settings

Contextual, behavioural, and external risk factors can cause significant challenges in security risk management. Organizations should consider the challenges they may face and adapt their approach in order to be successful. This section outlines some of the key challenges faced by organizations undertaking security risk management in international development.

5.2.1 *Global Risks*

In the interviews, participants described a general sense of increased risk and instability in the field. This was reflected in the secondary research with WEF's (2016, p. 11 and p. 88) report stating that within a ten year span, the most common international risks went from economic to environmental and conflict based risks. This report reinforces the notion that maintaining contextual understanding and risk thresholds is essential for navigating the diverse, evolving challenges in international development and humanitarian contexts. It also speaks to the need for more robust risk management approaches that follow the trends to ensure preparedness and effective mitigation.

Conflict Related Risks

As noted in the literature review, conflict has increased the requirement for aid and support from international development organizations in many regions. Both the primary and secondary research cited a need for increased vigilance regarding the potential for interaction with conflict related risks. As secondary research showed modern conflicts as having 90% civilian fatalities and an increased risk of aid agencies being targeted, organizations should be very clear on their risk threshold and the contexts they enter. Idealism does not have a place in security risk management. For example, if organizational threshold does not allow for loss of life or abduction, entering active conflict zones may be in contravention of organizational policies. According to Gaul et al. (2006, p. 9), political instability often removes the rule of law, a standard that many international development organizations rely on. It is important that organizations and their staff understand situational complexity and how this fits with duty of care, policies, and informed consent when entering a region.

Environmental Risks

According to WEF (2016, p. 30), natural disasters are expected to become increasingly more frequent and severe. Extreme weather events often have sudden onset causing crisis such as medical issues, unsanitary conditions, food insecurity or limited access to clean water (Stoddard et al., 2015, p. 33). Food and water shortages are said to create or increase tensions within community, and can create violence (WEF, 2016, p. 30). The complexity created by such events often necessitates multiple security mitigation measures to be enacted, requiring the taxing of many resources. According to the UNEP (2011, p. 8), early warning systems, understanding of context and risks, as well as the use of sustainable resources, are risk reduction activities. Organizations should approach such complex risks realistically, assessing organizational capacity to appropriately create sustainable and safe programming.

In regard to environmental risks, organizational actions are, in part, contributing to the creation of these risks. One interviewee mentioned the leadership their organization was taking on environmental policy to help play a role in reducing the risks. As a significant element of their programming and mitigation strategies they rank programs and interventions on their environmental impact and actively work to reduce their carbon footprint, for instance. Additionally, they focus on actively preparing for environmental incidents. One such example

was a global earthquake exercise hosted in all locations on the same day. This was in preparation for these types of events, in order to provide cohesive training and demonstrate the value placed on mitigating this environmental risk.

Sexual Assault

Sexual assault was noted by half of the interviewees as a significant concern experienced across sites. As expressed in the literature, it is a highly complex issue with a variety of beliefs catalyzing it. Interviewees noted the importance of having local staff who understand the context surrounding sexual assault, as this was an essential element to creating relevant mitigation measures. Reporting was a common concern in the primary research. One comment was that reporting may have been hindered by "white ex-military men" often being the first line of reporting. Additionally, for national staff, reporting such an incident could result in significant consequences – personally or socially. Incident reporting was said to be handled in a sensitive manner, which was important, but also limited the institutional knowledge and skewed statistics about frequency and context for further mitigation. Half of the interviewees worked for organizations seeking to address sexual violence in their work. A positive organizational culture around assault reporting that includes respect, confidentiality, and acceptance was said to increase reporting and discussion around concerns. Further research around this topic is recommended to assess effective mitigation.

5.2.2 *The Influence of Perception*

Perception and Danger habituation

Individual perception and danger habituation were stated in both the primary and secondary research as affiliated with the reduction of objective risk assessment and increased risk-taking behavior. This can have significant impact on both the development and effectiveness of a security risk management plan. This should be considered when senior managers or security advisors review plans and regional risk assessments. One security advisor interviewed stated that they checked regional risk assessments against embassy advisories and local news. When they found discrepancies, they would discuss these with the local team and plan a risk review trip to the locale in more extreme cases. Development by in-country teams with local knowledge, followed by a review by security advisors, the Board of Directors, or senior management, was thought to allow for more balanced assessments and accountability.

Media Influence

Important discussions arose in the primary research regarding the impact of the media on public and donor perception. Organizational reputation, which could be bolstered or damaged by media, was said to influence key stakeholders often resulting in significant impact on programs and funding. Examples were cited of negative press reducing community acceptance and causing significant harm to non-profit organizations in various regions. Social media was mentioned as an ignitor for high speed and sometimes low quality information. Organizational strategies to maintain public image and awareness were discussed as an important way to maintain public support. Further research on this topic and how it influences the communications practices of international development organizations would be valuable.

5.2.3 *Training*

Secondary research cited inconsistent training, training not in line with the threats in the region, and staff turnover, as harmful to successful security risk management (HPN, 2010, p. 30). Interestingly, all interviewees in the primary research noted inconsistency regarding training frequency, who was included, and type of training provided in their organizations. Lack of affordable and appropriate security solutions in different regions, often resulting in inappropriate private security training, was said to be a challenge in the primary research. Additionally, training expenses meant that some organizations did not consistently provide security training to both international and national staff in-country. This brings into question duty of care, fairness, and organizational commitment. Organizations should consider how severe the risks are in-country to assess whether they are putting national staff in jeopardy based on the assumption that they are equipped to deal with local risks. It is also important that organizations build capacity within a community, rather than interpret employing local people as performing their due diligence.

5.2.4 *Vulnerability Based on Identity*

Gaul et al. (2006, p. 10) noted that threats differ for international and local staff, as well as staff of different ethnicities, sexual orientations, religions, and genders. The primary research demonstrated that organizations need to look at the vulnerabilities that exist for each individual based on their various ‘identifiers’. Greater risks were found for national staff due to the assumption that they understand local context and language, and therefore know how to address

local risks (Gaul et al, 2006, p. 11). In the primary research, one interviewee stated that in situations that resulted in the evacuation of international staff, national staff were given the choice to stay and continue to work. This was stated as an option that one might want to exercise, as national staff are often loyal to their communities. From a social justice perspective, this may leave national staff with a very difficult choice. Knowing the limited prospects in their community for employment, choosing to demonstrate 'disloyalty' or 'abandon' community may lead to less than safe choices and raises the question of equity in organizational practices.

Gender Risks

In the primary research, the varied status of women worldwide was discussed. An understanding and awareness of gender differences was considered important in security risk management. This was reinforced in the literature by Persaud who cited gender sensitivity as a "human-centred approach" to security management (2012, p. 10). Sensitivity to gender biases when creating security plans and assessing risks was addressed as an important topic, as many interviewees felt that inappropriately applying a gender lens created inequality at times. Examples such as earlier curfews for women, or more rules related to the physical appearance of women even though inappropriate garb for both genders was considered deeply disrespectful in various regions, was discussed. Persaud (2012, p. 14 & p. 15) explains that security measures should not compromise gender equality and that integrating gender into security management required staff buy-in, awareness of biases, and consultation with relevant groups of staff. The literature revealed recommendations for implementing gender-sensitive security including: training and onboarding, standardized policies, procedural documents, and security plans (Persaud, 2012, p. 29).

5.3 Summary

The discussion section provides an in-depth analysis of both the primary and secondary research and how they find agreement or disagreement. Foundational knowledge required for development of an effective security risk management system was outlined in the smart practices section, along with frameworks, tools, and operational practices offering diverse strategies for success. In the challenges section, important practical observations and issues found in the literature were discussed. These provided an overview of typical contextual and internal challenges that might be faced by organizations, offering

opportunities to examine organizational preparedness. This research provides an overview of smart practices and approaches that are considered valuable by other groups. They do not represent a fulsome approach to security risk management for all international development organizations.

6.0 Recommendations

WUSC has undergone a security risk audit and is working toward implementing the recommendations from that audit. The following recommendations have been created based on the research outcomes, in alignment with the audit report recommendations, building on the work currently completed or in progress by WUSC. They outline relevant smart practices that will help shape the implementation of WUSC's security risk management plan and offer practical recommendations for how to execute these options in order of priority.

6.1 Recommendations for WUSC to Consider

The recommendations are divided into short-term (1 year), medium-term (3 years) and long-term (5 years and beyond) strategies. While some of these strategies can be implemented utilizing internal staff time, without an understanding of WUSCs budget and staff responsibilities, the resources required to undertake this plan need to be assessed. It is important to note that these selected strategies developed to support WUSC's implementation process do not represent a fulsome strategy for implementing security risk management plans.

1. **Communicate new risk philosophy and utilize this philosophy to foster a positive, inclusive and active security risk organizational culture and the associated implementation strategy**

Short-term strategies

a. Create and execute a security risk philosophy communications plan that:
    i. Explains the purpose and value of the philosophy;
    ii. Underscores how it will inform decisions and actions around security risk management across the organization;
    iii. Clarifies how it aligns with organizational mandate, mission, duty of care and risk thresholds;
    iv. Expresses how this will enable important programming to move forward.
b. Allocate messaging dissemination duties to managers, country directors and senior leadership (or other appropriate parties) in various global locations. Utilize site specific program examples to increase relevance and buy-in.
c. Develop behavioural expectations around security risk processes by:

i. Clearly stating requirements and goals for each process or protocol including schedule for completion (for assessment, analysis, monitoring etc), process for submission of reports or documents and systematized standard for the completion of reports or documents.

ii. Outline consequences for not following these processes/protocols.

Mid-term strategies

d. Develop behavioural expectations around security risk processes by:

i. Training staff on risk context, monitoring, mitigation strategies, processes, reporting, rights and responsibilities (including interdependence with other staff and volunteers and personal risk factors that should be disclosed);

ii. Creating opportunities for staff at all levels of the organization to discuss threats, concerns, and shared responsibility openly to maintain risk awareness and staff satisfaction.

e. Disseminate organizational charts and process flow charts for emergency response to all locations. Explain hierarchy for security risk decision making and process, for increased transparency.

f. Reinforce behavioural expectations around security risk processes by:

i. Creating opportunities for security risk dialogue at all levels, as well as a pathway for significant concerns to be shared with senior leadership and Board members;

ii. Rewarding proactive action by staff/volunteers;

iii. Sharing organizational consequences for not following risk management protocols;

iv. Sharing data across departments;

v. Highlighting the positive impact and adjustments made to the risk management process through new philosophy, and procedural or cultural successes on an annual basis;

vi. Ensuring ample resources for security risk management demonstrating the level of organizational investment.

2. Systematize processes while maintaining responsiveness and reactivity to context and risks

Short-term strategies

a. Clearly articulate organizational security risk thresholds and relationship to protocols.
b. Develop and communicate systems and schedules for context assessment, risk assessment, analysis, mitigation and reporting. Align this with the appropriate budget for mitigation and emergency response.

Medium-term

c. Assess policies and determine the level of flexibility in their application/who has the authority to make such decisions in different contexts.
d. Ensure the data management system is effective for building institutional knowledge.

Long-term

e. Integrate consistent and systematic security risk management processes into practice by:
    i. Training staff in processes and clearly outlining expectations for all staff/volunteers regarding procedures, timelines and deliverables;
    ii. Ensuring risk context in each locale is well understood and regularly monitored;
    iii. Updating risk analysis and mitigation measures in response to contextual/programmatic changes.
f. Maintain contingency fund for all projects to ensure ability to respond to changes.

3. Examine whether security risk management processes and protocols are applied equitably

Short-term

a. Have staff assess their own vulnerability based on their personal characteristics (see Appendix 6 for activity). Provide opportunities for this information to be discussed and/or to discuss informed consent, duty of care and personal responsibility.
b. Assess training practices – who is trained, how often and on what, against staff/volunteer knowledge.
c. Determine how capacity building is provided for national and international staff.
d. Assess policies, how they are applied across sites, and what lenses they apply (i.e. gender lens, anti-oppression lens etc).

Medium-term

e. Determine what areas have gaps and what type of training might be needed in each location.
f. Assess most appropriate way to acquire/provide this training (i.e. internal, in-country agency, consulting agency, with a network or forum group).
g. Develop a baseline of briefing and training information to be applied consistently across locations. Add country specific or issue specific briefing notes to each location document.

4. Develop a coordinated resource allocation and fundraising approach for programs

Short-term

a. Use risk level and context to:
    i. Determine organizational capacity for safe and secure projects in various regions;
    ii. Determine the associated security risk management funding requirements;
    iii. Decide on contingency fund allocation;
    iv. Develop fundraising proposals that reflect the level of resources that will be required for each program to ensure proposals clearly outline a budget for security management costs.

Medium-term

b. Utilize the risk level, mitigation workload and financial feasibility to determine the need for regional or local security advisors.
c. Determine the type of training required for the context and risks in each locale. Include these as direct costs in the funding proposals.

7.0 Conclusion

The evolving global risk landscape coupled with organizational responsibilities to protect stakeholders and assets, has encouraged many organizations to review their security risk management practices (HPN, 2010, p. 1). WUSC is one of these organizations who has recently completed an audit of their security management practices. This project was completed to complement the results of their audit and support WUSCs implementation of a more robust security risk management plan. In order to do so, literature was collected to gather information on smart practices in security risk management and semi-structured interviews were completed to gather relevant practical knowledge from the field. The research outlined frameworks, tools, processes and protocols, organizational culture and philosophies, as well as governance strategies. Global risk context was assessed along with common challenges for the implementation of security risk management. The goal was to provide a holistic overview on security risk management systems as well as the greater environment and context in which these systems are executed.

The discussion section was laid out strategically, beginning with foundational smart practices for developing an effective security risk management system and the context in which these practices would be nested. This was followed by tools, protocols and operational practices, where diverse strategies for success were presented. A challenges section beginning with the macro level – global context, to the micro level – individual perceptions and identities, was also provided to offer observations and lessons learned as found in the literature and the primary research. These typical contextual and internal challenges faced in international security risk management were posed to encourage individuals to examine their own perspectives and organizational preparedness.

The findings from the research informed the recommendations provided to WUSC. The goal was to offer recommendations and insights that would help WUSC affect positive change in their security risk management approach. Options provided overarching ideologies and considerations to assist WUSC with the transition of organizational culture, processes and practices. Additionally, it challenged the organization to consider current approaches and work toward more cohesion where possible. The goal was to provide WUSC with opportunities to evolve their practices within a shifting security risk landscape.

This report acknowledges the inherent complexity in developing and implementing security risk management systems for diverse international contexts. While the changing contexts can be seen as a challenge, a robust and flexible security risk management system helps to ensure organizations are meeting their duty of care and effectively enabling staff, volunteers and programs. While the above recommendations are based on the scope of this research, there are areas where additional research could benefit WUSC in the development of their security risk implementation process. Further research on how to address diverse individual vulnerabilities of staff and volunteers in security risk management protocols while avoiding discrimination and exclusion would be beneficial. This is a complex topic which has both legal and political implications that need further exploration.

References

Agard, K. (2011). *Leadership in non-profit organizations: A reference handbook.* Thousand Oaks, California: SAGE Publications Inc.

Bardach, E. (2012). *A practical guide for policy analysis.* Thousand Oaks, California: SAGE Publications Inc. Retrieved from https://www.ethz.ch/content/dam/ethz/special-interest/gess/cis/international-relations-dam/Teaching/cornerstone/Bardach.pdf

Berg, H. (2010). Risk Management: Procedures, methods and experiences. *Reliability: Theory & Applications #2*, 17(1), 79-95. Retrieved from http://ww.gnedenko-forum.org/Journal/2010/022010/RTA_2_2010-09.pdf

CBC News. (2016, January 17). Burkina Faso attacks: 6 Quebecers killed were on humanitarian trip. *CBC News.* Retrieved from http://www.cbc.ca/news/canada/montreal/burkina-faso-quebecers-killed-1.3407614

Chadwick, B., Gill, P., Stewart, K. & Treasure, E. (2008). Methods of data collection in qualitative research: Interviews and focus groups. *British Dental Journal.* 204, 291-295. doi:10.1038/bdj.2008.192

Childs, A. K. (2013). Cultural theory and acceptance-based security strategies for humanitarian aid workers. *Journal of Strategic Security*, (6)1, 64-72. doi: http://dx.doi.org/10.5038/1944-0472.6.1.6

Connors, T. (2012). *The volunteer management handbook: Leadership strategies for success* (2nd Ed.). Hoboken, New Jersey: John Wiley & Sons.

Committee of Sponsoring Organizations of the Treadway Commission. (2004). Enterprise risk management – integrated framework. Retrieved from https://www.coso.org/documents/Framework%20Reference%20Secured.pdf

Community Toolbox. (2016). Section 4. Collecting information about the problem. Retrieved from http://ctb.ku.edu/en/table-of-contents/assessment/assessing-community-needs-and-resources/collect-information/main

De Cordier, B. (2009) The 'humanitarian frontline', development and relief, and religion: what context, which threats and which opportunities? *Third World Quarterly*, 30(4), 663-684.

Desilets, A. (2016). *Security Management System. A changing landscape: Security at WUSC/Uniterra.* Ottawa, ON: Ad Management.

European Commission. (2004). 5. The logical framework approach. In *Aid delivery methods Volume 1 - Project cycle management guidelines*, pp. 57-94. Retrieved from https://ec.europa.eu/europeaid/sites/devco/files/methodology-aid-delivery-methods-project-cycle-management-200403_en.pdf

Gaul, A., Keegan, M., Lawrence, M., & Lya Ramos, M. (2006). *NGO Security: Does gender matter?* Unpublished master's thesis, The George Washington University, Washington, District of Columbia. Retrieved from https://www.alnap.org/pool/files/ngo-security-does-gender-matter-2006-40200.pdf

Gaskin, K. (n.d.). Risk toolkit: How to take care of risk in volunteering. *The Institute for Volunteerism Research and Volunteering England.* Retrieved from http://www.volunteermeath.ie/images/stories/risk_toolkit.pdf

Griffin, E. (2013). The ethical responsibilities of human rights NGOs. The International Journal of Not-for-Profit Law, 15(2), 5-23. Retrieved from http://www.icnl.org/research/journal/vol15iss2/art_2.html

Humanitarian Practice Network. (2017). About HPN. Retrieved from http://odihpn.org/about-hpn/

Humanitarian Practice Network. (2010). *Good practice review (Number 8). Operational security management in violent environments*. Retrieved from Overseas Development Institute website: http://odihpn.org/wp-content/uploads/2010/11/GPR_8_revised2.pdf

Humanitarian Outcomes. (2014). *Aid worker security report 2014. Unsafe passage: Road attacks and their impact on humanitarian operations.* Retrieved from The Aid Worker Security Database website: https://aidworkersecurity.org/sites/default/files/Aid%20Worker%20Security%20Report%202014.pdf

Humanitarian Outcomes. (2016). *Aid worker security report 2016 figures at a glance*. Retrieved from The Aid Worker Security Database website: https://aidworkersecurity.org/sites/default/files/HO_AidWorkerSecPreview_1015_G.PDF_.pdf

Humanitarian Outcomes. (n.d.). Blank risk register template. Retrieved from https://www.humanitarianoutcomes.org/ngos-and-risk

Humanitarian Outcomes. (n.d.). NGO risk management: Principles and promising practice handbook. Retrieved from https://www.humanitarianoutcomes.org/sites/default/files/ngo-risk_handbook.pdf

Institute for Economics and Peace. (2014). *Global peace index report. Measuring peace and assessing country risk.* Retrieved from Institute for Economics and Peace website: http://economicsandpeace.org/wp-content/uploads/2015/06/2014-Global-Peace-Index-REPORT_0-1.pdf

InterAction Security Unit. (n.d.a). *Security risk management NGO approach*. Retrieved from Interaction website:

https://www.interaction.org/sites/default/files/2581/NGO_SRM_APPROACH_FINAL_SAG_APPROVED.pdf

InterAction Security Unit. (n.d.b). Security collaboration best practices guide. Retrieved from https://acceptanceresearch.files.wordpress.com/2010/10/interaction_security-collaboration-best-practices-guide-201111.pdf

ISO. (2009). *Risk management – Principles and guidelines*. Geneva, Switzerland: ISO copyright office.

Lalonde, C. & Boiral, O. (2012). Managing risks through ISO 31000: A critical analysis. *Risk Management*, 14(4), 272–300. Retrieved from https://www.researchgate.net/publication/258820573_Lalonde_C_Boiral_O_2012_Managing_risks_through_ISO_31000_A_critical_analysis_Risk_Management_14_4_272-300

Law, J. (2016). *A dictionary of business and management (6th Ed.).* Online: Oxford University Press. Retrieved from http://www.oxfordreference.com.ezproxy.library.uvic.ca/view/10.1093/acref/9780199684984.001.0001/acref-9780199684984-e-4815

Leitch, M. (2010). ISO 31000:2009-The new international standard on risk management. *Risk Analysis*, 30(6), pp. 887-892. doi: 10.1111/j.1539-6924.2010.01397

Longhurst, R. (2016). Semi-structured interviews and focus groups. In N. Clifford, & G. Valentine (Eds.), *Key Methods in Geography* (3rd Ed., pp. 144-159). London, England: SAGE Publications.

Ministry of Citizenship and Immigration. (2009). *Taking risks the safe way: Risk management and insurance practices of Ontario's voluntary sector.* Retrieved from: http://www.citizenship.gov.on.ca/english/publications/docs/takingriskssafeway.pdf

Mitchell, T & Harris, K. (2012). Resilience: A risk management approach. Retrieved from https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/7552.pdf

Neuman, M. & Weissman,F. (n.d.). Humanitarian security in the age of risk management. Retrieved from http://msf-crash.org/livres/en/book/export/html/2327

Ng, W. (2014). A tool for everyone. Revelations from the "power flower". Retrieved from http://lgbtq2stoolkit.learningcommunity.ca/wp/wp-content/uploads/2014/12/flower-power-exercise.pdf

Norwegian Refugee Council. (2015). *Risk management toolkit in relation to counterterrorism measures*. Retrieved from Norwegian Refugee Council website: https://www.nrc.no/globalassets/pdf/reports/nrc-risk-management-tooolkit-2015.pdf

Persaud, C. (2012). *Gender and security. Guidelines for mainstreaming gender in security risk management.* Retrieved from European Interagency Security Forum website: http://reliefweb.int/sites/reliefweb.int/files/resources/EISF_GENDER_BriefingPaper.pdf

Pironti, J. (2012). Changing the mindset: Creating a risk-conscious and security-aware culture. *ISACA Journal*, 2, 1-7. Retrieved from https://www.isaca.org/Journal/archives/2012/Volume-2/Pages/Changing-the-Mind-set-Creating-a-Risk-conscious-and-Security-aware-Culture.aspx

Project Management Institute. (2013). *Standards for program management (3rd ed.).* Newtown Square, Pennsylvania: Project Management Institute. Retrieved from: https://goo.gl/qfn0o6

Stoddard, A., Harmer, A., Haver, K., Taylor, G., & Harvey, P. (2015). *The state of the humanitarian system*. Retrieved from Active Learning Network for Accountability and Performance in Humanitarian Action (ALNAP) website: http://www.alnap.org/resource/21036.aspx

Stoddard, A., Haver, K. & Czwarno, M. (2016). *NGOs and Risk: How international humanitarian actors manage uncertainty*. Retrieved from ALNAP website: http://www.alnap.org/resource/23095.aspx

The Association of Insurance and Risk Managers, Alarm & The Institute of Risk Management. (n.d.). *A structured approach to enterprise risk management and the requirements of ISO 31000*. Retrieved from Federation of European Risk Management Associations: http://www.ferma.eu/app/uploads/2011/10/a-structured-approach-to-erm.pdf

The Charity Commission. (2010). Charities and risk management – CC26. Retrieved from https://www.gov.uk/government/publications/charities-and-risk-management-cc26/charities-and-risk-management-cc26#understanding-the-basics-of-risk-management

The Charity Commission. (2011). *Protecting charities from harm: The compliance toolkit.* Retrieved from Government of the United Kingdom website: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/550682/Chapter_2_Summary.pdf

The Charity Commission. (2013). How to manage risks when working internationally. Retrieved from https://www.gov.uk/guidance/charities-how-to-manage-risks-when-working-internationally

Treasury Board of Canada Secretariat. (2016). *Guide to integrated risk management*. Retrieved from: http://www.tbs-sct.gc.ca/hgw-cgf/pol/rm-gr/girm-ggir/girm-ggir03-eng.asp#toc5

Uniterra [Web page]. (2016). Retrieved from http://uniterra.ca/en/uniterra/about-us

United Nations Somalia. (n.d.). *Risk management for NGOs*. Retrieved from http://so.one.un.org/content/dam/unct/somalia/docs/rmu/Risk%20Management%20For%20NGOs%20(0416).pdf

United Nations Environment Programme. (2011). *Environment and disaster risk: emerging perspectives*. Retrieved from UNEP Document Repository: http://wedocs.unep.org/bitstream/handle/20.500.11822/8624/env_vulnerability.pdf?sequence=3&isAllowed=y

Vesely, A. (2011). Theory and methodology of best practice research: A critical review of the current state. *Central European Journal of Public Policy*. 5(2), 98–117.

Volunteer Canada. (2012). *The screening handbook: Tools and resources for the voluntary sector*. Retrieved from http://volunteer.ca/content/2012-screening-handbook

Watt, A. (2014). 16. Risk management planning. In *Project Management*. Retrieved from https://opentextbc.ca/projectmanagement/chapter/chapter-16-risk-management-planning-project-management/

World Economic Forum. (2016). *The Global Risks Report 2016 (11th Ed.)*. Retrieved from World Economic Forum website: http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf

World Health Organization. (2017). HIV/AIDS data and statistics. Retrieved from http://www.who.int/hiv/data/en/

World Health Organization (2012). *International travel and health: Situation as on 1 January 2012*. Retrieved from World Health Organization website: http://who.int/ith/ITH_EN_2012_WEB_1.2.pdf

World Health Organization (2013). Road traffic mortality rate, 2013. Retrieved from http://gamapserver.who.int/mapLibrary/Files/Maps/Global_RoadTraffic_Mortality_2013.png

WUSC [Web page]. (2015). Retrieved from http://wusc.ca

Appendices

Appendix 1: Framework Tool, PESTLE Analysis Chart

Political	Factors may be altered by the government's influence on a country's infrastructure. This may include tax policy, employment laws, environmental regulations, trade restrictions, tariffs, reform and political stability. Charities may need to consider where a government does not want services or goods to be provided.
Economic	Factors include economic growth, interest rates, exchange rates, inflation, wage rates, working hours and cost of living. These factors may have major impacts on how charities operate and make decision.
Social	Factors include cultural aspects, health and safety consciousness, population growth rate and various demographics.
Technological	Factors include ecological and environmental aspects and available products and services. Charities may need to innovate, having considered the compatibility with their own technologies and whether they are transferable internationally.
Legal	Factors include any law which may impact on the charities' operations, including NGO regulation and criminal and terrorist legislation which will differ from country to country.
Environmental	Factors include an awareness of climate change or seasonal or terrain variations which may affect charities' service delivery methods.

(The Charity Commission, 2011, Tool 3: Risk Management)

Appendix 2: Framework Tool, Risk Register Template (*orientation altered to fit document*)

RISK REGISTER				
Approved by:				
Risk ID #		**1**	**2**	**3**
Risk Type		REPUTATIONAL	COMPLIANCE	LEGAL
Risk Category		CHILD PROTECTION	DONORS	HOST GOVERNMENT
Risk Description				
	Impact: 1 = Negligible 2 = Minor 3 = Moderate 4 = Severe 5 = Critical			
	Likelihood: 1 = Unlikely 2 = Moderately Likely 3 = Likely 4 = Very Likely 5 = Certain			
	Risk rating: (Impact x likelihood)			
Impact on Objectives	How did or could the risk impact objectives			
Mitigation Strategies	(List measures in place that would prevent or reduce this risk)			
Mitigation Outcomes	(Rate effectiveness of mitigation measures for each risk.)			
	Impact: 1 = Negligible 2 = Minor 3 = Moderate 4 = Severe 5 = Critical			
	Likelihood: 1 = Unlikely 2 = Moderately Likely 3 = Likely 4 = Very Likely 5 = Certain			
	Residual risk rating: (Determined by Impact x likelihood after mitigation)			
Program criticality score	PC1 = Critical (Lifesaving) PC2 = Important (Major impact) PC3 = Nonessential	PC1 = Critical (Lifesaving)	PC2 = Important (Major impact)	PC3 = Nonessential
Acceptable risk?	Yes/No (A risk rating of "High" can be accepted for PC 1-level activities)	Yes	Yes	No
Risk Owner (Lead)	(Individual responsible for risk)	STAFF NAME	STAFF NAME	STAFF NAME
Director Responsible	(Overall risk management owner)	DIRECTOR NAME	DIRECTOR NAME	DIRECTOR NAME
Timeline		Deadline	Deadline	deadline

(Humanitarian Outcomes, n.d., tools).

Appendix 3: Framework Tool, Risk Register Checklist

Communication & Consultation (10) – Ongoing Process	**Step**	**Key Concerns**	**Monitor & Review (11) – Ongoing Process**
• Has consideration been given to maintaining communication throughout the entire Risk Management Process? • Have stakeholders been identified? • Have decisions been made to communicate what and to whom? • Has a reporting and communication process been established? Linkages: Ongoing part of the Risk Management Process	1. Establishing the context (7)	• Have the organisation's objectives been taken into account? • Have stakeholders been identified? • Have the risk criteria been defined? • Have the risk assessment criteria been defined?	• Have the established procedures been followed? • Is there a requirement to escalate or de-escalate risks to the next level? Linkages: Ongoing part of the Risk Management Process
	2. Risk Assessment (8)	• What can go wrong, when and how? • What is the potential cost to time, money, and performance? • How likely is it to happen? • What are the impacts of each risk? • What is the source of the risk? • What can be done to reduce/control the risk?	
	3. Risk Analysis (8.2)	• Are there any existing controls? • Have the consequences of the risk been considered? • Has the likelihood criteria been applied? • Has the risk matrix been developed?	
	4. Risk Evaluation (8.3)	• Have the risks been compared against set criteria? • Have escalation and retention guidelines been developed? • Has a decision been made to treat the risks? • If yes, go to Step 3 • If no, continue to monitor and review the risks.	
	5. Risk Treatment (9)	• Have all treatment options been identified? • Have all options been assessed? • Have treatment plans been prepared and are they ready for implementation? • Have residual risks been analysed and evaluated? • Consider communication and consultation requirements.	

(United Nations Somalia, n.d., p. 23)

Appendix 4: Framework Tool, Risk Matrix Analysis Table

Likelihood	Impact: Negligible	Minor	Moderate	Severe	Critical
Very likely	Low	Medium	High	Very High	Unacceptable
Likely	Low	Medium	High	High	Very High
Moderately Likely	Very Low	Low	Medium	High	High
Unlikely	Very Low	Low	Low	Medium	Medium
Very Unlikely	Very Low	Very Low	Very Low	Low	Low

(Humanitarian Outcomes, n.d., Tools)

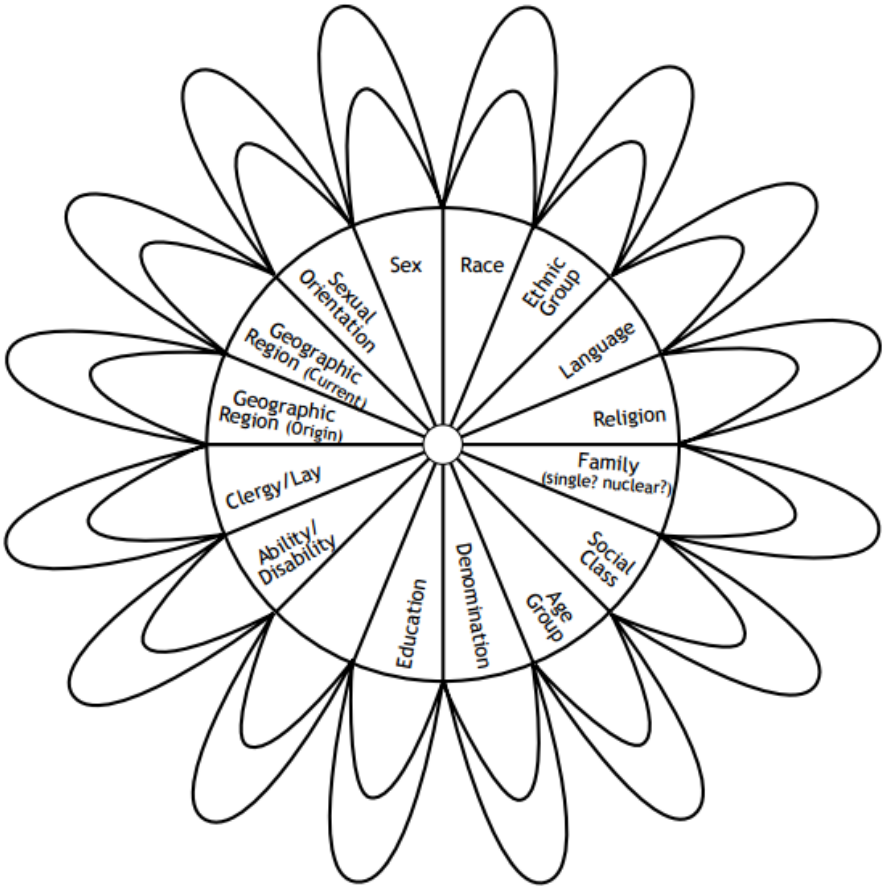
Appendix 5: Example Security Risk Matrix

UN Security Risk Matrix			
Impact	**Staff**	**Equipment / facilities**	**Activities**
Critical	Death and severe injury	Major loss	Cancellation
			Major delays Possible cancellation
Moderate	Injury	Some loss	Delays
Minor	Minor injuries	Possible damage, some loss	Limited delays
Negligible	Nil	Nil	Minor disruption

(Humanitarian Outcomes, n.d., Tools)

Appendix 6: Example of Personal Identity "Power Flower"

While the "Power Flower" has not been developed specifically for security, it was created by social change educators to help individuals learn about their identities and how it relates to social power dynamics (Ng, 2014, p. 53). The labels on the flower offer categories for social identity and individuals fill in the inner layer of petals related to their personal identifiers (Ng, 2014, p. 53). The outer petals can be filled in by the context specific dominant social identities (Ng, 2014, p. 53). This information can then be analyzed to consider how these identifiers might relate to power and risk in each context.



(Ng, 2014, p. 54).