Safety and Security of staff abroad. An analysis of international organizations working in non-industrialized countries.

By Matthias WAGNER

February 2014

MSc Dissertation in Risk Crisis and Disaster Management at University of Leicester

DOI: 10.13140/2.1.4968.8967

'The price of anything is the amount of life you exchange for it' **Thoreau, H.D. (1817 – 1862)**

Personal Statement and Acknowledgements

I am working in the field of security and risk management for almost 13 years. The experiences I made led to the idea to focus on security risk management and the comparison of private enterprises and (I)NGOs and (I)GOs in non-industrialized countries as well as the relation between SRM and security culture. I observed that more and more organizations and private enterprises are operating in the same theatre. Furthermore, I frequently recognize that the head offices of almost all international actors are underlining the importance of duty of care and security but it is not reflected in the field.

Due to my experiences I am aware of the fact, that I may be influenced due to my experience. Nevertheless, I had quite a lot of good supervision, critical discussions and the chance for self-reflection.

I would like to thank my University supervisor MSc Prof GCE LLS (DTLLS) FICPEM FEPS MIfL Gary Silver for his valuable and clear feedback.

Furthermore I want to thank Dana Hruby in particular. She always discussed my ideas in a constructive but critical way. She also kept a high level of pressure on me to keep track and to match my time planning. Without Dana, I would not be able to present the following piece of work.

Additionally I would like to thank the following colleagues and friend for their feedback:

Cornelia Schomaker – GIZ Crisis Manager and Head of Crisis Desk & COPE

Peter Lehmann – FDFA

David Napier – Goal ie

Euan Mackenzie – CAFOD/ Trocaire

H. Ebner – Securicon GmbH

Sascha Wichert – BMW

Lisa Reilly – EISF

Nathalie, Billy and Jacob for their advice

as well as all participating international non-governmental organizations, governmental organizations, political foundations, governmental installations as well as insurance companies and private business enterprises for their contributions and constructive discussions.

Abstract

Safety and Security of staff abroad. An analysis of international organizations working in non-industrialized countries. By Matthias Wagner

Natural disaster, acts of crime and terror as well as collapsing societies are threatening the world. This paper looks at how NGOs, governmental development agencies, humanitarian organizations and private companies are adjusting to complex contexts they are operating amidst. Organizations operating in these fragile environments become more and more exposed to risks deriving from political instability and even increasingly not only become the victims of violence, but also deliberate targets. This development signifies a substantial challenge to organizations and companies from industrialized countries operating in fragile contexts.

While those organizations or companies are legally responsible to ensure the safety and security of their staff they send overseas, they are often neither prepared for the challenging contexts nor do they have the necessary technical personnel and expertise to tackle present or emerging risks.

Therefore, this paper argues that the existence of an adequate risk management system is dependent on the development of a strong organizational culture attentive to security culture as sub-culture to ensure business continuity, minimize harm and fulfil social and legal responsibilities towards their employees.

In order to test the hypotheses quantitative and qualitative research on security risk management and security culture in the three aforementioned types of organizations was undertaken. Findings were visualized in a matrix to present the causality between security culture and security risk management along drivers of security culture and security risk management measures which leads to a certain degree of Humanitarian Risk Management. The results show, that the degree of Humanitarian Risk Management, is dependent on the degree of security culture and the level of security risk management. Furthermore there is positive causality between security culture and security risk management measures implemented by organizations.

Table of Contents

Table of Contents

Table of Figures

The dissertation also refers to figures developed during the assessment. These figures are available in Annex A.

Table of Tables

Abbreviations

(I)GO	(International) Governmental Organizations
(I)NGO	(International) Non-Governmental Organization
(I)O	(International) Organization
BCM	Business Continuity Management
CEO	Chief Executive Officer
CIMIC	Civil-Military-Cooperation
COIN	Counter Insurgency
COO	Chief Operation Officer
DfID	UK Department for International Development
EISF	European Interagency Security Forum
HPG	Humanitarian Policy Group
HQ	Headquarters
HR	Human Resources
HRE	Hibernation, Relocation, Evacuation
HRM	Humanitarian Risk Management
HRO	High Reliable Organization
ICRC	International Committee of the Red Cross and Red Crescent
IED	improvised explosive device
ILO	International Labour Organization
ISO	International Standardization Organization
NAT	Normal Accidents Theory
NIC	Non-Industrial Countries
ODI	Overseas Development Institute
OECD	Organization for Economic Cooperation and Development
PBE	Private Business Enterprise
PCA	Peace and Conflict Assessment
PiA	People in Aid
PR	Public Relations
PSC	Private Security Company
SMI	Security Management Initiative
SOP	Standard Operating Procedure
SRM	Security Risk Management
SRMS	Security Risk Management System
UK	United Kingdom
UN	United Nations
UNDSS	United Nations Department for Safety and Security
WHH	Welthungerhilfe (GAA – German Agra Action)
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH
NRC	Norwegian Refugee Council
DRC	Danish Refugee Council
BMW	Bayerische Motoren Werke
MAN	Maschinenfabrik Augsburg-Nürnberg
BASF	former ‚Badische Anilin- & Soda-Fabrik‘
ASI	Adam Smith International

Chapter 1 Introduction

Introduction

'We are angered by the senseless loss of life of dedicated and committed international servants who are trying to help those unfortunate enough to be caught up in war, civil conflict and poverty. In fact, the pendulum of UN security has now swung far past the mid-point and in many cases UN staff members are no longer seen as neutral providers of services but rather are considered as deliberate targets for terrorist attacks' (Bellamy, 2004: 1).

In 2011 the highest number of killed, kidnapped or wounded aid workers was recorded. The total number had increased significantly in comparison to the previous years (SMI, 2013; Stoddard et al, 2012, 2011; Van Brabant, 2010). Moreover, there is an increase of disasters and crisis worldwide And the number of deployed staff working in partner countries that present a serious security challenge increased, too (de Guttry, 2012). According to various studies the security situation became significantly more dangerous in the last decade in a number of regions (Schneiker, 2011: 628) although one has to admit, that most of the incidents were recorded in a small number of high risk countries (Stoddard et al, 2012, 2011; Van Brabant, 2010). Over time, a shift in the motivation of attacks occurred. Nowadays politically motivated attacks are increasing as well as the level of criminal acts against internationals in insecure environments (Van Brabant, 2010). But nevertheless, there is a slight decrease in security related incidents against aid workers in other contexts (non-high-risk settings). This could lead to the assumption that organizations improved and increased the application of better security management. The same applies for private business companies as well. One striking example was this: Following the French military intervention in Mali, the foreign jihadist group 'Signatories in Blood' with links to Al Qaida launched an attack against the Tiguentourine gas facility in January 2013. The group took over 850 civilians for hostage and killed thirty-nine foreign hostages. (Muhwezi et al, 2013).

Today, development, and humanitarian organizations as well as private business companies review their security risk management approaches, and increasingly discuss how to cope with security risks and how to prepare staff for overseas deployments. The basic approaches of security management and risk management strategies in industrialized countries are not fully applicable across contexts worldwide (Van Brabant, 2010). There is an urgent need for tailor-made approaches. Furthermore, approaches to protect civilians, e.g. beneficiaries, the local population, or the like may be quite different from those for the protection of aid workers (Van Brabant, 2010). Despite that, they may be similar to the approaches of private business companies, operating in the same environment.

Researchers often state that organizations miss out on dedicating time and resources to the issue of security. Security Management should not be an 'add-on or luxury for organizations' (Van Brabant, 2010: 3). Since the world financial crisis following the incidents in fall 2008, a number of mechanisms and controls in the field of financial risk management, such as BASEL I – III (a set of minimum capital requirements for banks) were implemented. In consequence, organizations should spend the same attention to the safety and security of staff. Van Brabant (2010) argues that the high level of insecurity organizations in NIC countries are exposed to is gravely hindering the access to certain regions and to stay in those regions, especially in high risk areas.

In general the host nation government takes the responsibility to protect civilians in their country (Van Brabant, 2010). Especially in post-conflict countries and high risk countries their overall capacity to do just that is very low. They are not able to keep law and order at an acceptable level where the safety and security of humans can be protected. Additionally host nation governments cannot take over the responsibility for duty of care for staff employed by (international) governmental or non-governmental organizations as well as private business enterprises (PBE). There is a necessity for the organizations to ensure duty of care according to their home country regulations as well as their understanding of values and responsibilities. As a result, the organizations need to implement measures to meet this responsibility (Van Brabant, 2010). The concepts of corporate security, generally

based on travel security, are insufficient to operate in insecure environments. Security risk management plays a much more significant role in insecure environments (Blyth, 2008: 6). One could even state that the complexity of these difficult environments, legal requirements as well as the general sense of social responsibility and duty of care towards an organization's employees therefore requires additional measures (de Guttry, 2012; UN, 1966; EU, 2000).

Aims and objectives of the dissertation

Nowadays, different sectors, such as governmental development agencies, non-governmental organizations (NGO), humanitarian actors, private enterprises and international military forces are operating in the same kind of 'theatre' at the same time. The research intends to discover what organizations like (international) governmental organizations ((I)GOs), (international) non-governmental organizations ((I)NGOs), humanitarian organizations, political foundations and private business enterprises (PBE) are doing to ensure the safety and security of their staff working in non-industrialized countries. Thus, one objective of this dissertation is to discover, whether the focus group organizations and enterprises fulfil their obligation in regards to duty of care or whether they are even going beyond their obligations and if so why. This study has a second aim: Analysing the differences or similarities between the different risk management systems of selected focus groups and determining whether the concepts of *security risk culture and 'just culture'* influence those systems. The intensity of Security Risk Management (SRM) systems resulting from those specific cultural traits will herein be called Humanitarian Risk Management (HRM).

The argumentation in this dissertation is assuming that the level of HRM depends on the level of security culture and SRM characteristics. General speaking: weak drivers of a security culture lead to a weak security culture in general which then leads to an ailing SRM. It is assumed that there is a causal link between security culture and SRM characteristics. As a result, the importance of security, the commitment by top

management and the basis of truth are seen to be the most essential drivers for a healthy security culture and thus a strong HRM concept.

To provide a framework for the research it is essential to define the main terms used.

Definitions:

Non-industrialized countries (NIC – countries)

The term '*non-industrialized countries'* (NIC) in this paper describe various contexts that cannot be categorized as industrialized countries. The term does not demand that non-industrialized countries reflect a state with a low level of economic industrialization. Moreover, organizations and enterprises from industrialized countries engage in NIC contexts such as developing countries, development countries, fragile states, high risk countries or failed states that are characterized by open armed conflicts or war, a lack of civil order and/ or the presence of groups aiming to fight the current political system with the tactics, techniques and procedures of asymmetric warfare. The term is introduced to describe a context which differs greatly from the context and framework in industrialized countries with a focus on security and good governance. The criteria for NIC countries are (1) living condition, (2) level of law and order, (3) stability of the political system, (4) level of democracy, (5) level of transparency, (6) level of corruption, (7) capabilities of security forces and lastly (8) security situation. Another factor for countries to be seen as NIC is a higher likelihood that the life and physical integrity of expatriates or host nation staff working for the organizations defined above are threatened and require measures to ensure the safety and security of staff which would not be necessary in industrialized countries. This leads to the necessity of a tailor made SRM approach, which in this research is called Humanitarian Risk Management.

Security Risk Management (SRM)

First of all SRM is used by various organizations and enterprises to cope with certain security situations, such as kidnappings or terror attacks and to ensure the safety and security of staff. Nevertheless, SRM is often based on an isolated process to identify and assess risk and to cope with uncertainty while implementing contingency measures or

to plan for emergencies. Michael Blyth (2008) characterized SRM as the management of security with a focus on business project management and an approach capitalizing on protection and deterrence. Furthermore SRM often focusses on a protection or a deterrence strategy and is based on travel security approaches.

Humanitarian Risk Management (HRM)

HRM is employing a holistic approach, considering the context of SRM including the cultural framework and aims to provide a model to ensure safe and secure working conditions for staff working overseas. It also considers the various human and non-human drivers of a security culture as well as activities and procedures of SRM. The HRM model consists of selected instruments, processes and good practices from different SRM concepts such as 'Corporate Security' (Blyth, 2008; Borodzicz, 2005; Vellani, 2009) or 'SRM in insecure environments' (Van Brabant, 2000, 2001, 2010). Furthermore, HRM is characterised by a combination of the minimum standards from People in Aid, VENRO, Irish Aid and insurance companies (Irish Aid, 2013; People in Aid, 2003; Unfallkasse des Bundes, 2008; VENRO, 2003) (figure 73 Annex A).

The term *humanitarian* does not imply that it is only applicable for humanitarian organizations or is only based on humanitarian principles (humanity, neutrality, impartiality, independence) (ICRC, 2004; OCHA, 2012). However, the HRM model and the people working in HRM are taking humanitarian principles into consideration to enable organizations to reach their goals. E.g. HRM is independent and neutral and risk management advisors following the approach are talking to all stakeholders but do not work together with all stakeholders. Moreover, the roots stem from (security) risk management approaches used by humanitarian agencies such as the ICRC in 2003 in Iraq (ICRC, 2004). HRM distinguishes itself from SRM by resorting to a strategic acceptance approach and the analysis of activities according to the do-no-harm approach (Anderson, 1999). The use of the do-no-harm approach can also be applied in PBEs. It even supports business success.

Duty of care

Duty of care describes an obligation of employers towards employees to protect them against foreseeable risks which may harm their life and physical integrity or impact healthy working conditions (BGB, 2013a, 2013b, 2013c; BMJ, 2012; Claus, 2009; Corporate Manslaughter and Corporate Homicide Act, 2007; de Guttry, 2012; ICJ, 1949; Unfallkasse des Bundes, 2008). Therefore it is the duty of employers to assess the working environment and to identify potential risks. Furthermore, risk mitigation measures should be applied to protect the life and physical integrity of employees or to ensure healthy working conditions. It does not only apply for safety issues (work safety, health) in home countries but also for security issues (acts of violence threatening the physical and psychological integrity of staff or values) for organizations deploying staff overseas (Van Brabant, 2010). This fact is essential for the evaluation of a SRM system or model and is therefore an essential driver for a strong security culture contextualized in a *just cultural environment* which is therefore of great importance for this research project (Dekker, 2008).

Just Culture

Just culture is one driver of security culture. James Reason identified four interlinked subcultures contributing to a safety or security culture. Safety can be used interchangeably with security in the argumentation. These subcultures are reporting culture, just culture, flexible culture and learning culture (Reason, 1997: 196). In general, 'culture is not what an organization *has,* rather than something what an organization *is'* (Reason, 1997: 220, original emphasis). It is characterized by a reporting system which supports a confidential (anonymous) reporting of all errors, incidents and near miss incidents without fear (blame-free), the follow up of incidents, the empowerment of staff on the ground, and the personal accountability of staff for safety and/or security (Lekka, 2011, Dekker, 2012). Dekker (2008) adds that there must be a clear statement about accountability available to the group of reporters. If there is a need for an official investigation (e.g. the commitment of a crime) the identity may me disclosed for trials. A no-fault/ no-blame approach to a certain extent is essential for a successful development of a just culture (Bohne and Peruzzi, 2010; Cohen, 2000; Cooper, 2000; Donahue and Tuohy,

2006; Douglas, 1992, 1994; Guldenmund, 2000; Hader, 2006; Harper and Helmreich, 2011; Helmreich, 2000; IOM, 1999; Johnston, 2005; Leape and Berrick, 1999; Lekka, 2011; Provera et al., 2008; Reason, 2000).

Contrary to this statement, Dekker (2008) cites Gain (2004) who argues at a different level. Gain (2004: viii, original emphasis) states that a 'no-blame' approach is neither feasible nor desirable. Most people desire some level of accountability when an error occurs. Pellegrino supports the statement and adds that a '*blame-free system with an absence of personal accountability is wrong*' (2004: viii, original emphasis). Dekker (2008: 177) underlines that it is not enough to draw a line between acceptable and non-acceptable behaviour but it is necessary to identify who draws the line. He further states that if there is no line, 'anything goes' – so why should errors be reported? Marx (2001: 3) argues that it is about the balancing of the need to learn from errors and the need to take disciplinary action. Dekker (2008) puts that in other words stating that 'just culture is meant to balance learning from incidents with accountability for their consequences'. He clearly argues that the accountability of people and blaming people are two different things. This supports the argument that SRM or HRM cannot be seen as isolated concepts. Moreover it shows the interactive complexity of the topic of SRM/ HRM, supporting the argument that sit is tightly coupled with cultural factors and concepts. This fact underlines the importance of the consideration of cultural aspects for the analysis of SRM.

<u>High Reliable Organizations (HRO)</u>

The just cultural approach was first identified in the discussion about HROs to foster an error-free environment. Charles Perrow's Normal Accident Theory (NAT) was the starting point for the development of a just cultural approach. He argues that accidents are not preventable due to interactive complexity and tightly coupling of a system (Perrow, 1999: 4-6). During the past ten years, organizations learned a lot and changed from being purely profit oriented, hierarchical organizations to organizations with a focus on social responsibility, safety culture and value management. Organizations seem to reach a state of high reliability and safety objectives (Lekka, 2011). In general, a HRO is characterized as (nearly) error-free organization, tightly coupled and with a high level of interactive

complexity (Perrow, 1999). Examples for HROs are nuclear power plants, chemical companies or air traffic controller. Weik and Sudcliffe (2007) argued that the characteristics for HROs are more specific as defined by Perrow. Weik and Sudcliffe (2007) defined organizations working under difficult circumstances with statistically less errors and incidents as high reliable.

Interactive complexity as defined by Perrow (1999) can also include system complexity. Therefore the term HRO is not limited to interactive technical complex and tightly coupled organizations such as nuclear power plants but also includes system complexity. To achieve a state of high reliability it is essential to take certain factors and developments into consideration and to foster just culture. (Lekka 2011: v).

The structure of the dissertation

This research comprises of 4 chapters. The literature review (chapter 2) focusses on security culture as a framework for SRM. Following this, the dissertation will elaborate on research methods used, focussing on the techniques of semi-structured interviews and online questionnaires (chapter 3). Chapter four will then represent the findings from the online questionnaire, interviews considering available data from the literature and discusses the argumentation with the findings. Finally, the main findings are summed up and suggestions are made for further research (chapter 5).

Chapter 2 Literature Review

The review of the literature starts with a review of literature on security and just culture. Late literature argues that organizational culture influences security culture and thus the concept of security risk management and implemented strategies as well as measures. The last section reviews SRM in insecure environments, leading over to the particularities of Humanitarian Risk Management.

Security and Just Culture

In 1939 Lewin et al (1939a) created the term ‘organizational climate’ which can be seen as the beginning of the discussion about organizational culture. Nevertheless, the

beginning of discussions about culture was focused on small rather than globalized groups (Prasad and Prasad, 2009: 129). In the mid-1970s researchers started framing the concept of organizational climate and later national culture (Morgan, 1986). Issues related to organizational culture were discussed for the first time as a by-product of the research on the 'Japanese economic miracle' (Prasad and Prasad, 2009: 129). Ashkanasy et al (2000) integrated methods from different sciences into the discussion about the definition of culture. In 1979 Pettigrew introduced the term organizational culture. Nonetheless, there is no unified definition of culture (Bellot, 2011).

Even though there is no clear definition, 'organizational culture exists' (Bellot, 2011: 30). It is widely accepted that organizational culture is focussing on the understanding of human values (Parker, 2000: 1). Culture is defined by people, their beliefs, behaviour, values and world views. Culture '*is socially constructed and the product of groups, based on shared experiences. Each organizational culture is unique and subject to continual change*' (Bellot, 2011: 30). It can be influenced or is constructed by its members who share the same beliefs, values and ideals (Bellot, 2011; Martin and Siel, 1983). Culture therefore is intended to improve the organizational output and create an environment based on the overall organizational values. It is an undefined set of normative values which can vary between organizations and their needs. Additionally it contains subcultures (just culture, learning culture etc.) contributing to organizational culture (Parker, 2000; Prasad and Prasad, 2009). There is no static set of subcultures which can be defined as necessary for an organizational culture; this depends on the organization and its members and what set of subcultures they deem necessary based on the same values and beliefs (Deitelhoff et al, 2010).

This dissertation focuses on security culture; a subculture which is closely associated with organizational culture and can strongly influence it. Additionally, a weak security culture may also hinder change (Ruighaver et al, 2007, Nosworthy, 2000). As it is noted in the relevant literature, security culture stems from legal obligations, and results in social and corporate responsibility and the importance of security in an organization. Borodzicz and many others argue that a risk, safety or security culture operates at an

organizational rather than a decentralized level (Borodzicz, 2005; Pidgeon, 1991; Waring and Glendon, 1998). The security culture at organizational level and therefore the individual or group behaviours in organizations are influenced by and dependent on the context people are working in (Mowday and Sutton, 1993). Ruighaver used the eight overarching descriptive culture dimensions, used by Detert et al in 2000 to provide an approach on how organizational culture and security culture are linked and defined.

The first dimension, 'the basis of truth and rationality', is about how important security is perceived by staff and the organization itself. It focuses on the perception of security at different levels in an organization and their importance in reality. The second dimension that is 'the nature of time and time horizon' focuses on the time horizon of security approaches and security planning. It describes whether an organization focuses on long-term security planning or assumes an *ad-hoc incident reaction* approach. The third dimension that of 'motivation' discusses the motivation of employees to participate and accept security in an organization. This dimension includes a discussion about the accountability of employees and includes a just culture approach to some extent. The fourth dimension discusses the willingness and the ability to 'change' versus a stability approach. Most organizations lack a security change approach while security change management and the continuous adoption of innovative approaches towards security should be a continuous process in daily base operations (Ruighaver et al, 2007). The fifth dimension, 'orientation to work' describes the concept of participation and ownership of employees in regards to security and the feeling of employees towards security. Employees participating in the discussion about security tend to feel less restricted. Therefore risk education of employees is an important factor towards providing continuous orientation to them. It fosters the perception of participation in security and ownership (Koh et al, 2005 cited in Ruighaver, 2007). The sixth dimension discusses the approaches of 'isolation versus collaboration' in security policies and processes. Often these policies and processes are handled by single individuals or small groups in organizations rather than in a collaborative manner. Being isolated from the process of risk assessment or the implementation of a security policy may negatively impact the motivation of employees and

the acceptance of security. The seventh dimension discusses the concept of security governance, that is, the level of responsibility in security decision making and the level of control by the organization as well as the accountability of security decision-makers. It means that the orientation of risk management depends on the level of participation and support from the upper level of the organization's management hierarchy. The eighth and final dimension examines the 'internal and external focuses' on security. According to Ruighaver (2007), most organizations focus on passing security audits and meeting standards rather than improving security and considering internal requirements. The eighth dimension argues in favour of a just cultural environment and the balance between internal (context and organization specific requirements) and external (standards, audits etc.) influencing factors (Detert et al, 2000; Ruighaver et al, 2007). Detert et al illustrate a theoretical framework that links the eight dimensions to a set of values and beliefs that represent the back bone of culture.

In this sense, it can be argued that culture as well as security culture is unique in each organization (Ruighaver et al, 2007) as it is dependent on all aforementioned parameters. In general, different organizations need different degrees of security but they may share the same approaches and concepts to security (Bellot, 2011: 57). Achieving an adequate degree of security for an organization is important as long as its employees and top management believe that doing so is important (Bellot, 2011). The importance of security in an organization is a crucial and essential factor for a strong security culture. The acceptance of security by employees is very much dependent on the motivation, the level of participation, the ownership of employees and the level of trust towards the management (Bellot, 2011). This means that, if both the management places a strong focus on security and carries out its responsibilities accordingly, and employees are invited to participate in security management, this will be accepted by the latter. Ruighaver (2007) argues that employees in organizations with high security standards more often accept limitations than employees in organizations with low security standards. Employees tend to be resentful of security restrictions and as a result are less likely to accept risk management systems. Bellot states '*Employees feel less restricted when they are motivated and feel responsible*

for security' (Bellot, 2011: 60; original emphasis). According to Koh et al (2009), the of the manner in which security culture as manifests itself as an organizational subculture depends on multiple factors, such as the following: The higher the responsiveness of an organization to suggestions of employees, the more frequently security is being discussed in an organization. And the more the responsibility for security is shared amongst stakeholders, the higher the acceptance of limitations is.

In its 'Humanitarian Principles', OECD (2012) recommended the establishment and improvement of a risk culture of organizations, specifically in fragile and transitional contexts. As it is explained, organizations should communicate expectations to members of staff so as to increase accountability, implement and develop specific security risk management frameworks for fragile and transitional contexts and set up special units for high risk environments. OECD (2012) describes four risk categories to be taken into account 'contextual', 'institutional', 'programmatic' and 'personnel risks' in fragile and transitional contexts when trying to identify risks and foster the organizational responsibility and ultimately culture in organizations. As it is to be expected though, in practice, attempts to foster just such an all-embracing culture are fraught with difficulty.

Another important factor for a proactive and adequate security culture is the level of incident reporting, the blame-free approach to reporting and learning in the organization or enterprise. Pidgeon and O'Leary (2000) identify two major reasons why organisations fail in doing so. The first one is simply (non)-communication and/or the overall lack of information and proactive discussion about security. The second reason is that organizations tend to blame individuals or groups instead of analysing failures and incidents. A blame culture or the lack of truth is dependent on organizational politics and corporate governance and has a significant impact on the level of learning in an organization or enterprise. Often conflicting messages are communicated in organizations. They significantly influence the basis of truth. On the one hand, the management communicates that security is important but on the other hand they are not willing to allocate resources (Bellot, 2011). A meaningful example can be found in many organizations where a policy is available but not implemented at operational level.

Deitelhoff and Wolf (2010) argue that employees of an organization must share the same beliefs in order to have the same basis of truth. Contrary to this argument Bellot states that it is not enough to share the same beliefs, but it is also important to evaluate and manage the same basis of truth. This means that the perception of the importance of security from employees and the management needs to be balanced with reality (Bellot, 2011).

Many (small) organizations are reactive and focus on short-term approaches towards security rather than long-term commitment and strategic management (identified in big organizations with a high level of security) (Bellot, 2011: 58). Furthermore organizations tend to delegate the responsibility for security to individuals or small groups, often junior advisors or non-specialized members of staff. Bellot underlines that this approach is not acceptable. It should be discussed rather in a larger framework to motivate employees and to influence the behaviour of employees positively. Another example that illustrates that especially small private business consultancies operating in the field of development aid neglect security due to short-term approaches towards security and limited resources.. Their main objective is the generation of profit. The ignorance of personnel security can lead to a significant collapse of an organization's posture (Bellot, 2011: 60). Support by the management is a significant driver for the development of an organization's security culture (Knapp et al, 2006).

One sub-culture contributing to organizational culture and closely associated with security culture is the so called '*just culture*' essentially important to the analyses of whether security culture supports HRM or not (Dekker, 2012). Reason identifies four interlinked subcultures contributing to a security and safety culture. These subcultures are reporting culture, just culture, flexible culture and learning culture (Hofstede, 1994; Reason, 1997: 196). Just culture is characterized by a reporting system which supports a confidential (anonymous) reporting of all errors, incidents and near miss incidents without fear (blame-free), the follow up of incidents, the empowerment of staff on the ground, and the personal accountability of staff for safety and security (Dekker, 2012; Lekka, 2011). All available definitions about just culture make a separation between acceptable and

unacceptable behaviour (Dekker, 2012: 15). In these cases, one finds that there is often an approach or culture of blame; a search for the one individual who is responsible and who is exposed to be blamed. There is often no real analysis of what is acceptable and of the extent to which the system itself contributed to an error or failure (Dekker, 2012; Lekka, 2011). Dekker argues that '*wilful violation of individuals is not acceptable; an honest mistake is*' (2012: 41). Furthermore, most organizations are lacking an accountability policy and a definition of what constitutes acceptable behaviour and what not. If there is no line between acceptable and non-acceptable behaviour, anything goes (Dekker, 2012: 16), and it is easy understood, such an approach has a negative impact on people's morale, the credibility of the management, the ability to learn from failure (Dekker, 2012: 16), the commitment to the organization and job satisfaction (Dekker 2012: 78). Organizational top management plays a major role in the implementation of a just cultural environment. CEO's are obliged to undertake good corporate governance and duty of care (ArbSchG, 1996; BGB, 2013a, 2013b, 2013c; BMJ, 2012). But they are often too far away from reality, due to a lack of information and/or a lack of emotional concern (Toft and Reynolds, 2006).

Just Culture is therefore about individuals in systems rather than individuals and systems. The individual is seen as a symptom and '*human error is an effect of trouble deeper inside the system*' (Dekker, 2012: 80). An organizational security (risk) culture sets the standards for good corporate governance and enables the management to minimize errors and failures due to the implementation of adequate SRM approaches. In this sense, security culture is crucial for SRM. Nevertheless SRM in corporate security departments often capitalizes on travel security, protection and deterrence approaches to cope with risks.

The next paragraph is dedicated to the discussion of research on SRM and its characteristics. The implemented SRM systems in the field are dependent on the security risk culture, believes of people, the size of the organization, the dependence on insurance and governmental rules and regulations as well as the ability to contact and to interact with local stakeholders and to build relationships and networks (Schneiker, 2011: 637).

Security Risk Management (SRM)

The beginning of the debate about risk and security and the management of risk can be traced back to Aristotle who stated that *'it must be expected that something unexpected will happen' (*Aristotle, undated cited in Barnes, 1991). In 1995 Nalla et al first researched curricula requirements for security professionals complementing the military/ law enforcement approach with business skills. He further identified that security professionals need to be able to deal with security screening; site security and site protection; PR, IT security as well as government security and information security (Borodzicz, 2005; Nalla et al, 1995).

In 1996 the 'People in Aid' (PiA) project first considered the security and well-being of members of staff in principle seven of their publication *'Code of Best Practice in the Management and Support of Aid Personnel'* (People in Aid, 1997, 2003). PiA stated '*that an organization can only value itself as highly as it values its people*' (Van Brabant, 1996: 17). Between 1997 and 2003 organizations significantly improved their approach on dealing with security challenges. 'The HPN Good Practice Review No. 8 discussed the characteristics of SRM including processes and procedures of which risk assessment is one of the core elements (Van Brabant, 2000). In 2001 Konraad van Brabant and the Humanitarian Policy Group published the HPN Report No. 9, which was titled '*Mainstreaming the Operational Management of Safety and Security'* (ODI, 2001). The report was based on the consultation among twenty Non-Governmental Organizations and a comparative review of their perception of their safety and security management. Van Brabant reviewed and discussed several factors contributing to a security culture, such as the commitment of top management or the importance of security in the organizations. Nevertheless, he did not explicitly focus on security culture. Furthermore van Brabant designed a security management framework based on the results from the review of those twenty organizations. He first outlined a 'cycle of security' considering the context, security strategies, such as acceptance, protection and deterrence as well as a small set of standard operating procedures, emergency planning and post incident procedures. Quite differently to van Brabant and his interpretation of security management, Borodzicz (2005)

focused in his research on contingency planning, crisis management and crisis response. Nevertheless, at this point of time no further research was available for SRM in aid agencies. In 2003 PiA published a revised Code of Best Practice describing eight indicators of health, safety and security, that is the availability of a written policy; program plans including a written risk assessment; pre-deployment health checks as well as risk briefings; evacuation procedures; reporting of accidents and incidents: rest and recreation; post-deployment debriefings and organizational support as well as health clearance and immunisation (People in Aid, 2003).

The indicators defined by PiA can also be found in van Brabant's SRM framework. Sennewald and Blyth also supported the statement outlined by PiA and van Brabant that a proper risk assessment is essential for security risk management (Blyth, 2008; Sennewald, 2003). All authors defined the process of risk assessment with the steps of risk identification and the analysis of risks. In 2008 Blyth, a former military officer, published a comprehensive handbook on security management for corporate security staff with a focus on business project management and an approach capitalizing on protection and deterrence in 2008 (Blyth, 2008). In there, he covered most of the 'hard-factor' characteristics of van Brabant's framework, such as standard operating procedures, emergency planning, evacuation planning and crisis management. However, he did not consider the 'soft-factor' characteristics, such as context analysis or the acceptance approach as defined by van Brabant or the International Committee of the Red Cross (ICRC). In addition, they discussed the first time components of a security culture and their dependence on SRM (Van Brabant, 2010; ICRC, 2004). Ast (2010) defined a best practice security management for private enterprises based on travel tracking and intelligence. He further defined SRM with crisis planning, communication, lessons learned, reporting, pre-deployment and security awareness training tailored to the context of business as well as necessary networking with other possible stakeholders and actors. Nevertheless, Ast does not consider security culture as a crucial element to foster SRM.

Contrary to the suggestions made by Van Brabant, humanitarian actors, such as ICRC in Iraq in 2003 , almost solely focus on the acceptance approach at strategic and

operational level, valuing local ownership, good relations and service provision to the different stakeholders and beneficiaries the most (ICRC, 2004). In this context, they defined their SRM strategy through their identification with and the adherence to humanitarian principles (Schneiker, 2011). Nowadays the complexity of contexts and the fact that neutral actors increasingly become targets nevertheless leads to an inconsistent adherence to humanitarian principles at an organizational level. The application of humanitarian principles was believed to be a crucial factor to being safe in insecure environments. But there is only a small number of organizations left that apply humanitarian principles as stand-alone SRM in a strict manner (Schneiker, 2011). The increasingly dangerous contexts force all kinds of organizations to consider other strategies rather than acceptance, in order to ensure safety and security of staff and operations, such as applying extraordinary measures (Vaughn, 2009: 278). Schneiker states that the use of an acceptance strategy alone is not adequate anymore (2011: 634). Van Brabant supports Schneiker's argument and states that acceptance alone is not liable (2010: 55). The use of the acceptance strategy based on the identity of organizations became impossible in these contexts (Schneiker, 2011; Stoddard, 2013). But some actors in the aid sector still reject security measures due to their belief they could question their identity and beliefs in humanitarian principles (Britton, 1997: 22; Edwards 1997: 241). The number of discussions regarding the characteristics of SRM has risen over the past years (Barnett and Weiss, 2008).

The OECD (2012a) uses similar characteristics for Security Management focussing on risk assessment, contingency planning, crisis response and crisis management, reporting and post incident reviews. The threshold is often defined by the balance of monetary costs and benefits. Despite that, in 2012 OECD identified that there is a lack of risk assessment frameworks for operations in fragile states (2012a:48).

Projects may be closed prior to completion which is resulting in lost projects costs for donors or the organization if there is no professional SRM in place (Blyth, 2008). A professional SRM system is understood as a tool to enter and remain in danger zones (Van Brabant, 2001: 1-2). OECD (2012a) underlines the importance of corporate governance

related to security risk management. Sufficient and appropriate measures require an organization-wide SRM by establishing clear lines of management and governance responsibility. As an example, having a policy in place makes security risk management a corporate responsibility rather than an operational issue and reduces inconsistencies in operational practices (Van Brabant, 2001). OECD demands to implement proper tools for the identification, the evaluation and monitoring of key risks (OECD, 2012a: 68). The engagement in non-industrial contexts, specifically in fragile and transitional contexts, as well as the acceptance of risks requires the backing of political decision makers, incentive structures, sufficient staff capacity and appropriate institutional processes and control measures (OECD, 2012a: 3). Risk Management is an investment in the present and future (Roper, 1999: 4). It cannot protect everything but the most essential assets first (Roper, 1999: 9). An organization working in a high insecure environment may only focus on emergency plans, neglecting the identification and assessment of potential risks. In fact critical risks may not be identified, considered and treated and therefore lead to significant or catastrophic consequences (Borodzicz, 2005: 23). Van Brabant (2001) described the lack of interest, right periodization and commitment by the top management to the concept of SRM as well as the negligence of the situation and of the acceptance of risks as influencing factors to this. Furthermore he argued that a lack of organizational culture significantly hinders the improvement of effective SRM. Argumentations against prioritising and investing in better safety and security delay and/or hinder improvements in security (Van Brabant, 2001: 1). In consequence SRM is only effective if the top-level management is committed to following up on recommendations (Van Brabant, 2001: 2). The top management or the CEOs have a crucial and essential role in the implementation of security risk management as well as a security risk culture in the organization. One respondent stated that '*safety and security does not start with the employee you recruit, it starts with the type of CEO you recruit'* (Van Brabant, 2001: 2, original emphasis). However, not only the will in organizations is crucial to implement SRM. Rather, insurance companies are putting enormous pressure on organizations and demand the implementation of risk mitigation measures.

From a legal perspective many insurance companies question what prevention measures organizations and companies apply (Borodzicz, 2005). Schneiker (2011:637) argues that there is no pressure from such insurance companies to implement proper risk management measures in organizations working overseas, as in the case of German insurance companies. A reason for Schneikers argument may be the fact, that German organizations under the umbrella of the Federal Accident Insurance always compensate damages and loss, except gross negligence and crime (HDI, 2013). In general there is a difference between federal accident insurance companies and private insurance companies. While federal accident insurances cover all costs regardless of nature and outcome, private insurance companies enforce a security concept. An illustrative example can be found in the fact that in 2007 there were more than 31,000 registered legal proceedings related to the negligence of corporate duty of care and compensation (Diedenhofen, 2008).

In addition to the legal obligations and duty of care SRM can also have positive impacts. Beside the obligation to ensure the safety and security of staff, security contributes to enterprise and corporate profits by reducing or eliminating preventable losses (Sennewald, 2003: 20). Ale's system theory provides a metaphor for a Humanitarian Risk Management model. According to this system, everything in our life can be described as a system. People and machines rarely, if ever, operate in isolation (Ale, 2009). Systems are dependent on sub-systems which are tightly intertwined (Ale, 2009; Reason, 1997). Ale's system theory is taking into account human factors as well as technology. He argues that there is always an input to a system, resulting in a certain output. The things happening in between are perceived as a *black box*. Especially in insecure environments it is essential to apply an adequate approach to manage risks. Organizations and companies operating in NIC countries are facing significant complex contexts and dynamic situations. Organizations and companies often claim to operate nearly error and fault free to deliver the services they are tasked to do or to make profits. They claim to be an error-free, 'high reliable organization' (Reason, 1997).

Chapter 3 Research Methods

The research project compares different approaches towards SRM in organizations and enterprises deploying staff overseas. It analyzes the relationship between security cultures in organizations and the implemented SRM processes and activities. Chapter 3 gives detailed information about the design of the research project, sampling procedures, data gathering tools and challenges which appeared during the research. In addition it describes the method of evaluation and interpretation of the data. The chapter will provide transparent information to the reader on how data was gathered and errors were handled. It explains why certain techniques, such as semi-structured interviews as well as an online survey/ questionnaire were used for data collection. The first paragraph gives an overview about the research design, followed by the description about data gathering tools used in the research. The next paragraph explains the techniques used to analyse the data followed by information on sampling procedures and the process of identification of focus groups. Finally challenges will be pointed out which occurred during the research project.

Research Design and techniques of analysis

Mixed methods were used for this research project (Bryman, 2009; Creswell and Plan Clark, 2007). The following paragraph discusses why the researcher decided to use an online survey/ questionnaire and semi-structured interviews for data gathering. All gathered data was triangulated between primary data from the online survey, semi-structured interviews and data available from literature as described by Porter (Porter, 1994 cited in Module 3: 5-32). Data from the online questionnaire (quantitative and qualitative) were complemented with data from semi-structured interviews (qualitative) (Prasad and Prasad, 2009).

The overall research design used in the project is based on a correlational design, looking for associations or relationships between variables (Institute of Lifelong Learning (2011) Module 3, Unit 5: 5-11). In this case it assesses the relationship between security culture and SRM.

The data analysis intends to show whether a causal relationship exists between the level of security culture and the level of SRM (figure 1). What is more, it attempts to compare the level of HRM in organizations. Beside the focus groups used in the research ((I)GOs, (I)NGOs, PBEs) two other organizations or sub-groups are presented in figure 1 as control groups to illustrate if there is a causal relationship between security culture and SRM. The data gathered from the online questionnaire was translated into percentages, showing what percent of each focus group chose a particular answer to each question. The figure below shows the relationship between security cultures on the x-axis, whereas SRM is on the y-axis. Thus, the more developed a security culture the more elaborate the SRM is and vice versa. Some of the questions of the questionnaires directly relate to the 8 dimensions of security culture and respectively to drivers of security culture, as mentioned above and characteristics of SRM. Interviewees were asked about their perception whether a security culture exists as well as whether the drivers of security culture exist. All aspects were translated into percentages and the median percentage presented the basis for the location at the x-axis (figure 1). The same applies for the characteristics of SRM. The focus groups are mapped on the graph according to their answers, reflecting their respective relationship to SRM and security culture.

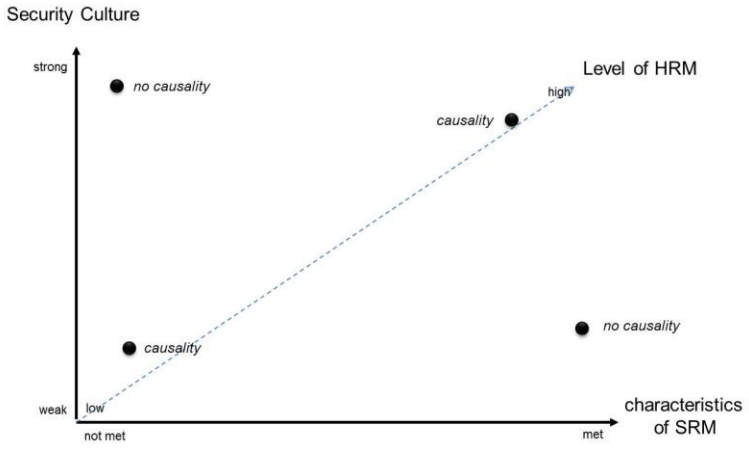

figure 1

The analysis of the raw data was done based on the outcome of the online questionnaire. Each question was evaluated by focus group. Errors were distinguished and percentages were calculated according to the de-facto participants of each question and focus group. That means each question was evaluated according to the actual participants

in each question. For instance, 20 participants from focus group A participated in the survey but only 18 participants answered question X. Question X was than evaluated with 18 participants. Graphs with all the answers as well as the focus groups mapped in them are available in Annex C of the dissertation.

The average percentages of the extent to which groups adhere to SRM characteristics as well as the drivers of security culture are shown in figure 2 presented in chapter four. The UN as well as political foundations were extracted from the focus groups so as to use them as control groups because it was assumed that such institution has a high level of HRM and therefore a high level of security culture and SRM characteristics. Political foundations were assumed to present a low level of HRM and therefore a low level of security culture and SRM characteristics. The assumptions were based on own observations and assessed with data from the questionnaire. The above mentioned control groups were also used to provide evidence for the causality of security culture and SRM characteristics. Data from interviews contributed to the analysis of data as well as the argumentation and discussion in chapter four. Having identified the methodological framework, the techniques and instruments for the data collection were then identified and designed.

Data Collection Tools

The author decided to use three different methods and instruments for data gathering. The first instrument was intended to gather quantitative and qualitative data about the existence of processes, procedures and measures used in SRM concepts by the focus groups. Therefore an online questionnaire was designed. It appeared that there is a significant amount of data necessary to analyse the level of SRM in organizations. The assumption was that open questions alone will make an analysis and comparison difficult. Therefore a self-completion ‘hybrid survey’ was used and the online questionnaire was designed in the form of a qualitative and quantitative questionnaire, as such a questionnaire is described by Rose (1982: 10 cited in Module 3: 6-23 – 6-24). The majority of answers were pre-defined according to the ‘Discrete Likert Scale’ to ensure the comparability of data (Module 3: 5-28) and to provide a set of categories to the participants.

Additionally, space was given for some questions to provide qualitative data as well. Therefore open and closed questions or 'free-text' fields were provided. It is important to note that questions can easily be understood by participants without further clarification The self-completion approach has the advantage that the researcher's bias, the so-called interviewer effect is substantially reduced (Rose, 1982 cited in Module 3: 6-23 – 6-24). Complementary to the online questionnaire, semi-structured interviews according to Fielding were carried out to gather qualitative data from representatives of the focus groups and to collect more detailed information (1993, cited in Module 3: 6-11). The researcher decided to use semi-structured interviews because of the biggest possible flexibility and the lowest possible 'interviewer effect'. Through the choice of this approach potential errors could be reduced and the researcher's bias was kept on an acceptable level.

Online Questionnaire

The questionnaire includes 58 questions related to the security culture, SRM processes and procedures as well as the acceptance of SRM in organizations. The questions refer to the minimum requirements from different actors (table 1), such as People in Aid, Irish Aid, the German Federal Insurance and the Humanitarian Policy Group, as well as lessons learned from the field.

The eight dimensions of security culture by Ruighaver et al (2007) were taken into consideration when designing of questions. Furthermore control questions were included to cross check answers from participants and to detect deviation from previous answers. In addition, advantages and disadvantages as described by Nachmias and Nachmias regarding the design of online surveys were taken into consideration (1981, cited in Module 3: 6-28). The researcher intentionally decided to use leading questions, hypothetical questions, closed and open questions to explore a wide range of information necessary for the research project. The reason is that the questionnaire was used to gather qualitative and quantitative information related to the dimensions of cultural aspects, measurable facts as well as the perception of participants. The order of questions was chosen, so that questions referring to the macro level (culture) come first before addressing Van Brabant's model on individual risk management measures (micro level) in SRM. Closed questions

were presented with pre-defined answers according to the discrete Linkert scale (1-6). This scale was employed in order to force the participants to decide for a value instead of choosing the middle which is possible on a scale between 1 and 5. Leading questions provided space for qualitative answers. In addition, in the case of closed questions, the possibility was given to add free text if the answers provided did not match the specific context of an organization. During the error correction phase in the data analysis the information from open text fields was taken into consideration.

The online questionnaire was sent to representatives from the focus groups via E-Mail. Additionally it was distributed through security business networks such as the European Interagency Security Forum (EISF) (a European NGO security network with 58 member organizations), the Securicon network (a security network of 25 German PBEs) as well as security groups in the social media networks LinkedIn and Xing. The author is a member of these networks and directly requested the participation from the network members and others outside these networks. The network includes development workers, humanitarian workers, risk management and security advisors, heads of corporate security units, CEOs, project team leaders and team members from all types of organizations from the focus groups. Potential participants were initially chosen according to their experience, technical knowledge and likelihood to provide valuable information. Subsequently, these participants were asked to forward the link to the online questionnaire to people with the required knowledge out of their organization (snowball sampling) (Module 3: 5-31). A disadvantage of this procedure is that the researcher has no control on who really fills out the questionnaire. To minimize potential errors as much as possible, certain cross-check questions were integrated into the questionnaire to ensure a higher reliability of data.

Due to the anonymity of the online survey responses cannot be traced back to a certain individual or organization. Nevertheless, participants were requested to answer to which type of organization they belong to. This approach ensures a high level of confidentiality to create a platform to discuss and describe security in organizations openly. Without this procedure it would not have been possible to gather data without any sanitization or to convince organizations to participate in the research in the first place.

Furthermore the participating organizations were highly interested in the outcome of the research, in order to use it internally as a benchmark for further risk communication, risk education and the improvement of their SRM setups. Therefore, it was offered to participants to provide the raw data as an incentive upon termination of the survey.

All participants received a description about the research project, the informed consent form as well as ethics officer approval together with a link to access the online questionnaire. Only a few respondents used the forms to provide a formal approval from their organization or company. The majority of respondents did not provide an approved form due to the anonymity of the questionnaire. The questionnaire was published on the online questionnaire platform Q-Set (www.q-set.de) and was accessible from April 30th 2013 until July 15th 2013. Due to the unavailability of some participants, the access to the online questionnaire was extended on request until August 6th 2013. Furthermore a reminder was sent to all contacted potential participants after the first 2 weeks and again after 2 weeks to maximize the response rate and to counter the disadvantage of a low response rate in online surveys. The reminders lead to an increase of participation and the number of participants were monitored through the back-end of the survey system.

Semi structured interviews

Semi-structured qualitative (telephone) interviews covering the issues addressed in the questionnaire were carried out to complement the data from the questionnaires. The target group consisted of employees from (I)NGOs, (I)GOs and PBEs. They were chosen according to the 'purposive sampling procedure' (Module 3: 5-31). That means that interview partners were chosen depending on their experience in the field, technical knowledge and the likelihood to provide valuable information for the research project.

The semi-structured interviews were carried out with selected contacts from the above mentioned networks. The members contacted include employees from all sectors, the German governmental organizations and German non-governmental organizations (e.g. German Agra Action (WHH/ GAA), German Development Cooperation (GIZ), German Development Bank (KfW), the former German private corporate security network Securicon

(nowadays IBWS Informationsbüro Wirtschaftssicherheit), international non-government organizations such as OXFAM, Norwegian Refugee Council (NRC), Danish Refugee Council (DRC), Irish Aid etc. and from the private sector (BMW, Siemens, MAN, BASF, ASI etc.) as well as insurance companies. The range of respondents was meant to contribute to a comprehensive overview about safety and security culture (some organizations do not differentiate between safety and security) and SRM set-ups in development organizations as well as the private sector. During the data gathering phase six interviews were carried out with individuals both on a one-to-one basis and via telephone between May 15th 2013 and June 15th 2013 for approximately 1.5 hours each. The questions for the interview had been provided via E-Mail to the participants in advance. Nevertheless, the interview scripts from two interviews were crosschecked by the media departments of the participant's organization. This led to some answers being deleted or left out. Furthermore the phrasing of some answers was amended based on the organizational media department guidelines.

Own observations

Own observations contributed to the data gathering according to Nachmias and Nachmias '*uncontrolled observational system'* (1981, cited in Module 3: 6-4). This technique enabled the researcher to study real life situations, actions and activities as they occurred. It further enabled the researcher to observe different organizations in different contexts without following a strict methodology. This ensured flexibility required during the research. The observation of procedures, actions and activities was not part of the research project as such but derived from the experience of the researcher in the field of SRM working in different contexts, with different organizations. However, the author did not record the results of his own background information due to his working experience (13 years) in the field of SRM. Own observations contributed to the analysis in chapter 4.

Research Focus Groups

Individuals participating in the research project were employees of organizations or enterprises working overseas. They share the same experiences while being deployed from an industrial country, working in the same context and being exposed to the same security situation. The types of organizations participating are divided into three focus

groups. The first focus group contains all types of private business enterprises (PBE) such as development aid consultancy companies or other PBEs from all private sectors with operations in NIC countries. The second focus group includes (I)GO including political foundations, governmental units such as diplomatic entities working in the field of development aid or humanitarian aid, subordinated governmental offices such as offices from police forces or ministries from donor countries, (international) governmental development organizations including their humanitarian aid units. This means (I)GOs from industrial countries with operations in non-industrialized countries were selected. The third focus group comprises all possible types of (international) non-governmental and non-profit organizations ((I)NGO) including (I)NGOs in the field of development aid, (I)NGOs including humanitarian operations and Humanitarian Organizations. NGOs from host nation countries were excluded, because this dissertation focusses on organizations from industrialized countries with operations in non-industrial countries.

The classification of individuals working in the same sector into a certain focus group was necessary to ensure the comparability of data gathered from the online questionnaire and the interviews. The criteria for the selection of focus groups were the type of operation and their perception of neutrality. The group of PBEs includes all enterprises with the aim to generate profit from the work they are doing. This also includes private consultancies in the field of development aid that provide services for profit. The group of (I)GOs includes all organizations subordinated to a government and primarily funded by home country government. This also includes governmental organizations or agencies with non-profit and profit units. Furthermore this group holds diplomatic entities, subordinated governmental offices and UN organizations. The third group comprises all international non-profit organizations that are non-governmental. Across the focus groups the questionnaire was open for all hierarchy levels in the respective organizations. Participants in the questionnaire included a wide range of employees, ranging from project staff to security advisors to CEOs. This offered the possibility to analyse the individual perceptions of SRM at all staff levels.

It was planned to collect answers from at least 50 individuals of organizations from different sectors equally distributed across focus groups in order to gather enough information for the research project. More than 150 individuals of different organizations were directly contacted and 350 times the link (through opening the link) to the survey was followed. This shows that the snowball-effect actually worked. 96 (64% of contacted organizations) individuals participated in the questionnaire, 71 (47.3% of contacted organizations) completed the entire questionnaire. Nevertheless, all answers were taken into consideration and each question was individually assessed in order to benefit from the biggest possible amount of data, experiences and opinions. According to Baruch (1999) the sample data fit the required benchmark (60% +/- 20%) to be representative.

Challenges

In an early stage of the research project a pre-evaluation of potential participating organizations was executed. It turned out that individuals and organizations were reluctant to participate in the research project as long as their identity could be discovered. The field of security risk management is still a sensitive topic for most of the organizations. The reason for this reluctance to participate can be found in the reputational risk and accountability of organizations on the occasion it turns out that they do not meet the legal or ethical requirements. In consequence, the potential organizations requested the anonymous participation in the research project. Therefore the research was conducted anonymously and answers and statements cannot be traced back to an individual or a specific organization or enterprise but only to a focus group and sector. This approach ensures that statements are provided without fear and data collected is based on real and true information about the level of SRM and security culture in organizations and enterprises. The confidentiality notice was integrated in the request for participation in the online survey, sent to potential participants. Furthermore participants are not under pressure to involve corporate media departments or the pressure of political correctness. Another challenge during the design and execution phase came up in the administrative design of the online questionnaire. It was not possible to use an ‘if-then’ algorithm during the design of the questionnaire. This resulted in the error that participants were confronted

with the same follow-up questions no matter if the basic question was '*yes*' or '*no*'. Participants were confronted with both possibilities and were forced to ignore the question not relevant to them.

It was a challenge that some questionnaires were not fully answered or not submitted. The reason may be on the one hand that some questions did not match the organization or the questions were deemed too critical to be answered. On the other hand some participants finished the questionnaire but did not click the 'send' button. The reason may be that it was not really clear that the 'send' button needs to be used to finish the questionnaire. The cause can be found in the online layout provided by the service provider Q-Set. Nevertheless, not using the 'send' button does not really have an impact because answers were saved but not registered as 'sent'. It was possible to use these answers in the analysis.

Additionally, the author experienced some difficulties during the research project. There has been a huge amount of data collected during the online survey as well as the interviews. The analysis of data provided so many data that discussion would have been able with different focuses. It was necessary to strictly focus on the intended area of research to avoid losing focus in the paper.

Reliability of data

The reliability of data was crosschecked through control questions in the online questionnaire as well as test questions during the interview sessions. Both data sets were compared and checked against each other.

The answers/ data gathered were not checked against the formal organizational requirements, such as policies, formal approaches or decisions and their availability in reality. Moreover the answers reflect the individual perception and opinion on how the individual systems and cultures look like or should look like. It was intended to gather data and individual perceptions from all levels of staff in organizations and to analyse what would be needed to minimize shortcomings and to improve the system. Furthermore it was

intended to collect information about the reality in organizations, in example what is written on paper and how reality looks like.

Chapter 4 Findings and Discussion

Chapter four presents an analysis of security culture and their drivers and how they interact and influence security risk management as well as SRM characteristics. Findings derived from the data collection are being linked to and discussed with statements form the literature review. Furthermore the results from the data collection were analysed in two dimensions. The data was analysed as a set in its entirely and then analysed along focus groups in order to identify deviations from one group to another.

Looking at the minimum requirements and standards for SRM together with the results of the survey, it shows that there are different approaches to SRM and no single approach to SRM across focus groups in NIC countries. In consequence, this paper argues that a set of certain standards in SRM – here referred to as HRM – are necessary to address the challenges faced in NIC environments. The most crucial factors are the development of a security culture including tightly coupled subcultures such as just culture (Dekker, 2012). The stronger a security culture the better the level and quality of SRM culminating in HRM, and vice versa. Deterts et al eight dimension model, modified by Ruighaver's et al (2007) has shown that it is possible to review an organizational security culture to some extent considering the eight dimensions and drivers supporting these dimensions.

Table 1 shows the minimum standards as defined by different organizations such as People in Aid, VENRO, Irish Aid or the German Federal Insurance. The data used is derived from the questionnaires as well as from information published by the respective organizations.

The classification into (I)GOs, (I)NGOs and PBEs represents the focus groups. Focus groups are ranked as adhering to or implementing an HRM characteristic if 50% (defined threshold in this paper) or more of its constituent organizations do so.

The HRM model, represented in table 1 results from best practices in SRM, such as van Brabant's Good Practice Review and a combination of Ruhighaver's eight dimensions as well as minimum standards from different organizations working overseas.

					50% + in Online Survey		
HRM characteristics	**People in Aid – Minimum Standards**	**VENRO – Minimum Standards**	**Irish Aid Minimum Standards**	**Federal insurance (DEU)**	**(I)GOs**	**(I)NGOs**	**PBE**
Safety and Security Culture	●		●		●	●	●
Reporting & Just Culture			●			●	
Accountability Policy			●	●			
Policy for safety and Security	●	●	●	●	●	●	●
Pre-deployment Medical Check	●			●	●		
psycho-social counselling/ debriefings	●			●	●	●	●
Context Analysis	●	●	●		●	●	
Conflict Analysis			●		●	●	
Risk Identification	●	●	●	●	●	●	●
Risk Analysis	●	●	●	●	●	●	●
Risk Evaluation	●	●	●	●	●	●	●
Presentation of risks in a matrix (risk communication)	●	●	●				
Risk threshold		●	●	●	●		
Risk management strategy		●	●		●		
Implementation of SOPs	●	●	●	●	●	●	●
Planning and implementation of HRE and MedEvac	●	●	●	●	●	●	●
Planning and implementation of	●	●	●	●	●	●	●

emergency plans							
Recall/ Cascade Emergency lists / attendance monitoring			●				
Preparation and implementation of BCM			●				
Reporting	●	●	●	●	●	●	●
Site Security		●			●	●	
Travel Security		●			●	●	●
Monitoring of the security situation		●	●	●	●	●	●
Distribution of information			●	●	●	●	●
Individual advice for employees or projects / programs					●		●
Security Awareness Trainings		●	●	●	●	●	
Security Briefings	●	●		●	●	●	●
Security communications (VHF/ UHF/ HF/ Sat)/ alternative communication							
Lessons Learned workshops after incidents		●	●				●
Crisis Management				●	●		●
Incident Response		●		●	●	●	●
Crisis Communication and PR services		●					
Dispatch & Airport Pickup					●		
Guarding/ Close Protection/ Private Security Companies Policy					●	●	

Table 1

In the discussion the author will be referring to the eight dimensions of organizational culture used by Detert et al (2000) and were then used by Ruighaver et al (2007) in order to discuss security culture. Ruighaver's et al (2007) argued that there is not a single static framework of security culture but that Detert's et al (2000) eight dimensions of culture can nevertheless be used to assess an organization's interest in and support to a

healthy security culture and SRM. The presence of a security culture in organizations is supported by several factors. The questionnaire discovered several drivers supporting the security culture of an organization (table 2). The most important drivers supporting the presence of a security culture are the commitment for, dedication to and promotion of security by the top management. Furthermore experiences and learning from past incidents supported by the open communication in an organization (table 2) support a security culture. Another important factor is the training of employees at all levels (risk education). In the following it will be assessed whether a solid SRM or even HRM occurs in conjunction with a security culture. If the latter is present or not will be indicated by the presence of the aforementioned drivers of security culture (table 2).

Drivers of Security Culture		
Employment of security professionals and trust into their competency	Commitment by the top management and allocation of necessary resources	Role-model approach by top management and security professionals
experience of critical situations and incidents and communication at all levels, especially the top management	Promotion of benefits of security risk management and communication about accountability of staff	Workshops/ training and risk education
Government and insurance requirements and regulations	Learning from past incidents	Yearly country audits (quality and existence of procedures and structures)
Exposure of the organization to the public	Just culture environment including confidential and anonymous reporting	Acknowledgement that employees are an asset and safety and security is first priority
Duty of care	Integration of security risk management in the organizations core processes	Good practice and understanding of benefits from security

Table 2

Taking all results into consideration and summarizing aspects from the data gathering into the characteristics of security culture as well as characteristics of SRM, evidence is provided that there is causality between security culture and characteristics of SRM. Weak drivers of a security culture lead to a weak security culture. A weak security culture leads to a low level of adherence or implementation of characteristics of SRM. Therefore the level of HRM is very low. The data shows that there are no organisations that score high on SRM and have a weak security culture at the same time. The analysis of the focus groups as well as the two control groups provide evidence that a causal relationship exists between the level of security culture and the implemented characteristics of SRM. Figure 3 presents an analysis of all relevant online survey questions to Ruighaver's et al eight dimensions of security culture, the matrix below (figure 2) shows that the level of security culture and implemented characteristics of SRM define the degree of HRM.

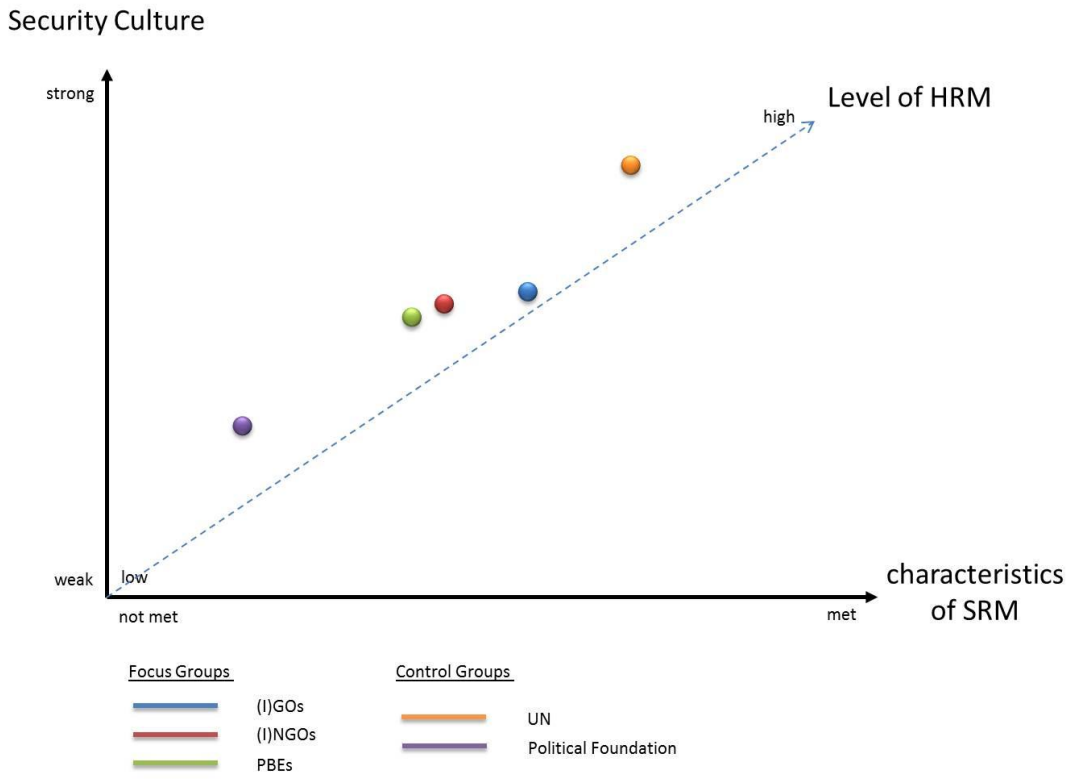

figure 2

While participants believe that their organizations maintain a strong security culture, the reality shows that their perceptions are conflicting with reality. People in organizations

were asked if there is a security culture present in their organizations. A high number of participants stated that a security culture in their organization exists. Going into detail and connecting answers from the questionnaire to the drivers of security culture, it presents a different picture. Considering Ruighaver's et al eight dimensions of security culture, one can detect a discrepancy between the perception of the level of security culture in organizations and the reality analysed according to the drivers of security culture. As a result the perception of the importance of security by different stakeholders indicates a shortcoming in the dimension of 'basis of truth' within the respective organization. The visualization of the data in figure 2 takes this into account by using the median of both, the perception of security culture and the eight dimensions as explained in the chapter Methodology.

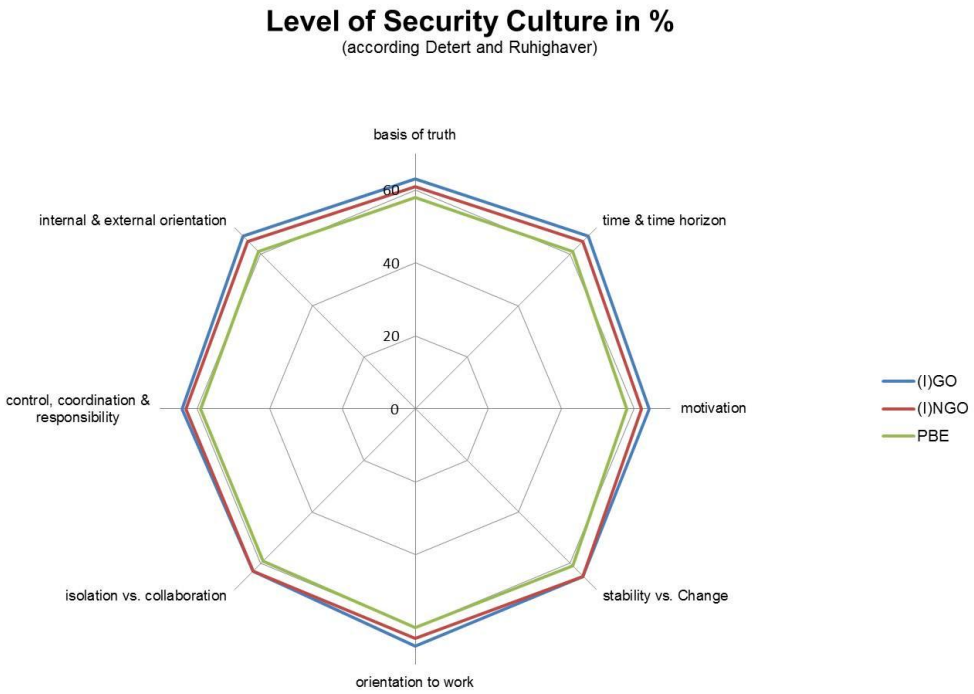

Figure 3 (8 dimensions of security culture) – focus group assessment

The majority of organizations (89%) implemented a policy on safety and security of staff (figure 7 and figure 58 Annex A). The high percentage is argued to result from the presence of a security culture (figure 9 Annex A; 79% and figure 75 Annex A) or the legal pressure. Another supporting factor may be the experience of incidents in organizations (figure 11 Annex A; 78%) including 74% of respondents experienced incidents individually

(figure 14 and figure 15 Annex A). The high percentage of organizations with a policy indicates that security is important in the organizations. Nevertheless, it does not indicate that the basis of truth is balanced between the end-user's believes and the organizational believe about the importance of security nor does it indicate the quality of SRM (Ruighaver et al, 2007). One interviewee from the financial and insurance sector stated there is no overall security culture but a fragmented set of decentralized security cultures. Another interviewee from the automotive sector supported the statement. Furthermore he stated that the topic of security and risk management is in general fractured in the company. Many small units are working to the topic of security and risk management. There is no common leadership and no formal organizational security structure. It indicates that there are isolated approaches towards security rather than a cooperative and participative approach. It results in an aspect influencing the motivation of employees and finally a negative impact on the security culture environment and SRM (Ruighaver et al, 2007). One interviewee from a (I)GO stated that non-participation of employees in SRM leads to the result that employees are opposing or resisting SRM which then perpetuates a weak SRM. This is supported by 37% of responders stating that there is no need for SRM because it hinders project implementation, it restricts freedom of personal, it is too expensive or organizations are not exposed to security risks (figure 30 Annex A).

More than 71% of the respondents stated that security is important in their organization (figure 23 and 66 Annex A). 68% stated that the policy is accepted by employees and integrated into day-to-day operations (figure 8 and 67 Annex A). But only 34 % of respondents stated, that SRM is manifested in their organization and supported by the management and only 23% stated that it is mandatory for all business units. This indicates that the importance of security perceived on the individual level does not necessarily correspond with the appraisal on the management level. In consequence, awareness for security related matters on the employee level does not result in a sustainable organisational security culture. An interviewee from a diplomatic entity stated that their management realized the importance of security as management tool and fostered the improvement through the provision of a strong mandate and financial

resources to the security department after they encountered an incident. It strongly supports Detert's et al dimension about the basis of truth. Believes about the importance of security are balanced between employees and the management which results in necessary resources being provided (Ruighaver et al, 2007). This indicates that a strong security culture is in place. This good practice was only discovered in one of the organizations participating in the interviews. All others indicate shortcomings in commitment and provision of resources. Van Brabant (2010) discovered the same shortcomings during his research. The interviewee further stated that it is a continuous process to convince the management to keep the same level of support. Another interviewee from a diplomatic entity stated that a security culture only exists on paper and there is a lack of understanding in top management. Van Brabant (2011) and Bellot (2011) support the evidence. In general security culture is not only driven by the acceptance of employees, but also dependent upon the support within management. Without buy-in from the executive level security culture remains on the individual level, but not on the organisational level, aiming for a common basis of truth (Ruighaver et al, 2007).

An interviewee from a humanitarian organization stated that they have a policy in place. Their security culture is defined by their identity as a humanitarian actor and thus the humanitarian principles. Their policy does not consider roles and responsibilities, accountability of employees and the leadership or other aspects of security risk management. It shows that the mere availability of a policy for safety and security of staff does not provide any evidence about the quality of the content and how important an organisation deems security.

All interviewees argued that the organizational security culture is driven and triggered by incidents. A PBE interviewee stated that the level of organizational security culture and the importance of security decreases after the longer an incident dates back. Another employee from a PBE stated that the importance of security depends on the individual emotional impact. While people requiring support from security professionals appreciate the support, people without the experience of incidents and SRM support tend to be opposed to SRM. It indicates that a lack of risk education and a lack of ownership by

employees may lead to the perception that security is not important. As a result it indicates an ill security culture. Interviewees from the PBE but also (I)GO business perspective stated that business is profit driven and if loss harms profit, SRM is getting attention. The statement indicates that an organization with a weak security culture and a lack of long-term strategic security planning only recognises the importance of security if profit is threatened. Another crucial factor is that individual annual goals of senior management are not related to security but business related matters. As long as security supports the achievement of aims, senior management will foster security.

As argued above, the number of incidents an organization experienced is influencing the importance of security in an organization. Figure 11 Annex A shows that 78% of organizations already experienced security related incidents in non-industrialized countries. But only 31% responded that incidents are reported regularly (figure 12 and figure 35 Annex A) while 55% stated that there is an obligation for reporting (figure 35 Annex A). 78% responded that they also report errors and near-miss incidents (figure 38 Annex A). This fact shows that the number of organizations reporting on incidents, near-miss incidents and errors is critically low. This shows that SRM is dependent on the level of just culture and security. There are no indicators that the critically low level of reporting is caused by a reporting approach without a feedback loop. 63% responded that they would appreciate receiving a feedback or a follow up to the reported incidents (figure 13 Annex A). A cause for the low level of reporting can be seen in a weak just cultural environment of the respective organizational security culture (Dekker, 2012). Only 55% of respondents stated that there is a possibility to report confidentially and anonymously (figure 37 Annex A). Furthermore most of the organizations do not foster or award the reporting of incidents. More than 72% responded that there is no just cultural environment present in their organizations (figure 39 Annex A). A PBE interviewee stated that the organizational security culture depends on the level of error culture. That means people try to avoid being blamed for errors by reporting of error, near miss incidents and incidents. It indicates that there is a fear driven environment and a lack of a just cultural environment as well as an appropriate accountability policy. An interviewee experienced that people only talk about

failures, errors and incidents once a project is closed and they cannot be held accountable as easily. Being in the know of accountability policies and the repercussions for individuals contributes positively to the level of reporting and the level of security culture. Only 32% of all respondents stated that there is an accountability policy or statement available in their organization which results in a lack of guidance for employees (figure 40 Annex A). In detail, only 22.2% of PBEs, 31.6% of (I)GOs and 47.1% of (I)NGOs stated that there is an accountability statement available (figure 59 Annex A). An interviewee from a humanitarian organization stated that their accountability policy is really strong and non-compliance to safety and security rules and regulations is charged with disciplinary or contractual consequences. It is made clear that the action of individuals impacts the entire project or operation. If people are not aware if they are accountable or not and if there is a possibility to be blamed instead of being supported, people tend not to report errors, near miss incidents and incidents. The level of just culture and thus security culture as well as the level of organizational learning is dependent on the level of reporting and therefore dependent on a clear accountability policy or statement in organizations. Another factor influencing the reliability of accountability is the action taken in case of non-compliance or reckless behaviour. As an example, an employee of a governmental development organization was kidnapped in a high risk country while he was hiking in the mountains and thus not complying with a no-walking policy outside the perimeters of the town. He survived the kidnapping and was relocated from his duty station to headquarters, without any disciplinary action or contractual consequences. Other colleagues recognized the action of the organization as promotion for the employee. This indicates that negligence towards security rules has no consequences in that specific organization. An interviewee from a diplomatic entity stated that there is an accountability policy available – but just on paper. In reality it does not have any effect on people's reckless behaviour as it is not being followed-up.

At organizational and corporate security level, the importance of security risk management also depends on the extent to which SRM is integrated into core processes of the organization, the location of SRM units in the organizational structure and their

authorized mandate. Only 4% of the responding organizations stated that the security unit is directly located at CEO or top management level. On the other hand 46 % responded that the security risk management or corporate security department is an independent unit in the organizational structure (e.g. staff unit, independent unit subordinated under the top management, subordinated under the operations branch) (figure 10 and 68 Annex A). More than 23% of the security risk management units are subordinated in the central services department or the human resources department including direct lines of communication to the top management. A PBE interviewee stated that their SRM unit was shifted and is now directly reporting to the senior executive level and subordinated to the COO. This allows the unit to support the management in protecting the organization's values, assets and reputation. Organizations with SRM units located at HQ level, subordinated to departments without a direct connection to or reporting mechanism allowing to directly addressing the top management tend to have less support from the executive level (lack of promotion of power) and thus a weaker security culture. SRM departments subordinated to the top management level reach a percentage of 76.80% of HRM characteristics as well as characteristics of a security culture. SRM units without a direct connection to the top management (65.36% - subordinated to the HR or other departments and 57.39% - individuals with a security responsibility as secondary or third function) only reach 61.38% of HRM or security culture characteristics (figure 72 Annex A).

As a result HQ security units lack the possibility to communicate risks to top management or risk that information are altered on the way up through middle management. It supports the argument that the importance of security differs at the employee, middle management and executive level and hinders that a common basis of truth can be developed. In consequence, all focus groups do see a lack of support and commitment from top management, a strong mandate for SRM units and a lack of responsibilities to execute tasks to ensure the safety and security of staff to the best possible extent.

The increasing number of staff working in high risk environments or the increasing number of environments turning into high risk environments and an increasing number of

business travellers or HQ staff from the focus groups require improvement of their current organizational approach towards SRM. One crucial point is the pre-preparation of employees for their assignment or travels to high risk countries. 84% responded that they took part in an incident awareness training (figure 16 and 61 Annex A) but only 59% responded that they were trained for insecure environments prior to their deployment or travel (figure 16 and 62 Annex A). 34% did not participate in security training for NIC countries or never participated in any security training (figure 17 Annex A). In 2013 one advisor of a PBE was sent to Mogadishu in Somalia for an assessment mission. He just booked a hotel and moved without any support, back up, contingency planning or restrictions in Mogadishu. This reflects the understanding and acceptance of security and the relatively low level of security culture in an organization. Furthermore the top management of the respective organization is neglecting their duty of care towards their employees (Williamson, 2010). It indicates that a security culture and the adherence to duty of care are non-existent in some organizations.

In regards to post incident support 73% responded that there is psychological and support to families available in their organization while 11% of the organizations do not offer any psychological support (figure 18 Annex A). In detail, more than 90.9% of (I)GOs, 70.6% of (I)NGOs and 55% of PBEs provide a psychological service to their employees (figure 60 Annex A). Especially the increase of asymmetric warfare and the use of insurgency tactics, techniques and procedures and improvised explosive devices resorted to by groups like Al Qaida, Taleban or Boko Haram lead to an increasing number of (complex) attacks aiming at indiscriminate targets, which leads to more civilians being affected. Experiencing high profile incidents such as complex attacks but also kidnappings or the becoming the victim of criminal activity is often leading to traumatic experiences and post-traumatic stress disorder. Furthermore attacks targeting international actors such as private business enterprises (e.g. attack against Tiguentourine gas facility in Algeria in January 2013) or aid agencies (e.g. complex attack by Al Shabab against UN in Mogadishu in June 2013 or the complex attack against ICRC in Jalalabad in May 2013 or the complex attack against the Taverna Restaurant in Kabul in January 2014) increase the likelihood of

employees being directly affected or experiencing the loss of colleagues and friends. The examples underline that psychological support mechanisms are a necessary component of SRM and are thus essential for business continuity and for the protection of employees. It further requires a proactive approach to assess all incidents or near miss incidents to actively learn. Bluelight services in most of the industrialized countries execute institutionalized debriefings or after action reviews after rescue missions or critical events. There are no indications that these instruments are used by (I)GOs, (I)NGOs or PBEs working in NIC countries.

The increase of casualties amongst aid worker or employees of PBEs especially in high risk countries leads to a high level of security awareness at field level, often driven by the emotional impact on employees (figure 1 Annex A). But while 64% of all respondents stated that their organization implemented SRM structures in NIC countries, such as security focal points. An interviewee of a diplomatic entity stated that they are going to employ security risk management advisors to field offices, with a secondary function of conflict sensitivity advisory services. SRM advisors are working on day-to-day, context and situation dependent questions rather than standardized or along methodologies following the SRM concept for insecure environments (Van Brabant, 2010) which is based on ISO 31000/ 31010 norms and good practices (ISO, 2009a, 2009b). In general more than 90.9% of (I)GOs, 82.4% of (I)NGOs and 50% of PBEs implemented SRM systems in contexts with varying security challenges, often development or emerging countries (figure 63 Annex A). The percentage underlines that SRM structures and setups are implemented in more secure environments such as emerging countries and development countries rather than high risk countries and fragile states. Contrary to that only 8% implemented *appropriate* SRM structures for high risk environments or fragile contexts (figure 19 Annex A). The reason for the very low percentage of appropriate SRM measures is that security has no priority in the organization (18%), there are no financial resources available (13%), no support from the top management (10%) and a weak security culture (9%) fostering SRM (figure 33 Annex A). Additionally, respondents stated that the top management is too far away from the operational level. Even 5% stated that the organization has no interest in

SRM or do not see the need (3%) (figure 33 Annex A). As a result, organizations are underestimating the security situation and the importance of SRM structures in high risk environments or fragile contexts.

Focussing on different actors in the same theatre, there is an increasing number of PBEs working in the field of development or humanitarian aid. An interviewee from a development PBE stated that their donor fully transfers potential risks to the consultancy. The European Union is using the same approach. In the consultancy structure they do not have a SRM setup. Project managers are supposed (according to their own individual believe) to ensure an appropriate setup but lack the capacity for SRM. In terms of financial resources, a small budget is included into the proposals as development PBEs try to keep security costs down in order to be competitive in the run for projects and programs. There is *no real* interest from donors that legal obligations and social standards are met by implementing agencies. It strongly depends on the donor, the nationality and even the funding government. In example, DfID, the EU or the Federal German Foreign Office tend to balance foreign politics and potential achievements as well as the reputation of their entity (to fulfil international responsibilities) against the personnel security of implementing agencies and consultancies to some extent. The analyses along focus groups ((I)GO, (I)NGO, PBE) discovered that (international) governmental organizations ((I)GO) follow the approach of a security risk management unit at HQ level complemented by local and regional security risk management advisors at field level (25%) with the unit at HQ acting as focal point (20%) and a holistic *all level* approach (20%). (I)NGOs mostly follow an *all-level* approach (29.4%), followed by security risk management responsibility at program and project level without a supporting HQ structure (23.5%). The least represented set-up consists of a HQ approach without decentralized structures (11.8%) and an *individual staff security risk management* approach (11.8%). In comparison with (I)GOs and (I)NGOs, the private business enterprise (PBE) approach is different in some characteristics. 31.6% of respondents stated that they follow the *HQ point of contact* approach. 15.8% responded that there are no decentralized SRM structures available, followed by security focal points not integrated in a security structure (10.5%) and an *all level* approach (10.5%) (figure 25

Annex A). A PBE interviewee stated that the organization currently restructures their approach, implementing regional hubs with professional SRM staff rather than an isolated HQ point of contact approach. Regional SRM advisors will have the responsibility to rollout HQ standards and approaches and have a bridging function between HQ and field level to counter the HQ lack of emotional impact and distance to the field level. Nevertheless, there are 10.5% of responses stating that there is no structure at all available (figure 25 and 63.1 Annex A). In total, 81% have access to at least a security focal point in their organization, while 16% do not have any access to an individual or a structure dealing with SRM (figure 21 Annex A). An organization is putting a SRM unit in place if the organizational culture deems security as being important. In consequence, it is more likely that SRM characteristics are met. Despite that there are organizations which do not value security in the same way, which leads to a low degree of security culture. Often the need to implement SRM units is not seen.

In total 93% of all respondents stated that they expect from their organization that professional security risk management processes and systems are implemented based on the employer's duty of care (figure 26 Annex A). 100% of (I)GOs and (I)NGOs respondents expressed the expectation while 26.7% of PBEs do not expect the implementation of professional SRM structures from their employer as obligation for duty of care (figure 64 Annex A). Nevertheless, 88% stated, that there is a need for a professional risk management system while working in NIC countries (figure 28 Annex A). The data indicates that there is a lack of risk education and ownership in organizations and as a result it indicates a weak security culture and a divergence of beliefs between employees and organizations. In total 33% of all respondents believe that security risk management should be manifested at top-management, board of directors or CEO level, beside an 'all level' approach (figure 27 Annex A). Nevertheless, 76.5% of (I)NGOs and only 52.6% of PBE support this approach, while 100% of (I)GO respondents do see the need to manifest security risk management at top-management level (figure 69 Annex A). It indicates that employees believe that security is important but in reality it does not match the beliefs of the organization. The weak provision of resources underlines the statement (figure 33 and

figure 71 Annex A. (I)NGOs responded that security should be manifested at all levels (between 70.6% and 82.4%). Contrary to that, only 33.3% of (I)GOs and 26.3% of PBEs believe that security should be manifested at employee level or middle management level ((I)GO – 33.3%; PBE – 36.8%). Finally, all groups see the need for a multi-level approach with the commitment and promotion at top-management or senior executive level (figure 69 Annex A).

More than 65% of respondents believe that incidents or the impact of incidents could have been reduced if the organization had implemented security risk management structures. 94% of respondents believe that the level of risk can be managed and minimized through the setup of a professional security risk management system (figure 34 Annex A). Nevertheless, 16% do not believe that it would have changed anything (figure 20 Annex A). The data leads to the assumption that employees would be supportive of a SRM system if it would be established. Furthermore, 19% responded that they addressed the need for SRM structures and measures but the management did not allocate any resources or did not react at all. It supports the argument that there is an imbalance of truth about the importance of security in organizations. It further indicates a lack of long term strategic planning and the favouring of an approach attempting to establish organizational stability rather than security change management (Detert et al, 2000; Ruighaver et al, 2007).

The acceptance and supported of SRM by employees is reflected in the answers provided to the questionnaire. 84% of employees responded, that they trust the competency of security professionals in their organization while 51% only partly show trust in the competencies (figure 22 Annex A). Those 51% respondents believe that there is a high level of uncertainty if security professionals appointed as security focal points only have a military or police background or are program/ project staff without any professional security background. It indicates that the importance of security in organizations is often lacking professionalism if security staff is only employed because of their background (and the misinterpretation of the definition of security) rather than a formal comprehensive security and risk education. This may hinder trust into the organizational SRM system and

influences the organizational security culture. Nalla (1995) supports the argument and developed curricula requirements for security professionals complementing the military/ law enforcement.

The data was also intended to review the methods being used as part of the organizations SRM. One crucial activity is the execution of a risk assessment. It was observed that many organizations are doing risk assessments based on 'the seat of ones pants'. The data shows that 41% of interviewed organizations are not basing their risk assessments on a transparent, qualitative or quantitative methodology. More than 16% do not even know if their organizations are executing risk assessments. Only 16% of organizations are using risk assessment methods according to ISO 31000 or ISO 31010 (e.g. likelihood-impact matrix, fishbone assessment, cause-effect assessment etc.) (ISO, 2009a, 2009b). Since the legal requirement (e.g. corporate governance, duty of care, health and safety legislation or corporate manslaughter and homicide legislation) as well as requirements from insurance companies (risks must be identified and known to the organization), the data show a critical status quo in the participating organizations (figure 24 Annex A). It means that organizations do not fulfil the obligations derived from insurance standards or duty of care. On the other hand available legislation is not fully clear and leaves organizations with a wide range of interpretation. Instead of conducting their own assessments many are resorting to assessments provided by others, such as UNDSS or private information providers and fully adopt them. This data applies for (I)GOs, (I)NGOs and PBEs to the same extent. While (I)GOs (58%) and (I)NGOs (57%) are using no standard methods for risk assessments, 30% of PBEs implemented risk assessments according ISO 31000/ 31010 in comparison to 16% of (I)GOs and 7% of (I)NGOs (figure 44 Annex A). An interviewee from a development PBE stated that information and assessments from other actors, such as UNDSS are used as benchmark. They fully comply with the UNDSS recommendations and assessments. The interviewee further stated that the PBE would be more restrictive if there would not be any 'third party source' available and the PBE would have to decide in own responsibility. It indicates that some actors define a very low risk threshold if no SRM resources are available that indicates

weak drivers of the organizational security culture. In consequence, an organization with no SRM capabilities and no interest in the implementation of SRM capabilities would rather define a low risk threshold. As a result, the lack of security culture would impact the SRM system of the organization.

Another current development but also source for conflict is the integration of SRM into the concept of peace and conflict assessments (PCA) or vice versa (Kruk, 2008). The concept of PCA provides a framework for conflict sensitive planning and management of development projects. Essentially, it is the risk management of the effects from a conflict on development cooperation. It includes risk management as a step in the entire process but is not explicitly focussing on safety and security of staff. Furthermore PCA focusses on the acceptance strategy using the instrument of do-no-harm (GTZ, undated). PCA starts with a conflict analysis identifying connectors and dividers, in order to allow for programming that aims to build peace and mitigate existing conflicts as an add-on to the primary project goals. The concept of *'do no harm'* is not directly aiming at building peace, but to avoid negative unintended impacts for the beneficiaries and the program (Anderson, 1999). The rationale behind this is that by avoiding unintended negative impacts and building peace the organization delivering activities on the ground avoids becoming a target of negatively affected stakeholders. PCA has a strong project focus, considering programmatic and contextual risks (OECD, 2012). Some perceive do no harm and PCA as tools or methods of SRM. An interviewee from a diplomatic entity and an interviewee from a governmental development organization stated that both fields are currently merged to reach the best possible result for the safety and security of employees and the achievement of project objectives. This requires the dedication of organizations to the priority of safety and security of staff instead of prioritizing project aims and profits against personnel security. In fact, if PCA and SRM complement each other without being in competition to each other it supports the safety and security of staff and foster successful project implementation. The impact of projects or interventions is tightly coupled to SRM and safety and security of staff and both approaches interact with each other. Considering both approaches while prioritizing personnel security support the organizational security culture and motivate

employees to take responsibility and ownership for security at their level because it is linked to project or business activities.

In the past different authors, such as van Brabant in 2001 discovered that a number of organizations do not see the need to implement appropriate security risk management measures. This paper argues otherwise. Taken the balanced and diverse focus groups into consideration, there is evidence that approximately 63% do see a need while 9% believe that the existence of a professional security risk management system would hinder project implementation rather than supporting it. Only 8% believe that it restricts project implementation and freedom of personal. It can be assumed that it is related to the fact, that movement restrictions in high risk environments are heavily influencing the operations planning of programs and projects in terms of time-frames as well as the freedom of people to move freely. The high positive percentage and low negative percentage indicate that security is perceived as important at employee level. As an example, staff in contexts such as Afghanistan or Somalia need to report their location, their movements etc. to the security department, even after working hours. They have the feeling to be controlled or constrained and not being able to make their own decisions.

Another argument against setting up a more comprehensive SRM system is the allocation of financial and human resources for SRM units in headquarters. The HQ SRM units do have a technical and quality backstopping function but a lack of human and financial resources. This indicates a lack of commitment by top management and consequently at organizational level, which indicates a weak security culture and thus has an impact on the quality of SRM. Ruighaver et al (2007) argue that organizations focus on policies and procedures and the adherence to legal obligations instead of focussing on the qualitative improvement of security systems. There are still 6% of responding organizations who believe they do not need security risk management mechanisms because being a neutral actor ensures safety and security and because they do not see themselves exposed to significant risks. 1% of the responding organizations believe that security related incidents do not affect their operations (figure 30 Annex A). It indicates that there are still organizations neglecting security and lack a security culture. The analysis provides

evidence that mainly PBEs, humanitarian organizations and political foundations do not see the need for SRM mechanisms. In consequence they show a weak security culture. Some of them are lacking a security policy; they do not provide any risk education in terms of trainings or pre-deployment trainings and do not use any systematic methodologies to identify risks.

Often there are discussions in the SRM community that the management of organizations do not react to the assessments of security professionals or project team leaders and that resources are not provided. But often the management is not aware about the needs to react to risks or even the mere presence of risks. The research discovered that 68% of employees address their needs and assessments to their leadership while 24% do not address their need (figure 31 Annex A). Only 7% of people who addressed their needs to the leadership did not receive any response. In more than 81% the leadership responded and implemented measures. But measures are often deemed inadequate and were limited to naming focal points, advisors at field or HQ level or training and risk education. It can be assumed that the management will act in most cases if needs are communicated (figure 32 Annex A). Furthermore it can be assumed that needs are not communicated to the management and therefore the management is not aware about requirements. It can be argued that there is a need for a direct connection or reporting structure between SRM units and the top management to ensure a risk culture that results in adequate responses to risks. The allocation of SRM units as subordinated units in other departments may hinder reporting to executive management since there are too many hierarchy levels between the SRM units and management. As a result, information does not reach the top management-level. Middle management structures are able to influence reporting of risk professionals and requirements identified in the field. Therefore top management is not able to fully grasp and understand the needs of the field level. It underlines that the commitment by the top management is dependent on a compliant middle management ensuring a flow of information to the executive level. Direct communication between risk professionals and top management would be beneficial for a

security culture triggering down from the top, through middle management to the employee level.

The commitment by top management is only one aspect necessary for a strong security culture. More than 46.2% of responders experienced that security or the implementation of appropriate measures was not prioritized in the respective organizations. Other issues or governance related issues enjoy more attention than security. One third (33.3%) claimed that there are no financial resources available for security (approx. 50% of (I)GOs and PBEs) and 25.6% stated that there is no promotion of power (SRM is one topic at CEO level, supported and demanded by top management) at top management or board level (48.2% of (I)GOs, 12.5% of (I)NGOs and 25% of PBEs) (figure 71 Annex A) which is related to 12.8% claiming that there is no interest by the management. 23.1% experienced that there is no security culture which fosters the security risk management in the organization and almost 20.5% believe that the management is too far away from reality and is not emotionally effected (figure 33 Annex A). The data leads to the assumption that the commitment from the management and thus the promotion of SRM and the allocation of resources in order to fulfil duty of care is essential to foster a security culture. A supporting driver for a strong security culture and necessary SRM setups is the commitment from top management and the knowledge about incidents and lessons drawn from incident assessments and lessons learned. Approximately 15% of organizations just archive reported incidents, there is no further assessment or use of incidents for the learning of the organization. More than 85% analyse reports, integrate them into an internal statistics (10%) or use them for case studies and lessons learned (44%) (figure 36 Annex A). 75% believe that reported incidents support the learning of the organization while 9% believe that people can only learn at individual level rather than organizational level (figure 41 Annex A). Only 55% of all responders are obliged to report incidents and thus report them regularly; 20% report incidents only sometimes; 12% only report business related incidents and 8% report incidents through whistleblowing (figure 35 Annex A). An interviewee of a diplomatic entity stated that there is no defined threshold in place. Nevertheless, the organization currently discusses the need and the necessity. The same

argument was stated by an interviewee from a PBE in the automotive sector. An interviewee from a humanitarian organization stated that he has no knowledge about a threshold in the organization, which indicates that there is none or it is not communicated sufficiently. In the end both result in the same: No knowledge about security risk thresholds in the everyday activities on the ground. An interviewee from a development PBE stated that their organization does not have a threshold at all. One reason is that contracts are based on outputs and the consultancy is only getting money if required results are delivered. Donors are putting enormous pressure on their implementing partners and the consultancies are balancing security requirements against profits and finally against the survival of the PBE. Thus there is a conflict of interest, which results in a weaker security culture. That leads to the assumption that a fear driven environment hinders proactive incident reporting as it might bring project activities to a hold. This then hinders organizational learning and negatively influences the commitment from top management to SRM. If there are no (reported) incidents affecting the organization, the organization believes that there is no need to foster the topic of security and as a result to allocate resources. The gathered data indicate that there is a critically low level of reporting in organizations that leads to the assumption that there is a weak just cultural environment supporting the security culture.

Another essential driver for security culture is the motivation of employees and the ownership for security amongst employees. Ruighaver et al (2007) argued that as long needs and recommendations from employees are ignored or neglected by management, employees will lose their motivation to invest in security and as a result may compromise security practices and expose the organization to risks. Beside duty of care, legal responsibilities or corporate responsibility at technical level, it is essential for organizations to keep employees motivated, especially in high risk and fragile environments. The motivation of staff is important to keep staff in difficult environments and to ensure they can work with an acceptable level of stress to succeed in project work. Therefore the consideration of individual feelings and perceptions is crucial for the motivation of staff, the trust in the organization and a healthy security culture. 67% of respondents would feel safe,

if the organization would implement a professional SRM setup in the field (figure 42 Annex A). On the other hand only 15% would feel safe without a professional SRMS (figure 43 Annex A) while more than 42% would not feel safe; 11% would even reject a position in insecure environment without any SRM setup. This fact shows that motivation of staff, the trust in the employer and the recruitment of potential high qualified technical personnel is dependent upon the existence of SRM. In consequence it indicates a weak security culture and that the safety and security of staff is perceived not being first priority.

One aim of the research was to review the SRM setups used by the focus groups working in NIC countries. The analysis of HRM sub-processes and characteristics discovered that there is a tendency that PBEs are neglecting the analysis of the context (38.9%), the conflict (38.9%), the definition of a security risk threshold (38.9%) and the implementation of a proper security risk management strategy. PBEs are strong in the implementation of risk assessment processes (78.9%). In average only half of the PBEs are implementing preventive security risk mitigation measures or emergency planning (e.g. SOPs (55.6%), medical evacuation or hibernation, relocation, evacuation (55.6%) or emergency planning (50%)). Only 44.4% of PBEs are actively planning business continuity in terms of SRM. Only 50% of errors, near miss incidents and incidents are reported to the respective HQs. This is why PBEs are ranked in figure 2 with the second lowest result after political foundations, reflecting a low degree of security culture and a low level of SRM. In consequence, PBEs show a low level of HRM. (I)GOs and (I)NGOs spend roughly the same attention to the characteristics of HRM. The biggest difference between the focus groups is located in the definition of a security risk threshold. 57.9% of (I)GOs defined an acceptable risk threshold while 75% of (I)NGO and 61.1% of PBEs did not. This might be grounded in the fact that (I)NGOs and Humanitarian Organizations are strongly based on humanitarian principles and through their definition of identity they are dedicated to the people in need and the support for the beneficiaries has first priority. Their SRM strategy is one-dimensional and based on an acceptance approach to ensure the safety and security of their employees. An interviewee from an (I)NGO stated that the one-dimensional application of an acceptance approach ensures the identity of (I)NGOs and Humanitarian

Organizations and therefore the safety and security of staff better than a protection or deterrence strategy compromising the identity of the organization and therefore the safety and security of staff. Contrary to this statement Marc Houben (2012) stated: *'It is no longer relevant whether you carry a weapon or not. It is relevant whether you carry values and that makes you to a legitimate target.'* He means that an acceptance approach is not enough anymore to ensure the safety and security of staff in the field.

Nevertheless, only 37.5% are using the strategic instrument of counter threats while applying a multi-dimensional strategy of acceptance (participation of the host nation, e.g. beneficiaries, target communities, affected communities; based on local ownership, do-no-harm approach), protection (use of protective measures, e.g. technical equipment), deterrence (applying a counter threat, e.g. armed security) or avoidance (withdrawal from an area or avoidance of certain areas). The SRM of PBEs is based on corporate security principles and therefore is based on protection, deterrence or avoidance. The flexible implementation of a broader security risk management strategy would foster security change management and positively contribute to the security culture. In general evidence is provided that PBEs are lacking a security risk management strategy and the definition of a risk threshold.

The services provided as part of the SRM-systems by the three focus groups show that (I)GOs reached a perceived high level of service provision for their staff to ensure a safe and secure environment in NIC countries but are still lacking management commitment and the attribution of necessary resources. The weakest characteristic in (I)NGOs are the process of lessons learned after incidents (30% of (I)GOs) and Crisis Communication and PR services (45% of (I)GOs). The cause may be a lack of feedback and reporting culture and the lack of a just culture environment which enables staff to report confidentially and blame-free. Another cause may be the political pressure towards (I)GOs to avoid errors and negative media reporting which may negatively impact the reputation and credibility of the responsible government. A cause for the low level of crisis communication may be internal agreements with the governmental media departments about a restrictive communication policy. A similar tendency in comparison to (I)GOs can

be seen in the implementation of HRM characteristics in (I)NGOs. Roughly 50% of (I)NGOs implemented HRM characteristics. Nevertheless, there is a lack of lessons learned (29.4% of (I)NGOs), the provision of transportation in terms of airport facilitation and disposition of office vehicles as well as crisis communication (35.3% of (I)NGOs) and PR services (35.3% of (I)NGOs). There are only 52.9% of (I)NGOs implementing proper crisis management procedures in NIC countries. The cause can be found in a lack of financial and HR resources and a lack of risk education (pre-deployment training and security risk management training) and therefore indicates a weak security culture. The focus on services in PBEs is manifested in travel security (77.8%), information distribution (66.7%), crisis management (66.7%) and the briefing about security (61.1%) as well as the individual advice to employees or programs (66.1%). The lowest attention is paid to site security (38.9%), transportation and disposition of vehicles (27.8%) as well as crisis communication and PR services (22.2%). The focus on technical protective measures may be caused by the professional training of security risk management advisors for corporate security units. In consequence, (I)GOs are prepared best for operations in NIC countries, followed by (I)NGOs and PBEs in terms of SRM (figure 46 - 54 Annex A). It can be argued that the implementation of HRM in NIC countries would foster the safety and security and create an acceptable work-environment for employees, the operational excellence of organizations and thus the success of programs and projects.

In general there is an improvement of professional SRM in comparison to the past research conducted by the Humanitarian Policy Group. Gains made by organisations working in NIC countries are still not leading to SRM systems that fully reach the level of HRM. Thus SRM systems of organizations operating in NIC countries, especially in high risk and fragile environments reach neither the level of excellence nor professionalism required. It can rather be described as *blissful ignorance*. Reasons for this may be grounded in the lack of commitment by top management, no allocation of necessary resources and the low esteem for SRM.

Taking all results from the online questionnaire and interviews into consideration, (I)GOs reach a percentage of 64.75%, (I)NGOs of 63.38%, PBEs of 59.63%, UN of 92%

and political foundations of 38% in the assessment of the eight dimensions of security culture, respectively the drivers of security culture. The level of SRM was assessed according the presence of characteristics, reaching 63.50% in (I)GOs, 51.96% in (I)NGOs, 46.05% in PBEs, 77% in the UN as well as 23% in political foundations. The analysis shows that a weak security culture in organizations is resulting in a low level of SRM and vice versa (figure 3). Chapter 4 provides evidence that there is causal relationship between security culture and the level of SRM and therefore influences the level of HRM.

Chapter 5 Conclusion and further research

The fifth chapter summarizes the findings from the research and emphasises the causality. It reflects how the evidence discussed in the previous chapters proves that there is causality between the level of security culture and the degree of SRM measures which leads to a certain level of HRM. Furthermore it outlines issues for further research since the topic of HRM or security risk management represents a complex framework.

The research intended to gather data about focus groups and to analyse if there is a difference between the SRM concepts applied by the different organizations. In a second step, the existence of causality between security culture and the degree of the implemented SRM measures was analysed. The findings are that an analysis of security culture based on a single framework is not possible due to the complexity and the tightly coupling sub-cultures such as *just culture* as well as legal and social requirements. Each organization is unique and implements SRM concepts based on individual corporate requirements. But the analysis has shown that standard concepts of corporate security approaches are not applicable and sufficient for NIC contexts. The HRM model combines security culture, good practices and lessons learned as well as minimum standards in SRM in NIC countries. No focus group that was analysed in this dissertation fulfils HRM requirements entirely. There is even a lack of adherence in insurance minimum standards present in organizations.

The analysis of Ruighaver's et al (2007) along Detert's et al eight dimensions provides a good framework to analyse the existence and the degree of security culture in

organizations. The data gathered was used to test the relationship, connection and interaction of SRM and security culture. Evidence was found that a lack of implementation of drivers of security culture negatively impacts the degree of security culture. Again a weak security culture results in a low level of quality of SRM implemented which leads to a low level of HRM. On the other hand a low level of SRM measures shows a low level of security culture in organizations. There have not been any indicators that there are organizations with a strong security culture but a low level of SRM measures implemented or a weak security culture but a high level of implemented SRM measures. In consequence the degree of HRM is dependent on the level of security culture and the level of SRM measures. It has been identified that the most critical drivers of security culture that determine the level and quality of SRM are the commitment of top management in the respective organizations, as well as the direct exchange of information between security professionals or focal points and the management. Most of the organizations from all focus groups lack the commitment by senior management and direct reporting lines, clearly defined roles and responsibilities as well as mandates. Additionally there is a lack of quality control from HQ for SRM in the field.

In most of the organizations the formal framework of SRM is present but the basis of truth and the balance between perceptions and believes about the importance of security by employees, the management and the organization conflicts in reality. As a result a weak security culture hinders proactive security risk management and therefore hinders HRM in NIC countries. Evidence was provided by the fact, that incidents could have been avoided if the organization would have implemented appropriate setups or measures (figure 20 Annex A).

The comparison of setups of PBEs with the setups of (I)GOs and (I)NGOs confirm that (I)GOs and (I)NGOs are focussing more on comprehensive setups to protect their operations rather than traditional standard models (e.g. corporate security management) used by PBEs. Nevertheless, PBEs concentrating on transparent and qualitative models of risk management while (I)GOs and (I)NGOs are lacking standard methods. A major difference between the focus groups is the use of risk management strategies. (I)NGOs

based their strategy on an acceptance approach and they believe that their identity as humanitarian or development actor provides sufficient protection. PBEs are focussing on protection and deterrence strategies, rarely applying acceptance approaches. The application of a mixture of required SRM strategies is dependent on the security culture in organizations including their world view and their definition of their identity. This leads to the assumption that no focus group implemented the required strategies for NIC countries entirely which consequently leads to deficiencies in their applied SRM measures.

Finally, taking into account earlier research on the issue the security culture of organizations working in NIC countries improved significantly since 2011. Nevertheless, taken the increase of insecure environments into consideration, none of the types of organizations under consideration here are fully prepared to deal with an increasing number high risk and fragile contexts and incidents. As argued by different researchers such as van Brabant, organizations and their top management should take their legal obligation for duty of care as well as their social responsibility towards their staff seriously. Systems and success are driven and carried by its employees. Safety and security is a value for industrialized countries worth to be protected; for the target community, the partner countries, the people in need and their own employees. Organizations should focus on long-term security risk management planning including the allocation of necessary resources. Top management should be clearly accountable for the safety and security of staff in their organizations as a part of corporate governance.

Having pointed out the main issues and findings of the research, there are many open questions and facts to be taken into consideration in further research. The quality of security culture and SRM, the legal perspective in terms of duty of care or one detailed case study of SRM from an organizational perspective and a top management's or employee's perspective. The analysis has shown that the topic of security risk management or humanitarian risk management has many more issue to offer for further research.

This study focused on the gathering of data based on the opinion and belief of people. A qualitative, comprehensive research of the security culture of a selected few, or

even one organization would contribute greatly to the current discussions. Furthermore the research about the quality of SRM measures and procedures and its impact on security would contribute to a more comprehensive evaluation of procedures and measures used by organizations. This could be done by using the security culture matrix in figure 3, analysing individual organizations. A problem for further research on the impact of SRM on security that is taking the quality and degree of procedures and measures into account is posed by the fact that the method of counterfactuals would need to be applied. This makes it difficult to get reliable data.

A further research topic could be the focus on specific drivers of security culture such as the commitment of top management, why they are committed or not and how they perceive the setup of SRM in organizations.

'It is no longer relevant whether you carry a weapon or not. It is relevant whether you carry values and that makes you to a legitimate target.' Marc Houben, 2012

Statistical Analysis of the Online Survey

Safety and Security Risk Management in non-industrialized countries

Research Data

Statistical Analysis of the Online Survey

Safety and Security Risk Management

By M. Wagner

Background Data:

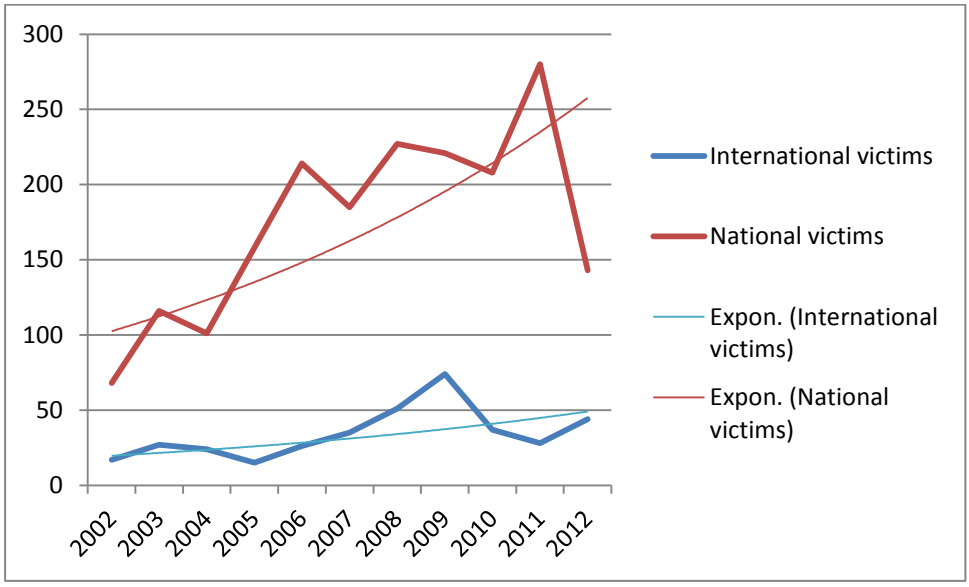

figure 1 © 2012 AWSD

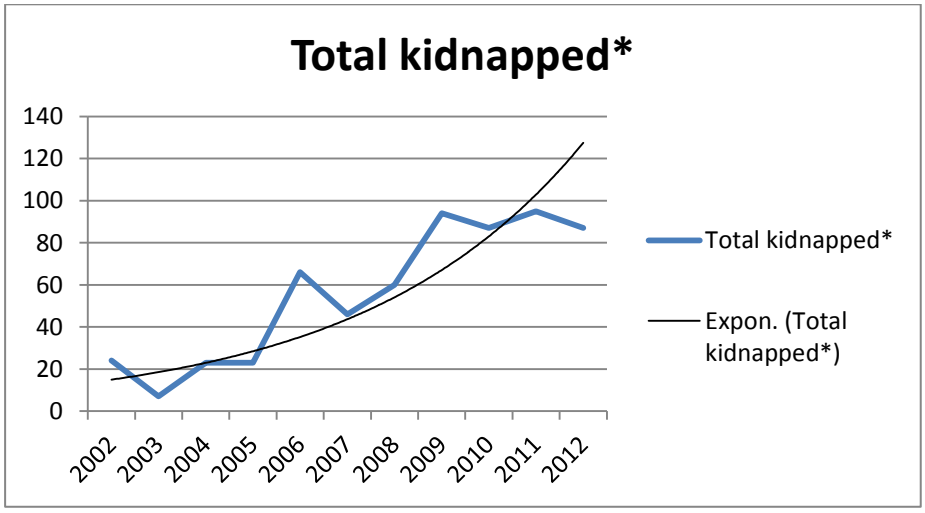

Figure 2 © 2012 AWSD

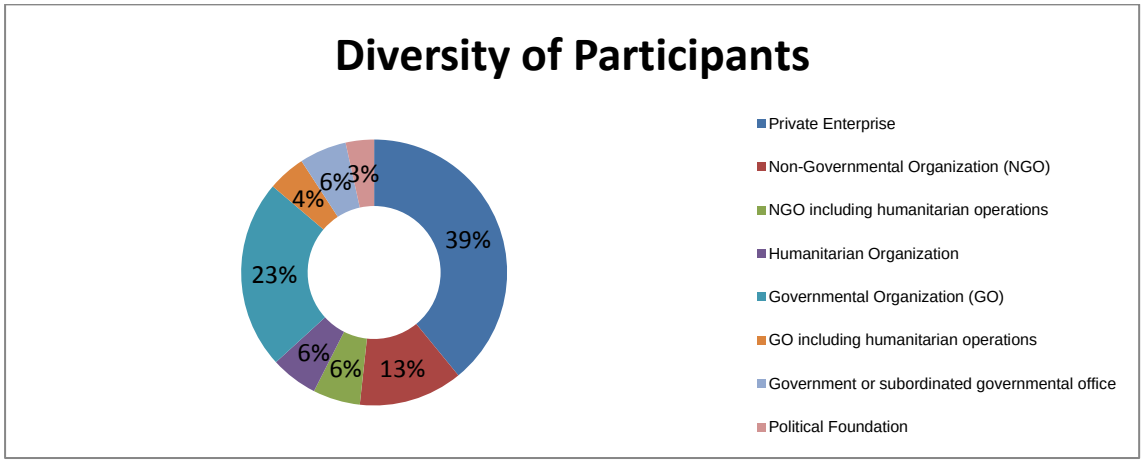

Figure 3 diversity of participants

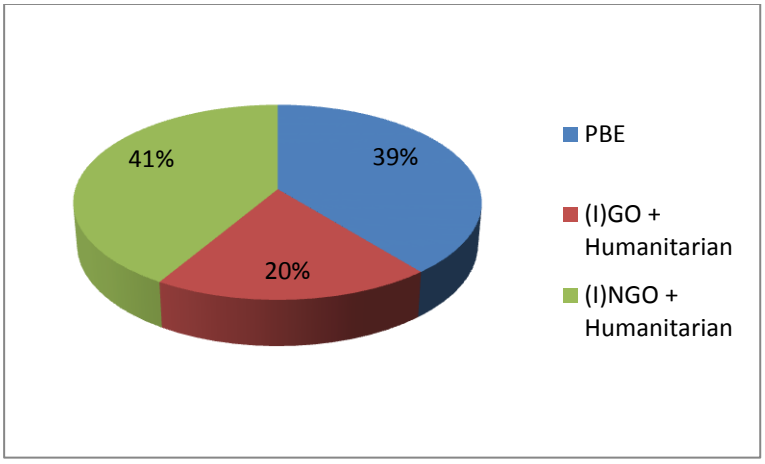

Figure 4 participating groups in %

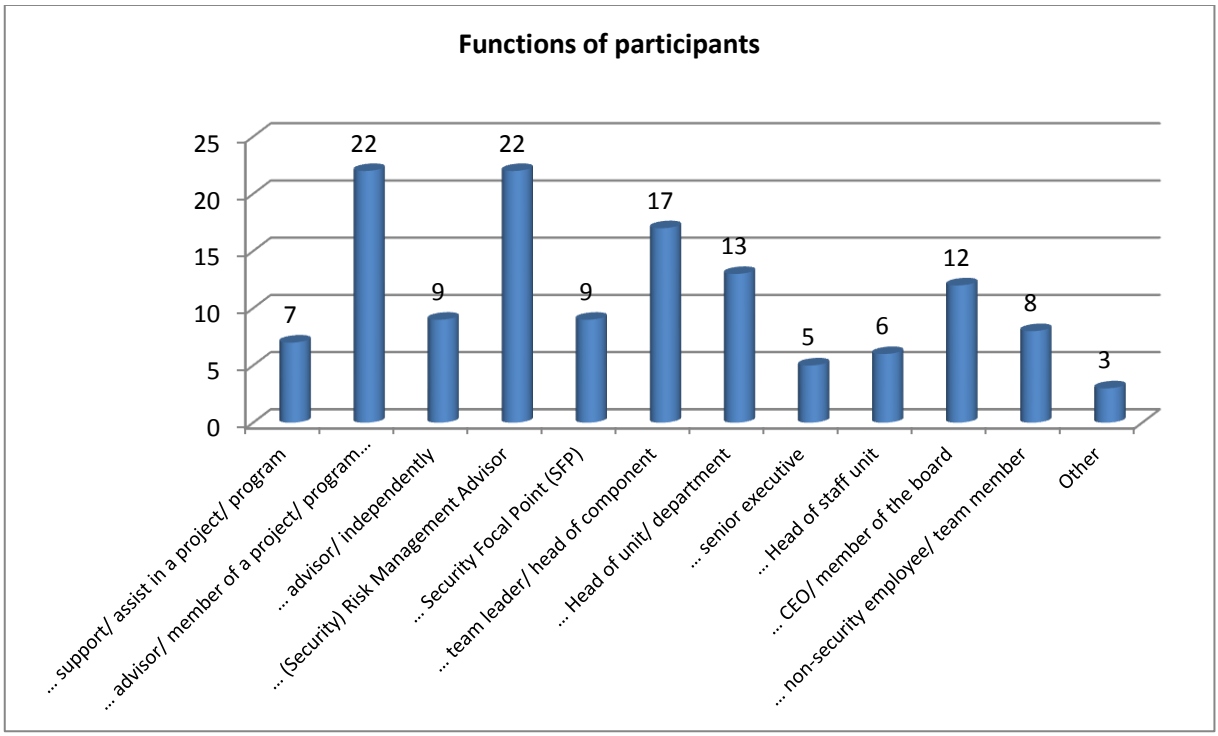

figure 5 functions of participants

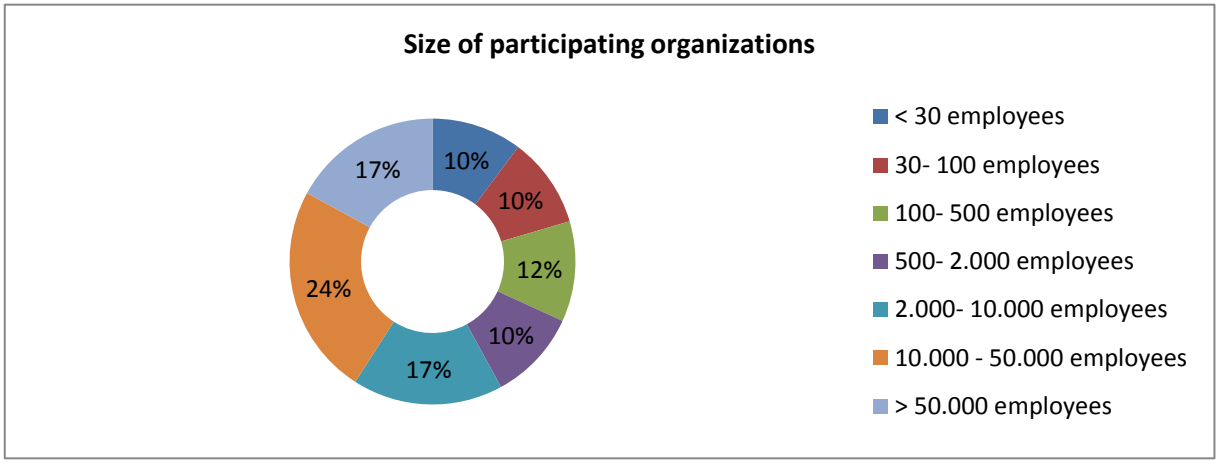

figure 6 size of participating organizations

Overall Assessment based on questions

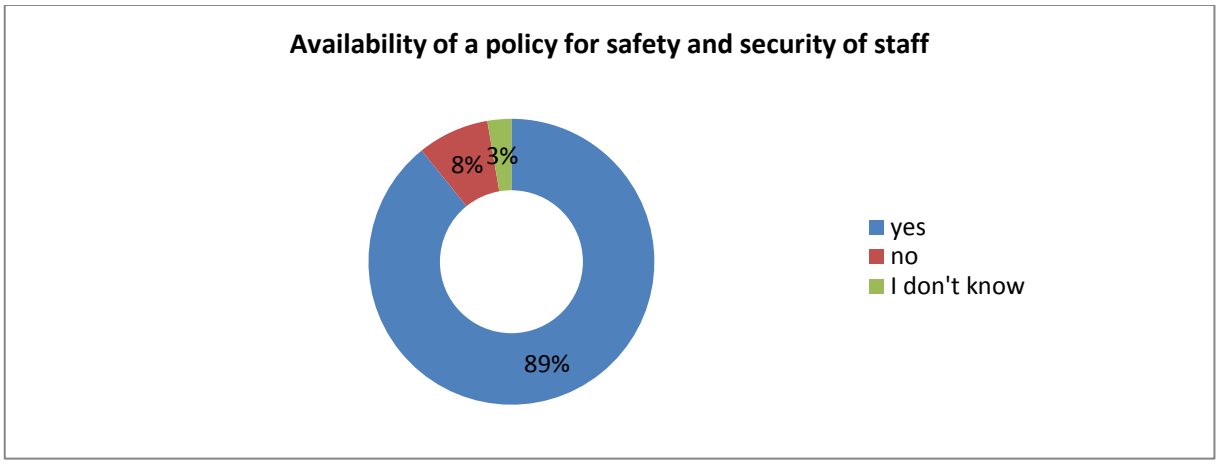

figure 7 availability of a policy

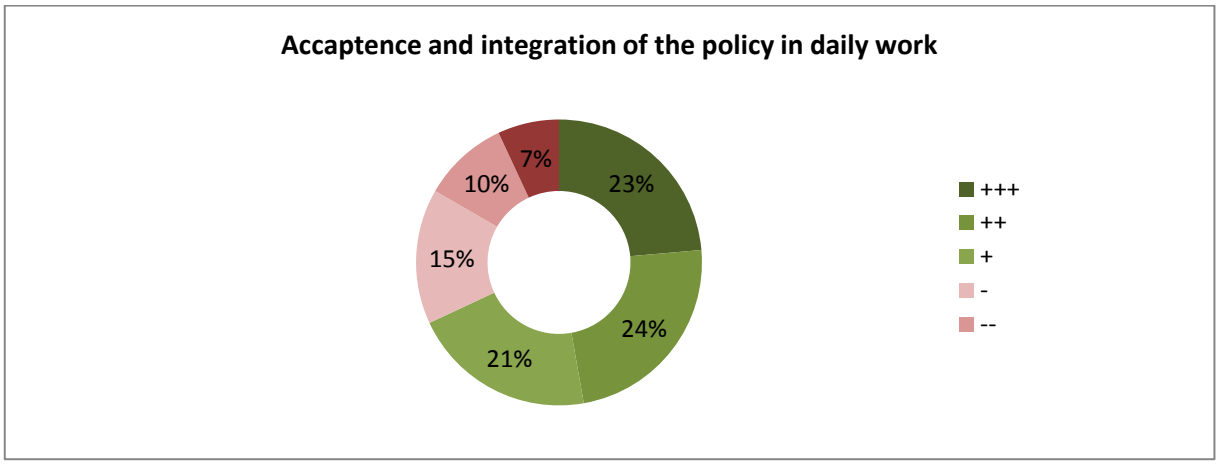

figure 8

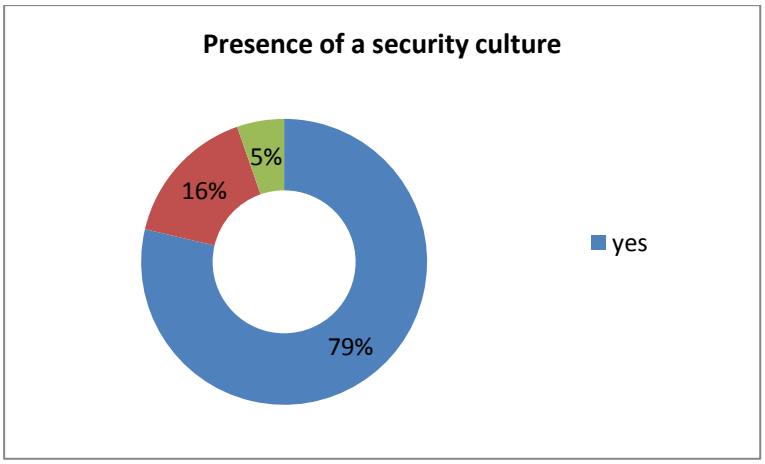

Figure 9

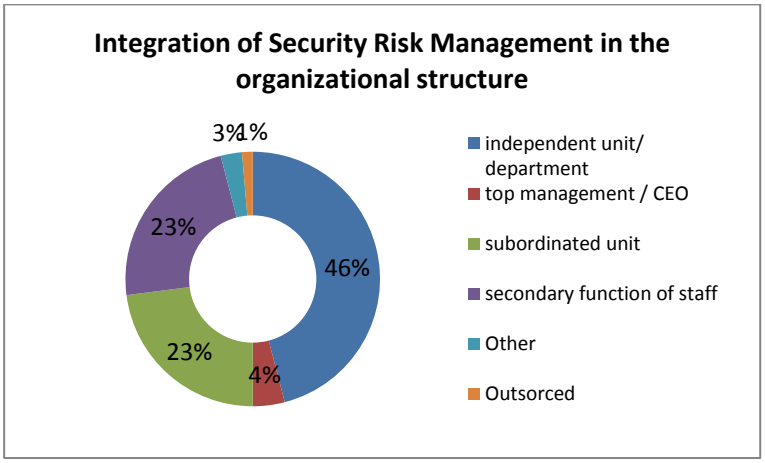

Figure 10

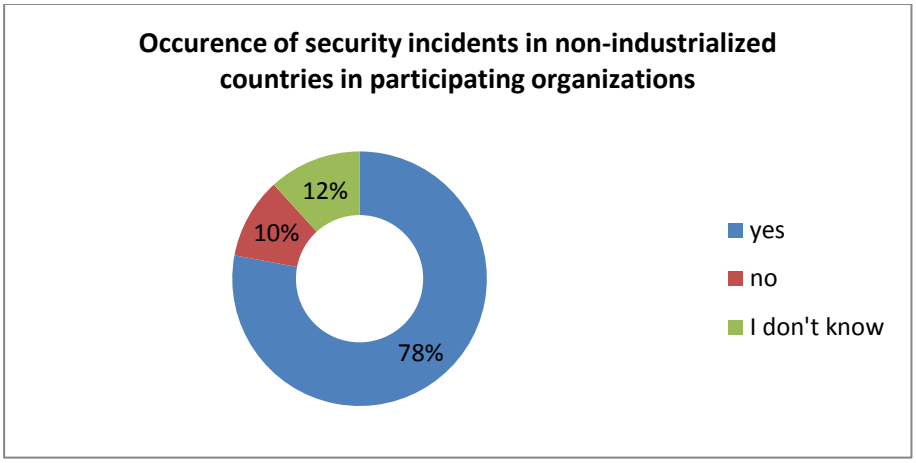

Figure 11

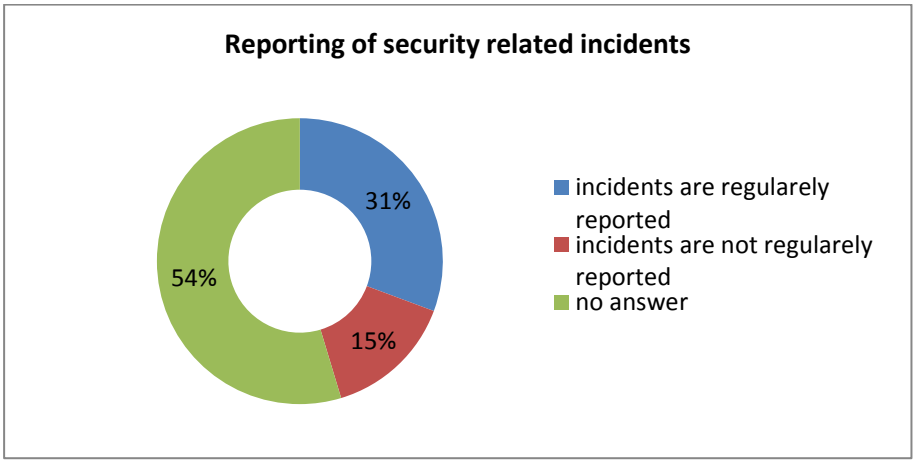

Figure 12

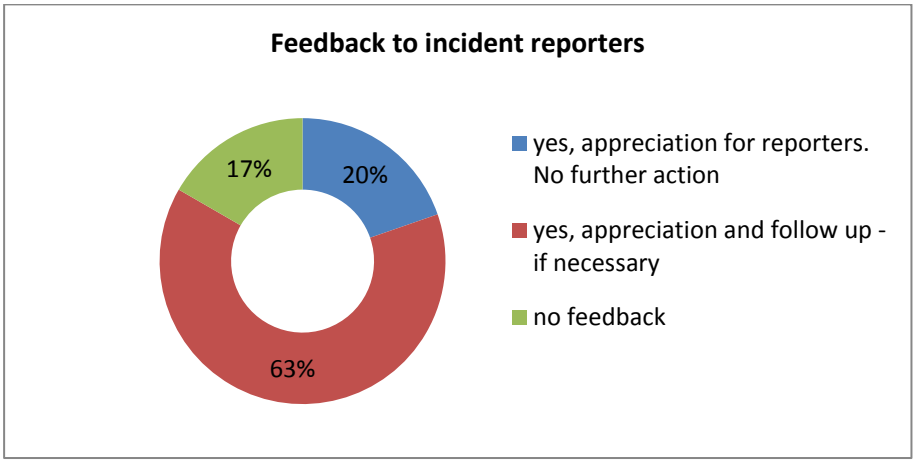

Figure 13

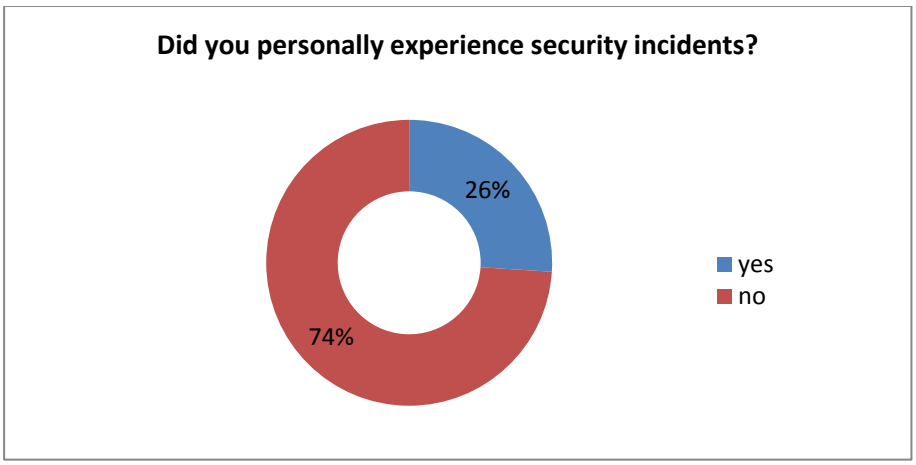

Figure 14

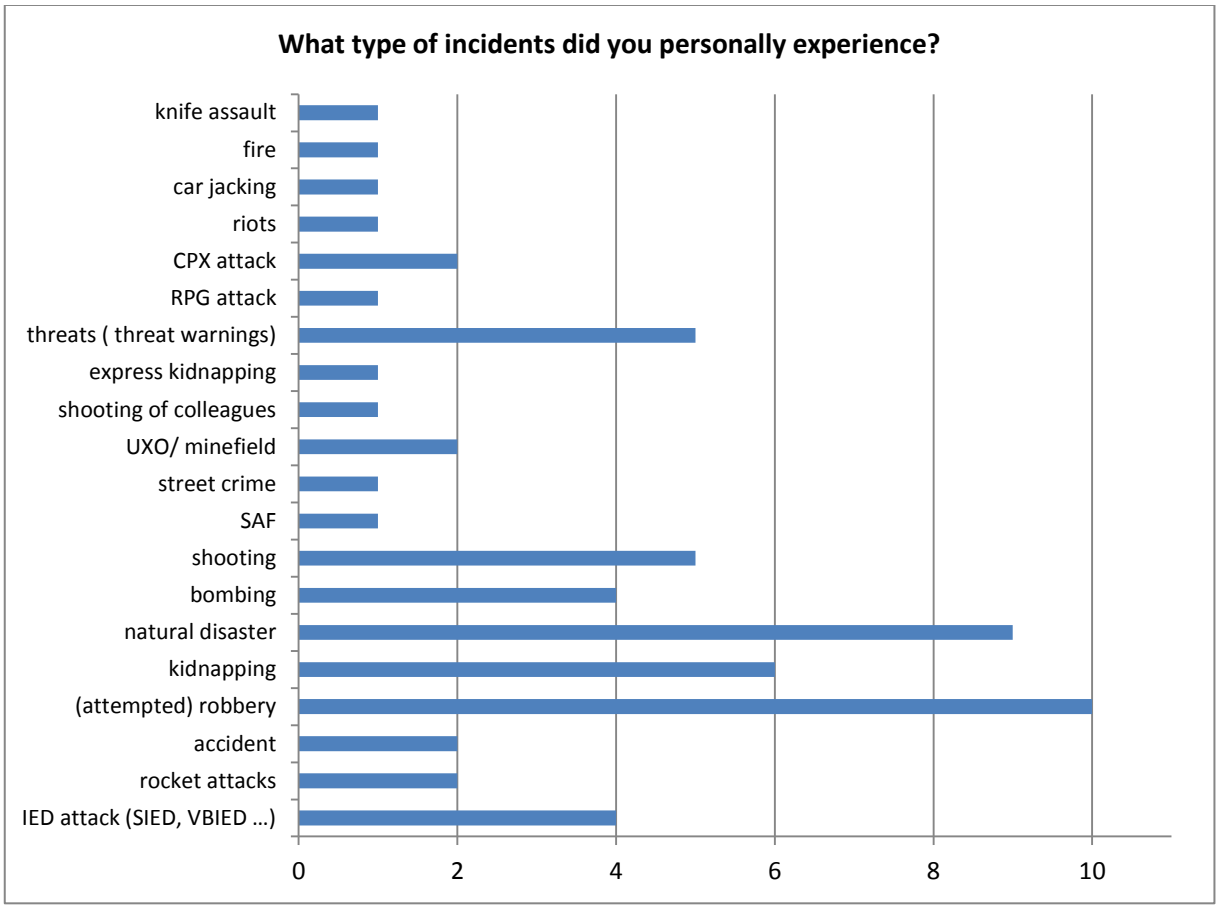

Figure 15

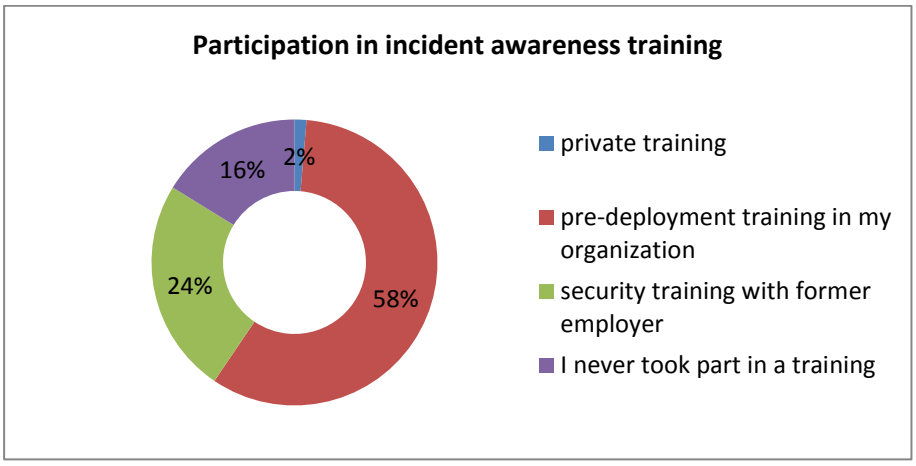

Figure 16

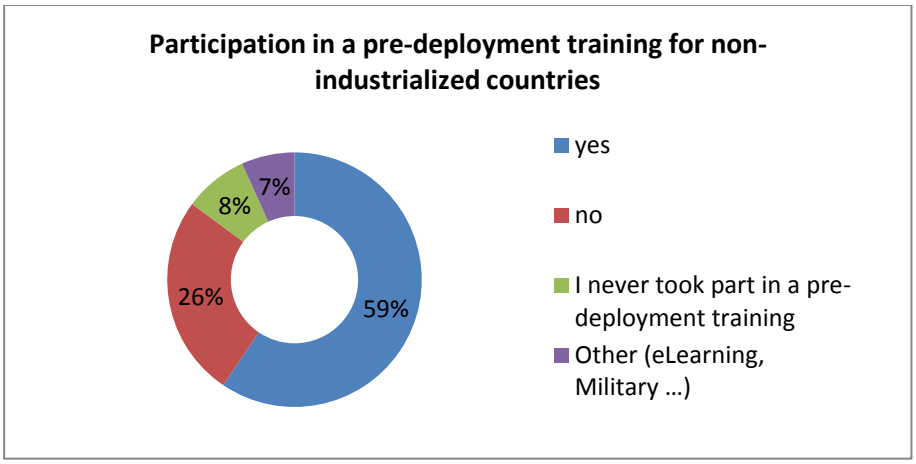

Figure 17

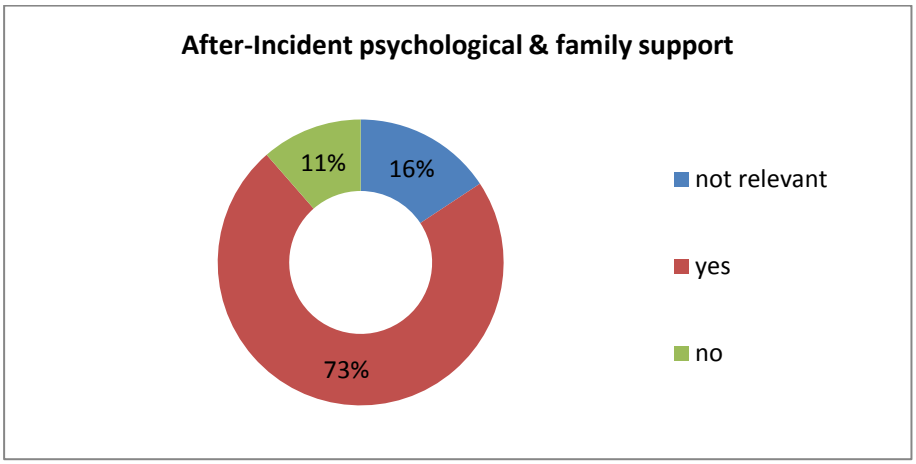

Figure 18

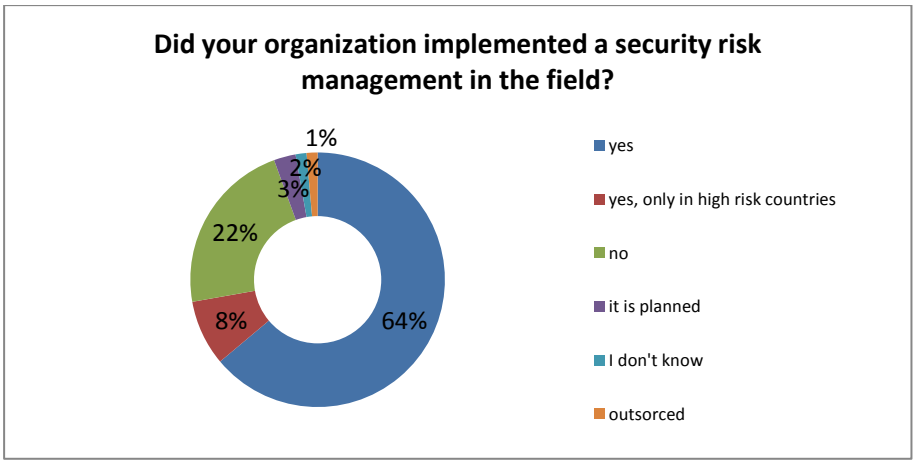

Figure 19

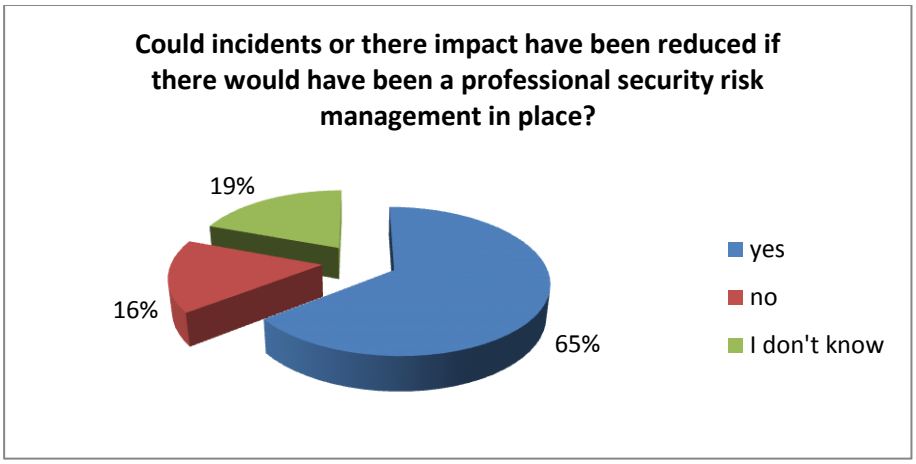

Figure 20

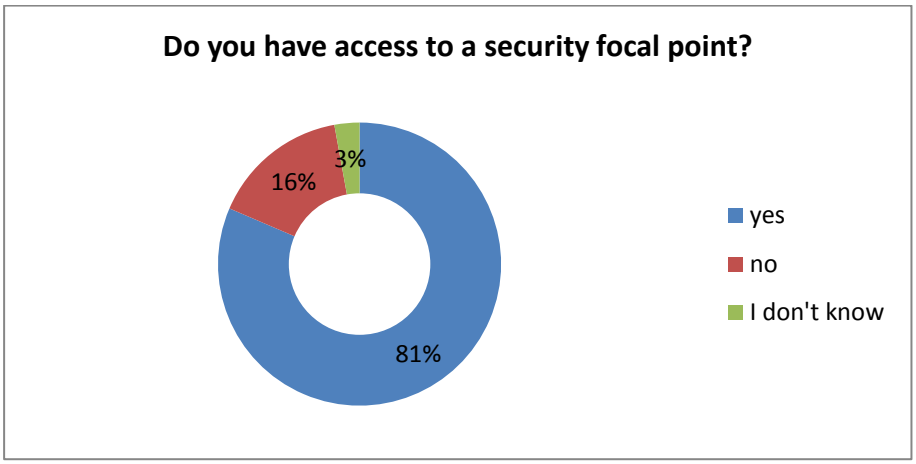

Figure 21

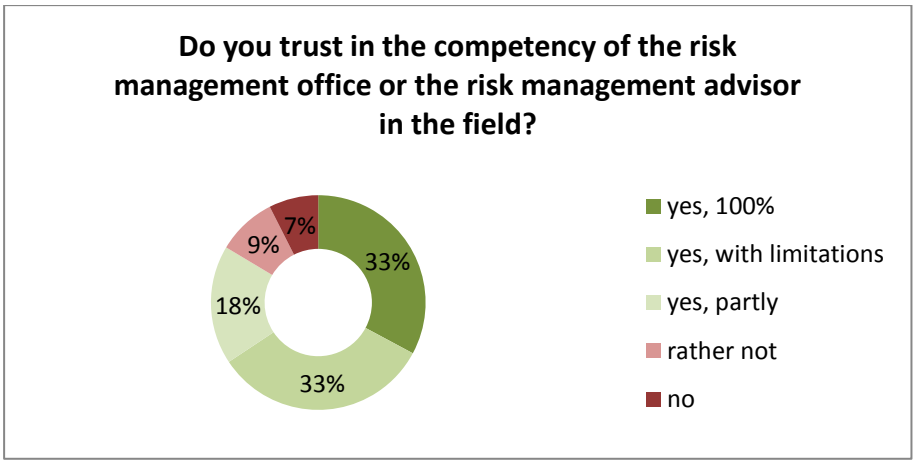

Figure 22

Figure 23

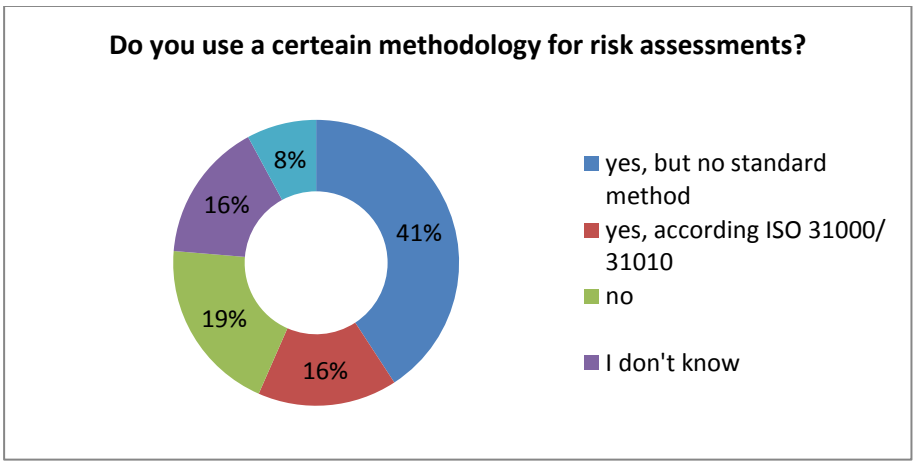

Figure 24

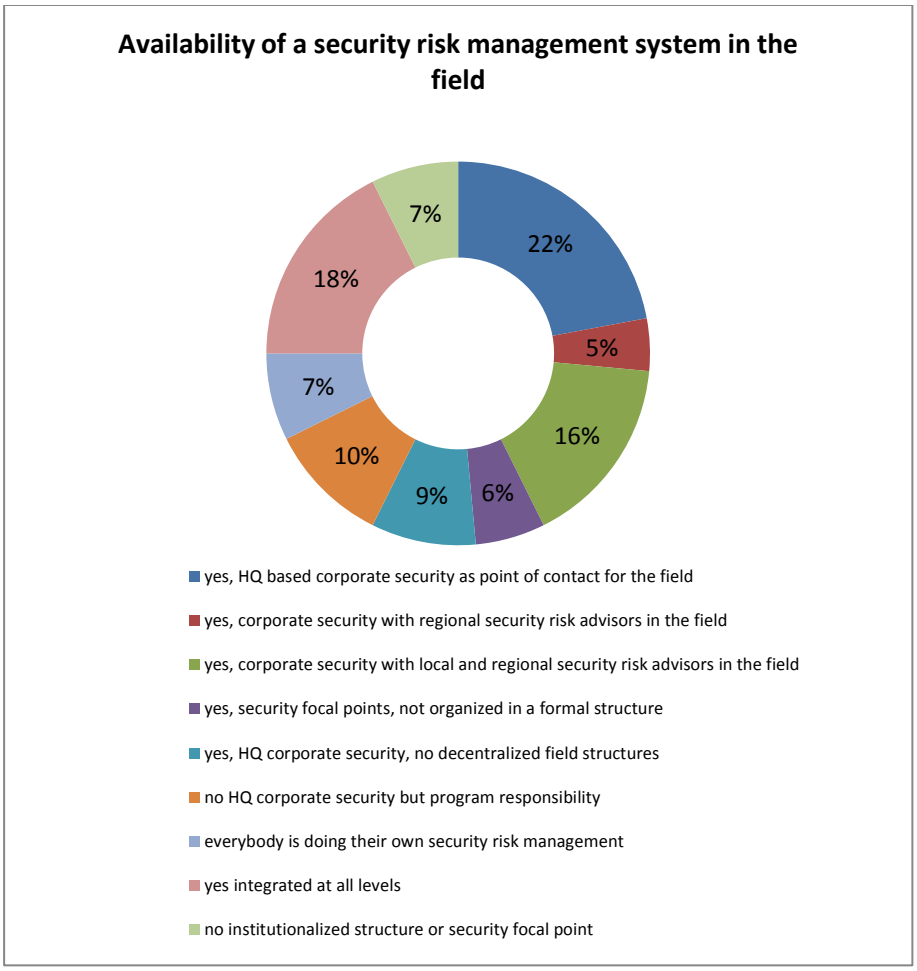

Figure 25

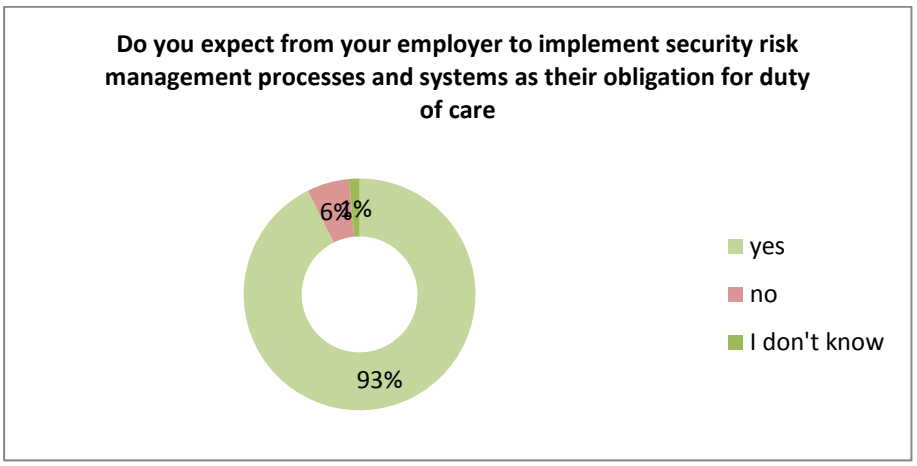

Figure 26

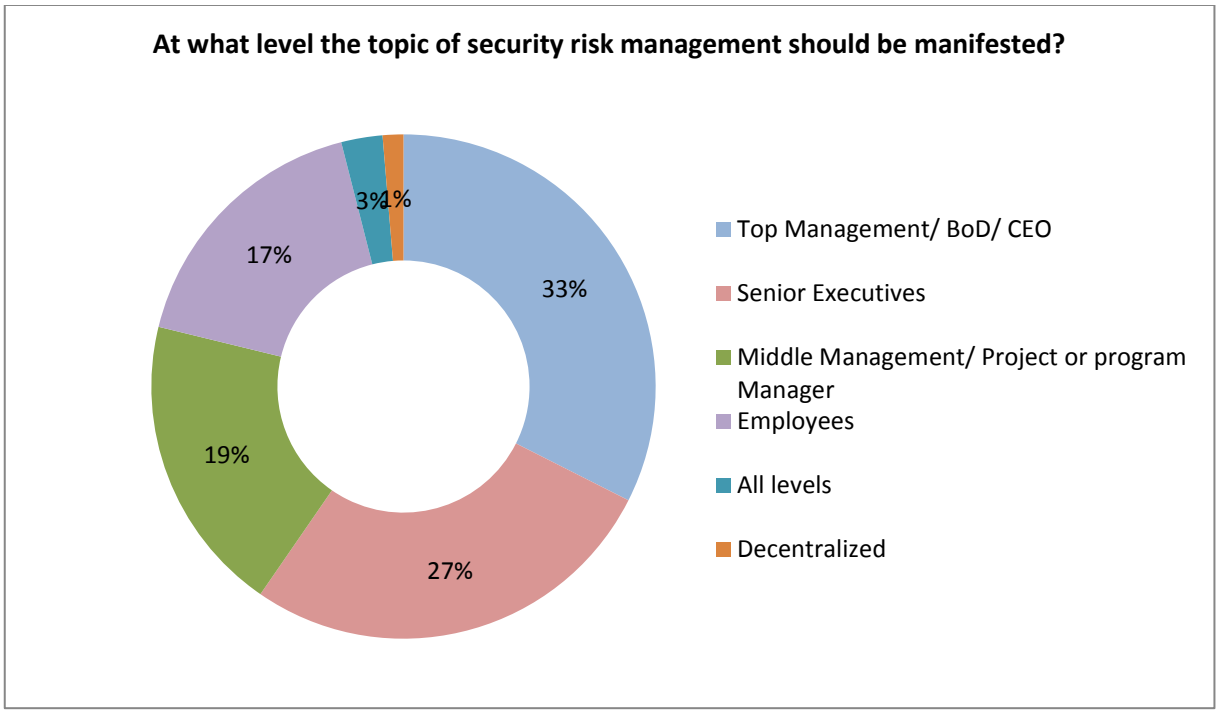

Figure 27

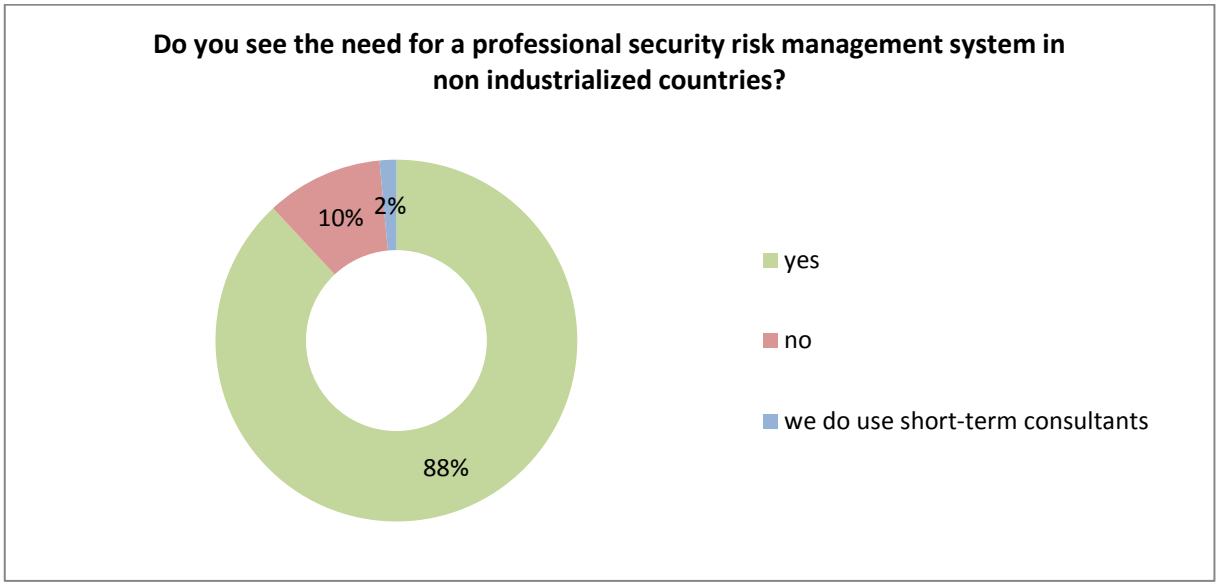

Figure 28

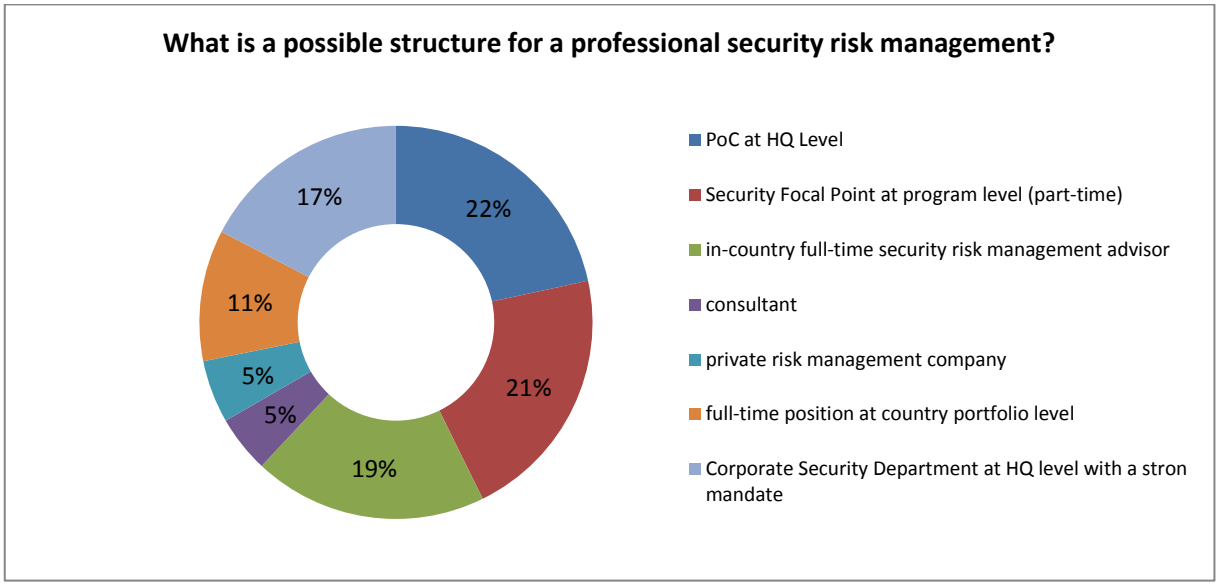

Figure 29

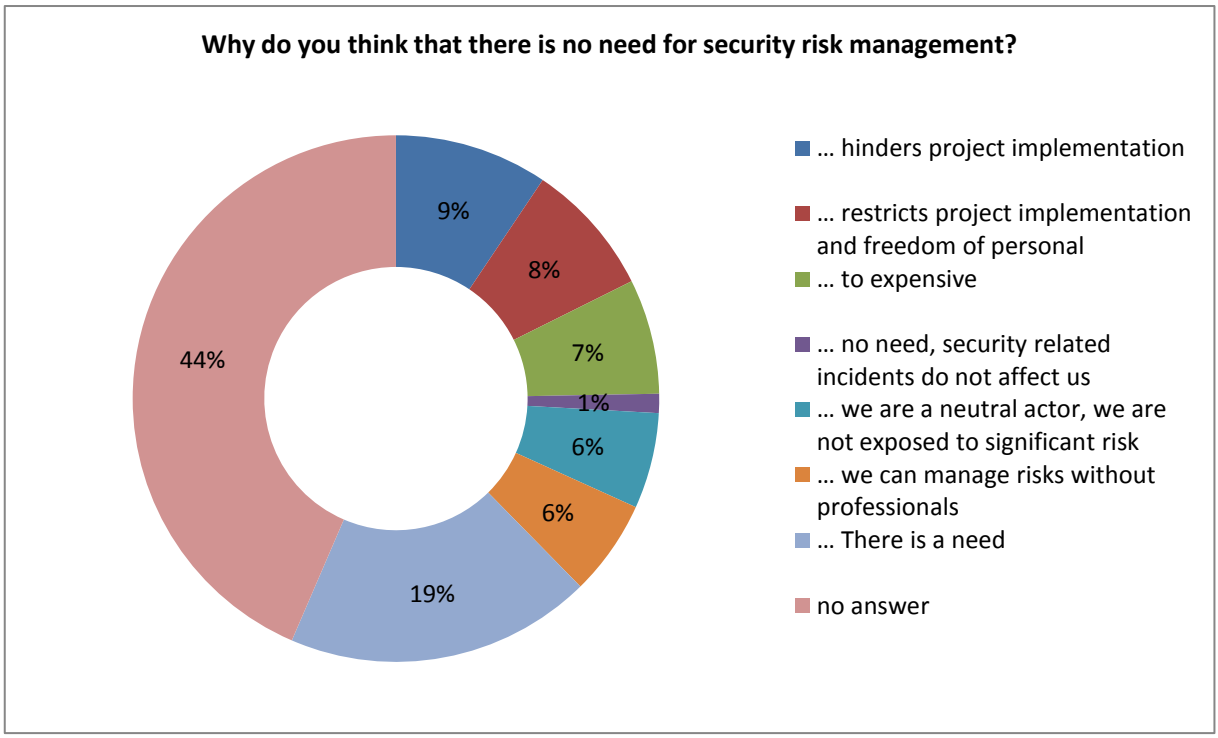

Figure 30

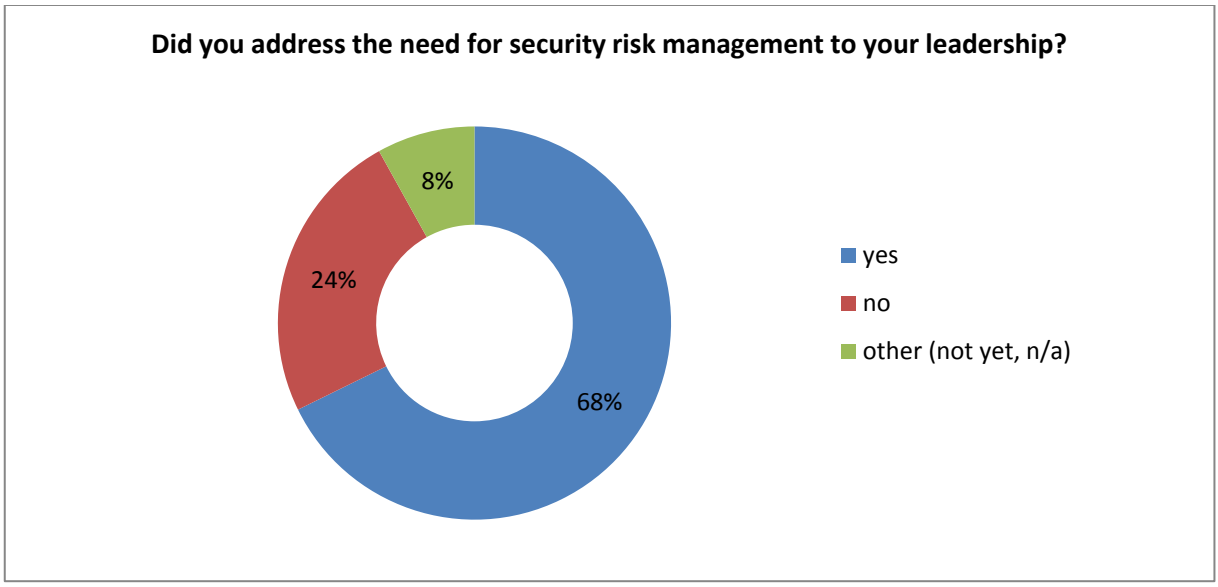

Figure 31

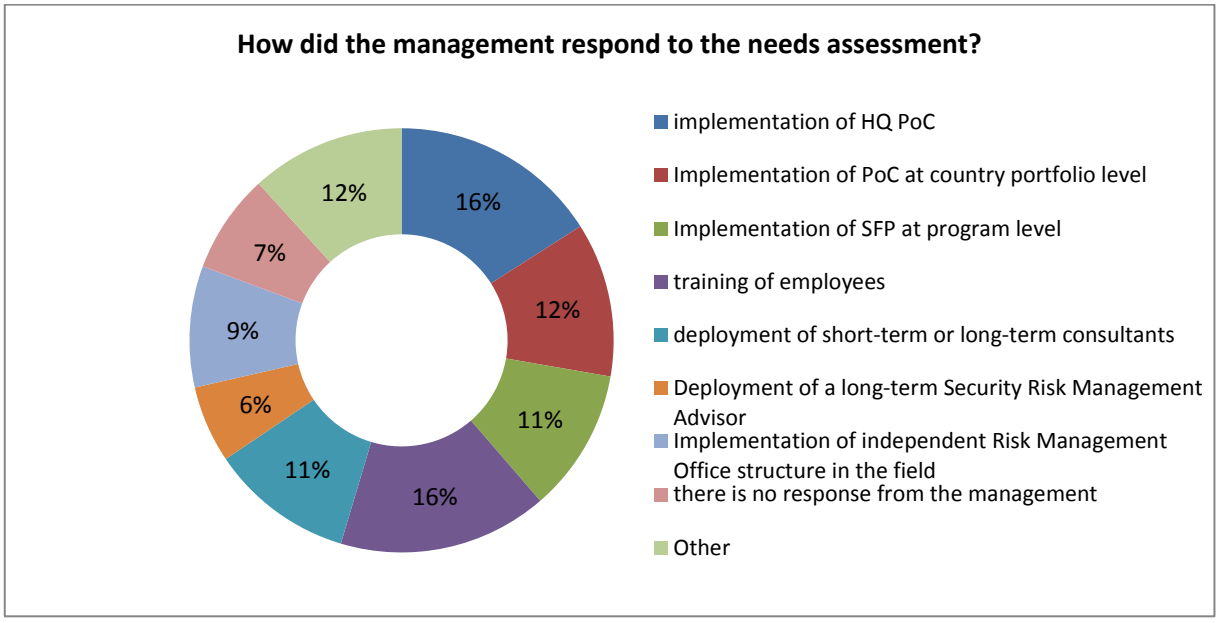

Figure 32

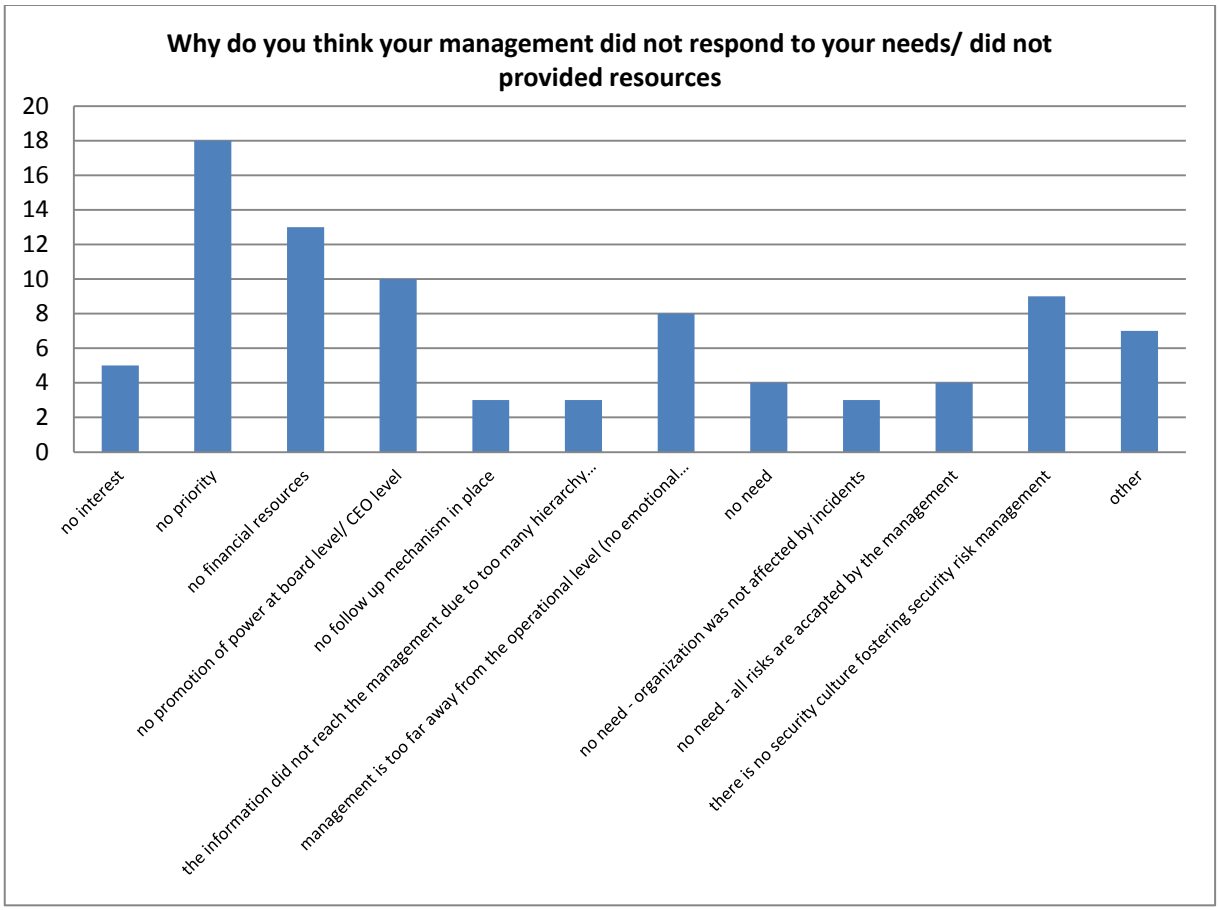

Figure 33

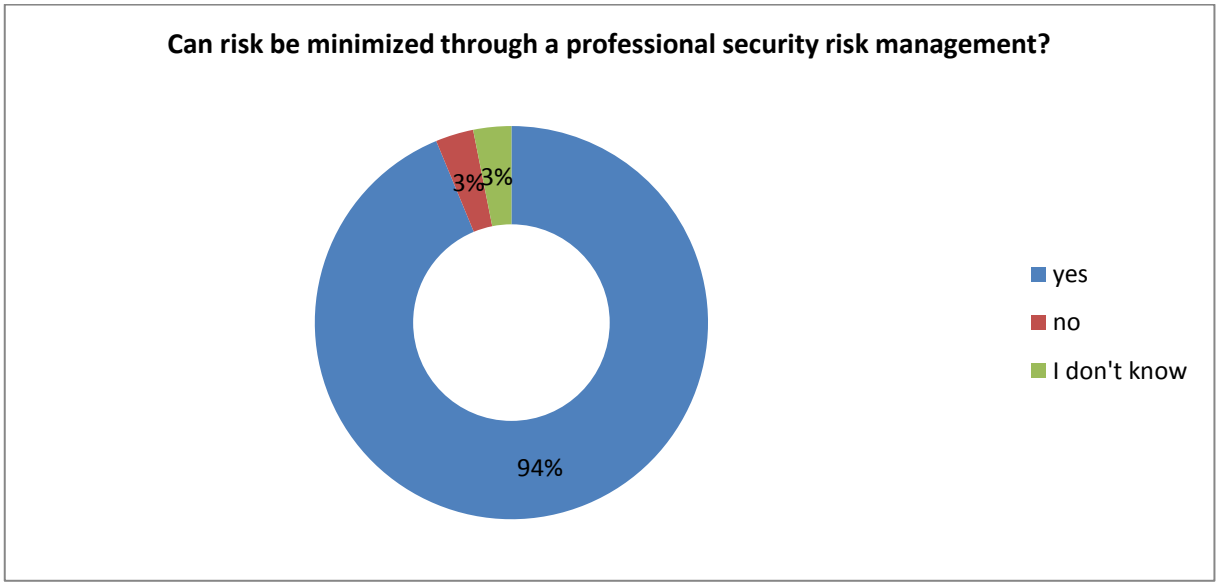

Figure 34

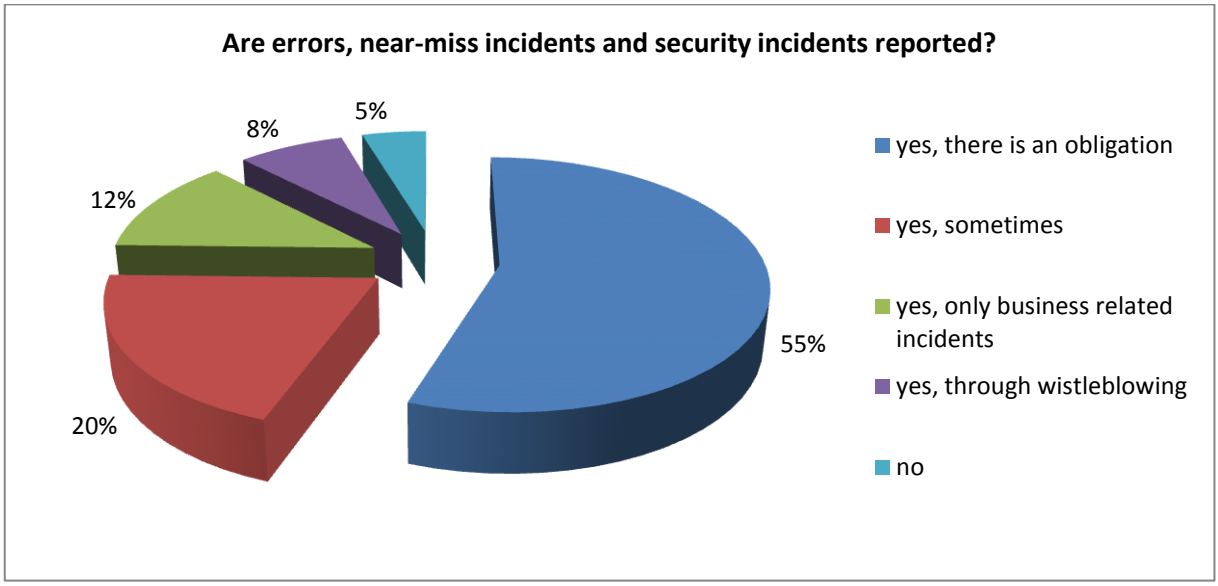

Figure 35

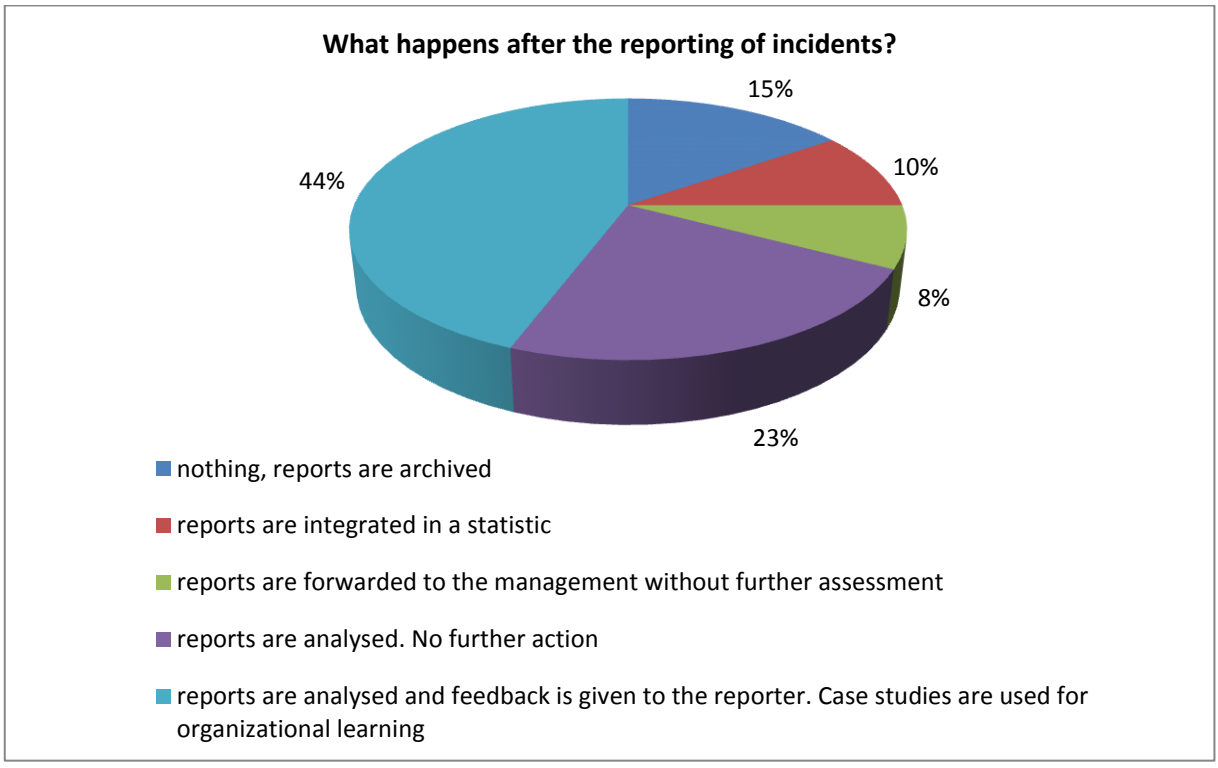

Figure 36

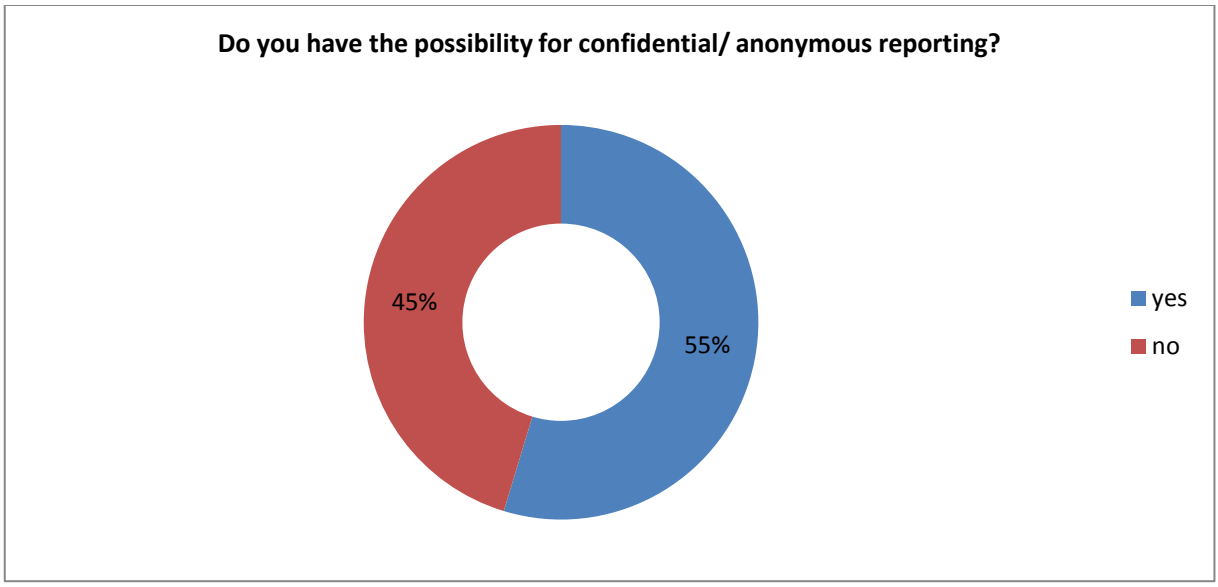

Figure 37

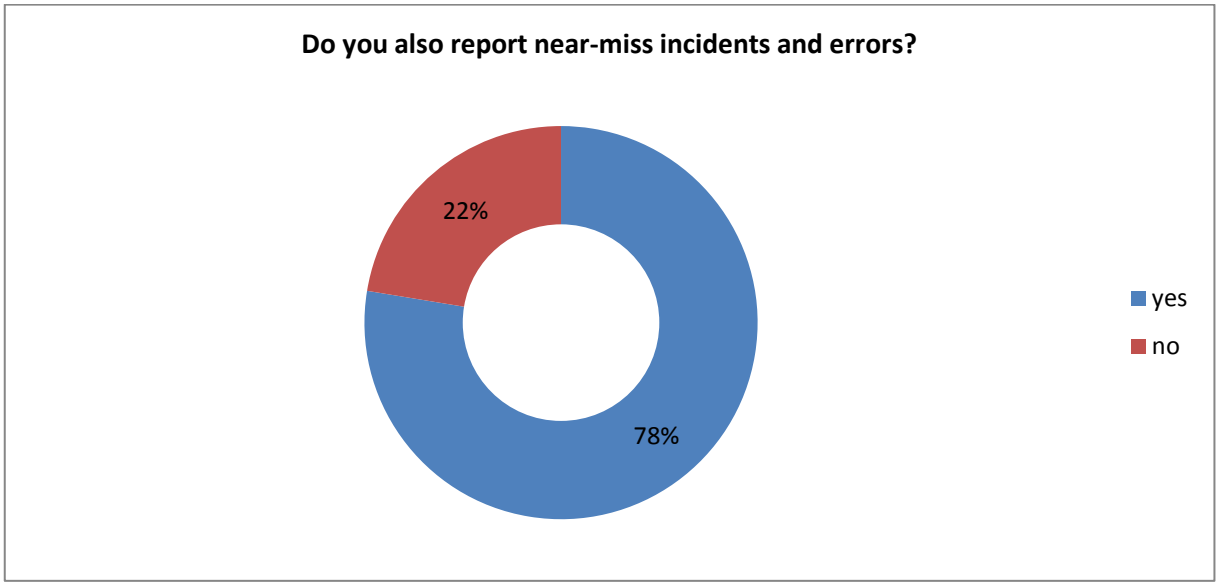

Figure 38

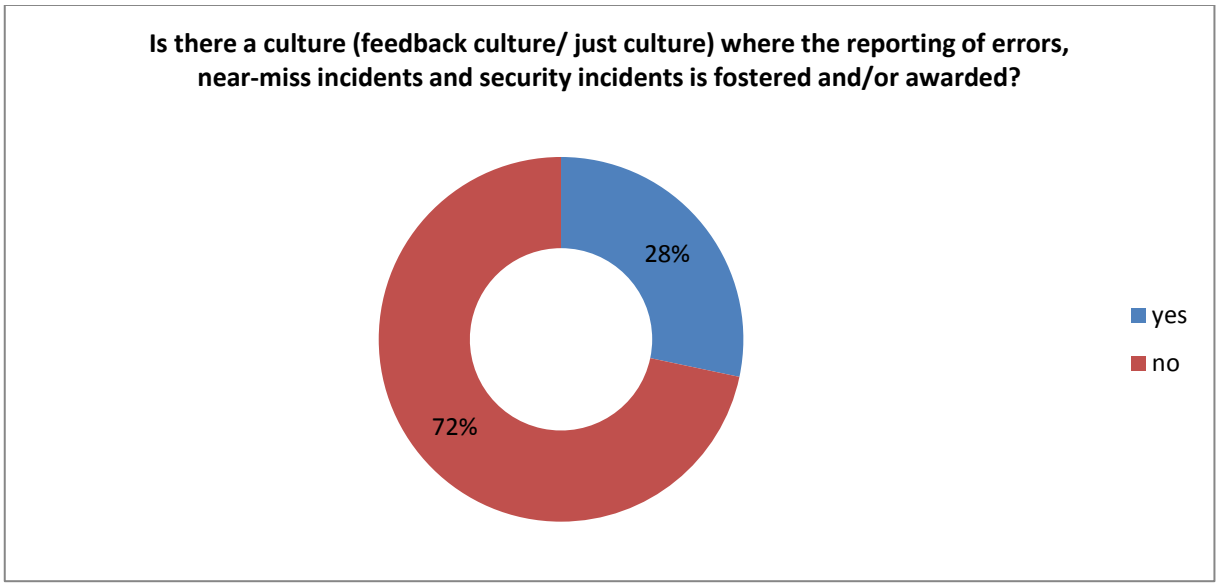

Figure 39

Figure 40

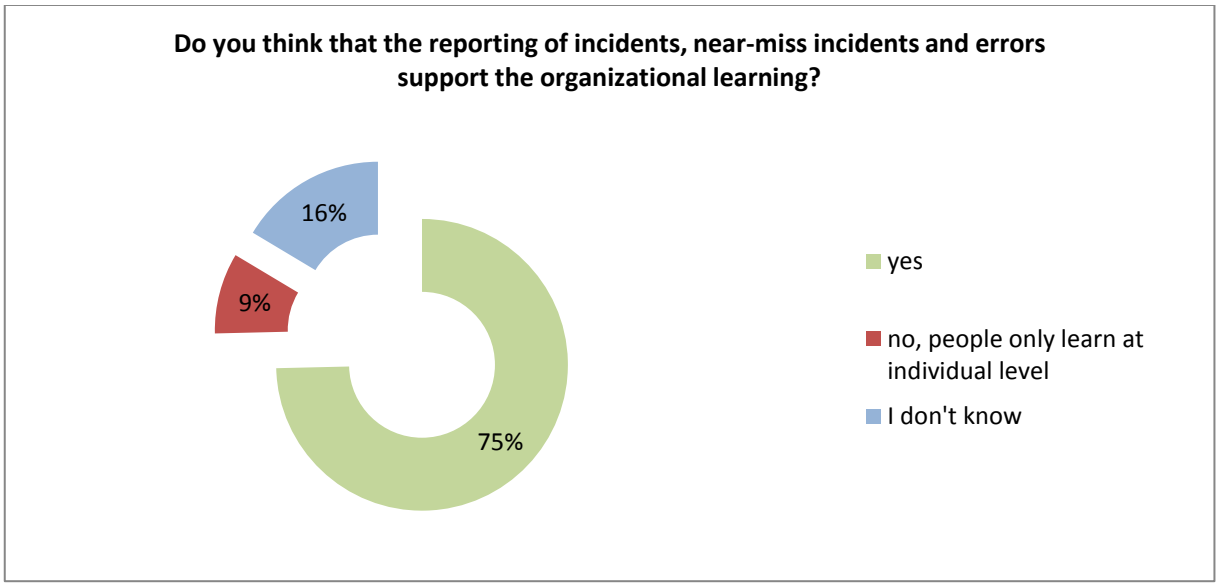

Figure 41

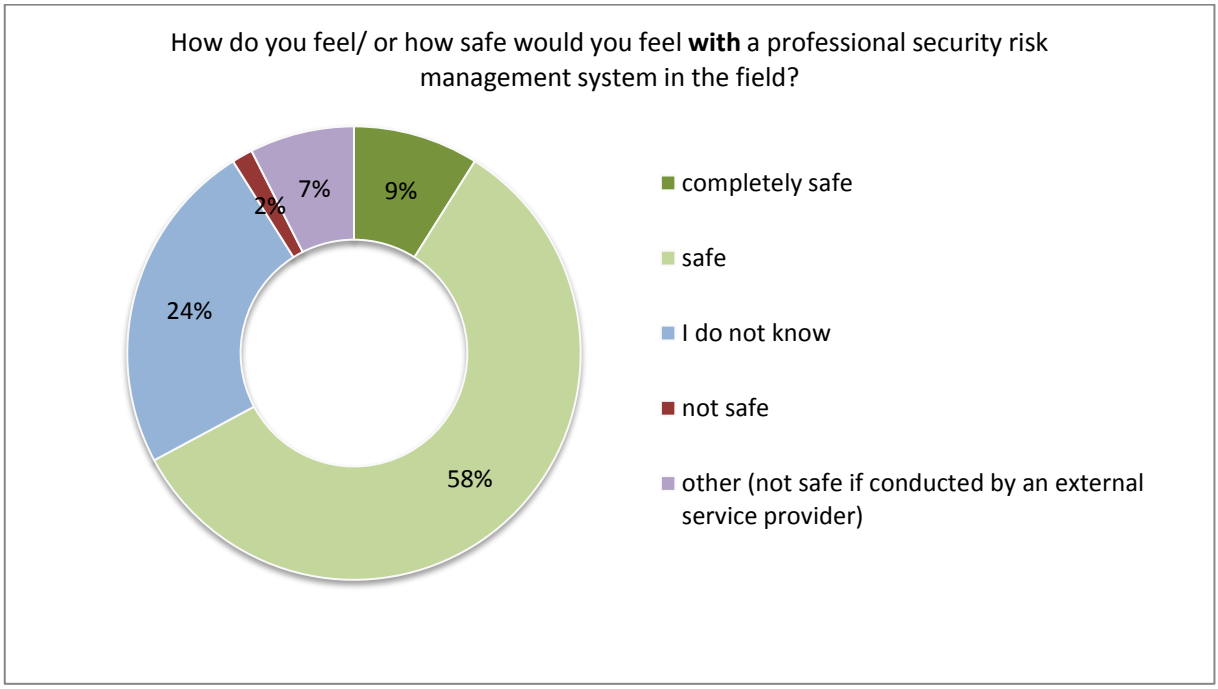

Figure 42

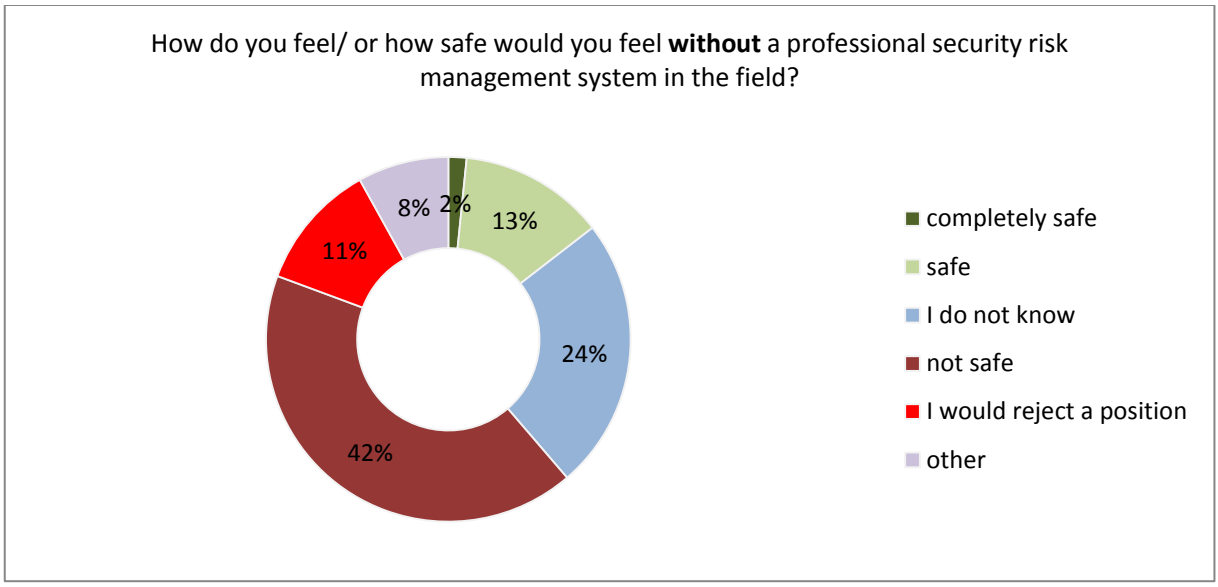

Figure 43

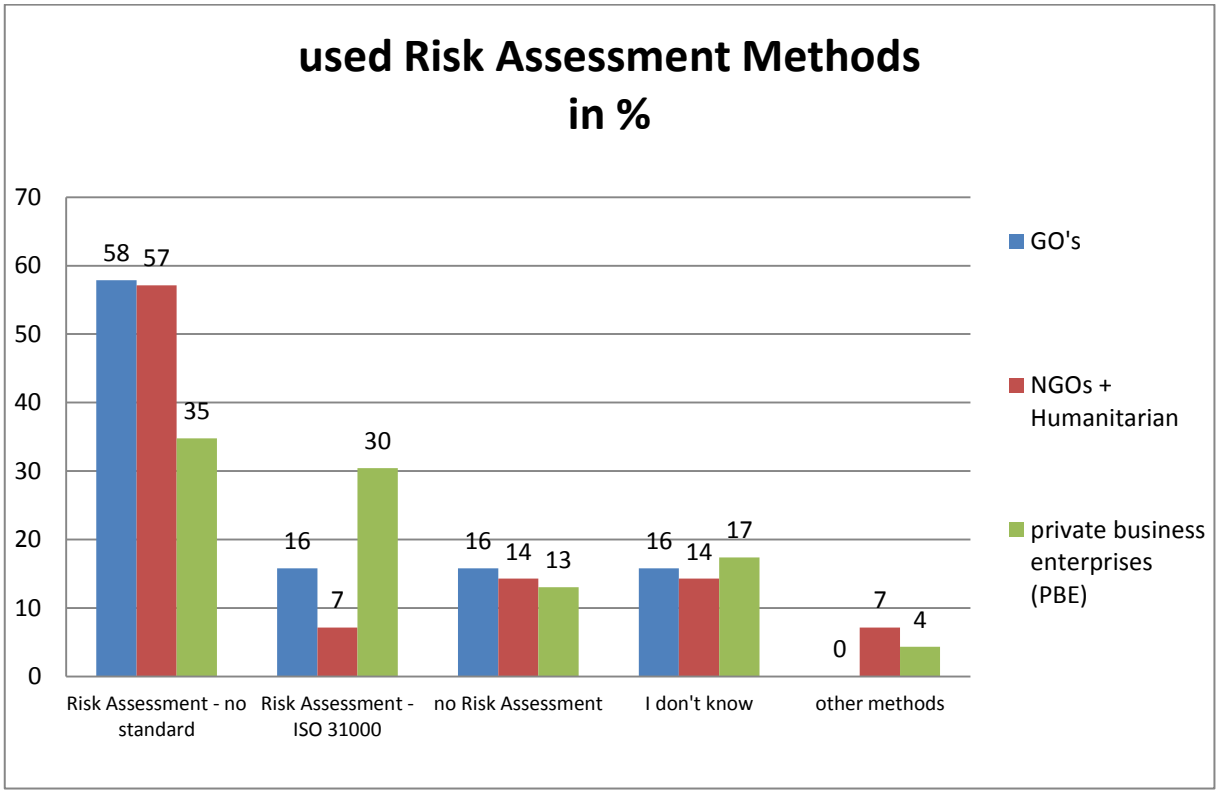

Figure 44

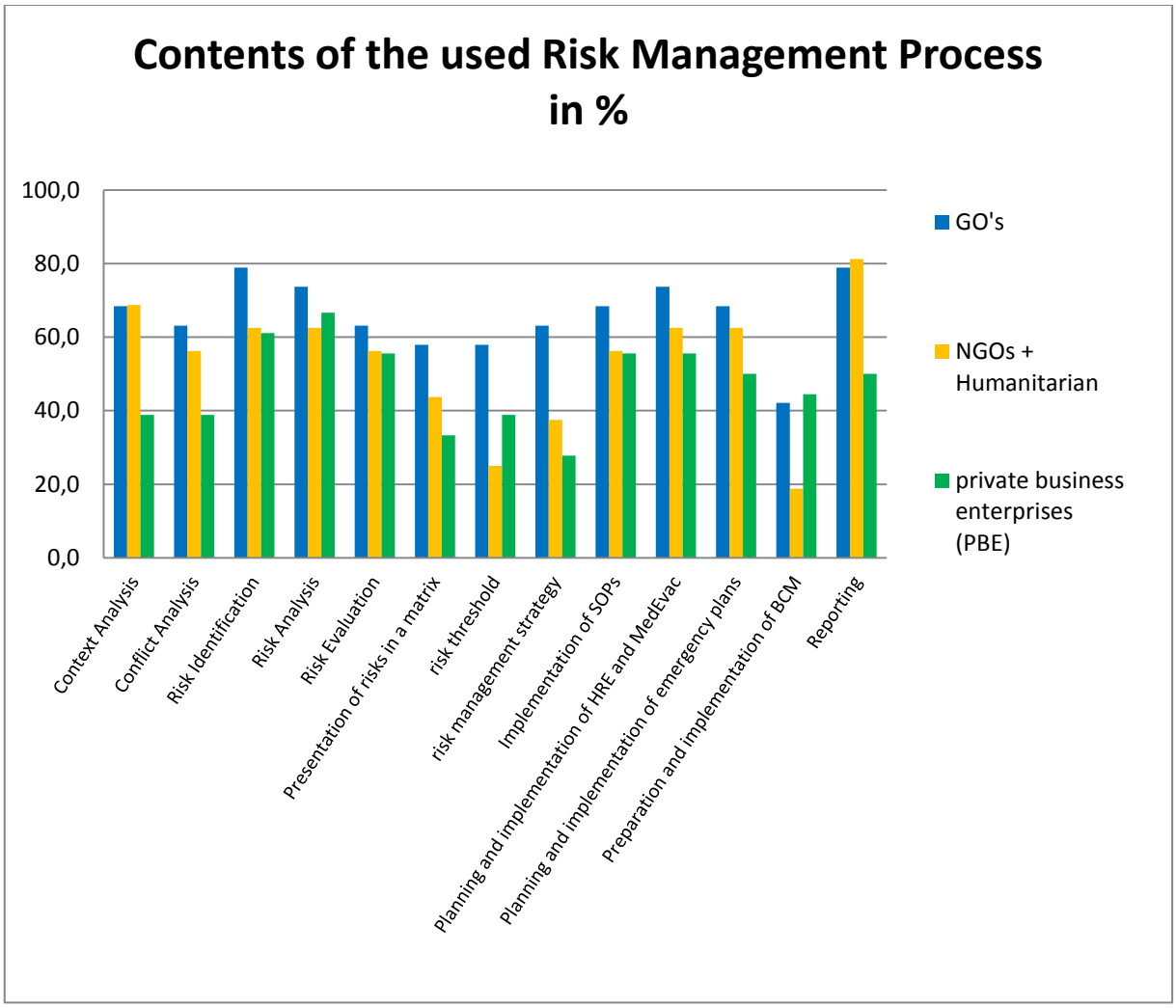
Contents of the used Risk Management Process in %
100,0
80,0
60,0
40,0
20,0
0,0
GO's
NGOs + Humanitarian
private business enterprises (PBE)
Context Analysis
Conflict Analysis
Risk Identification
Risk Analysis
Risk Evaluation
Presentation of risks in a matrix
risk threshold
risk management strategy
Implementation of SOPs
Planning and implementation of HRE and MedEvac
Planning and implementation of emergency plans
Preparation and implementation of BCM
Reporting

Figure 45

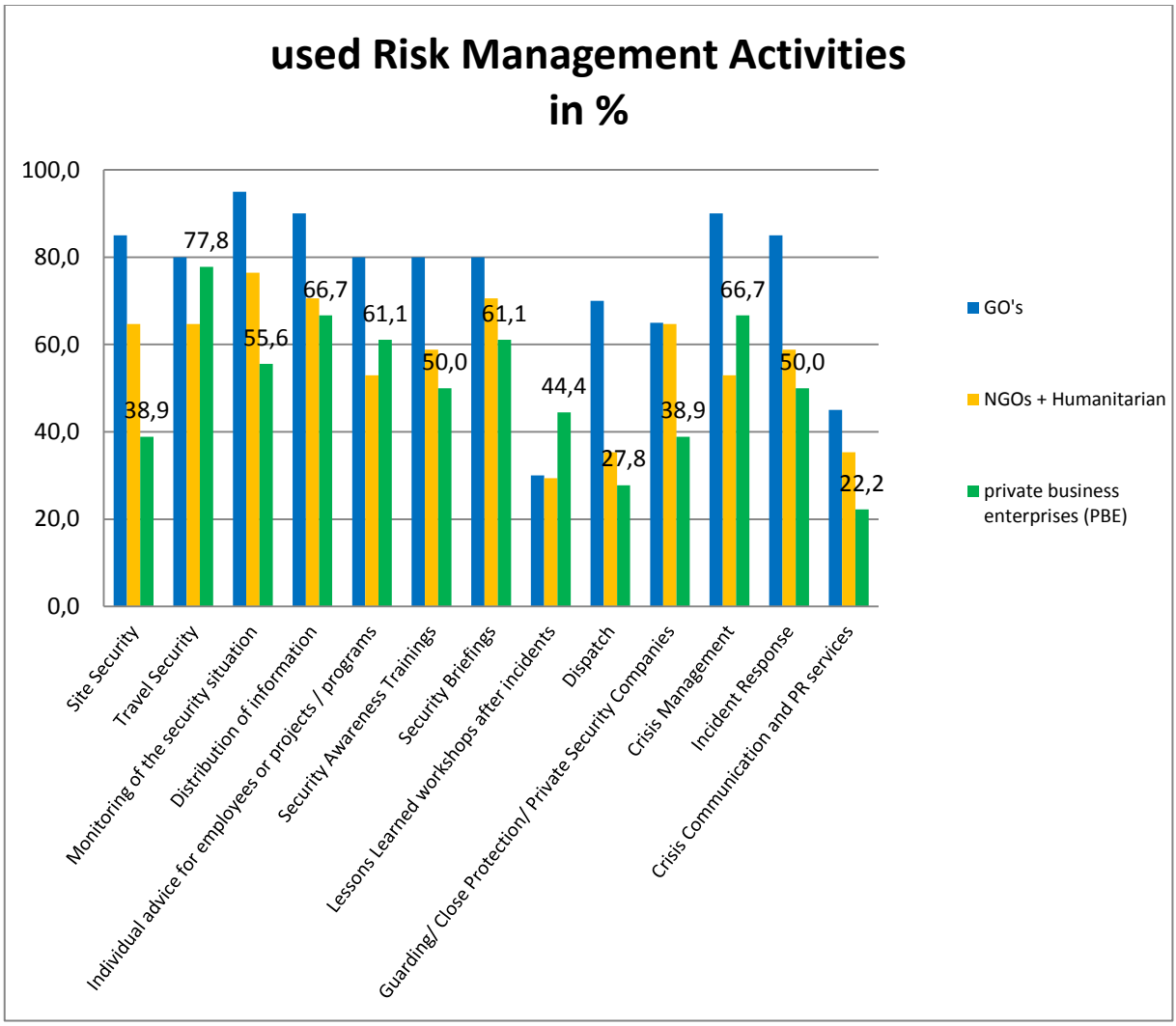
used Risk Management Activities in %
100,0
80,0
60,0
40,0
20,0
0,0
38,9
77,8
55,6
66,7
61,1
50,0
61,1
44,4
27,8
38,9
66,7
50,0
22,2
Site Security
Travel Security
Monitoring of the security situation
Distribution of information
Individual advice for employees or projects / programs
Security Awareness Trainings
Security Briefings
Lessons Learned workshops after incidents
Dispatch
Guarding/ Close Protection/ Private Security Companies
Crisis Management
Incident Response
Crisis Communication and PR services
GO's
NGOs + Humanitarian
private business enterprises (PBE)

Figure 46

Statistic Assessment – Type of Organization

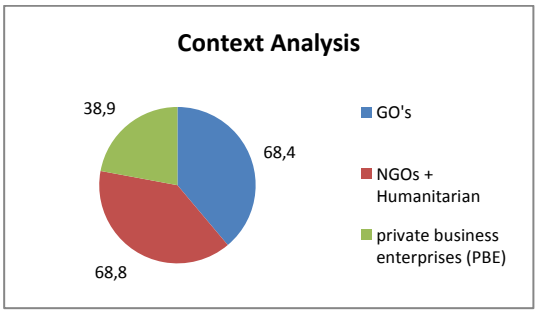

Figure 47

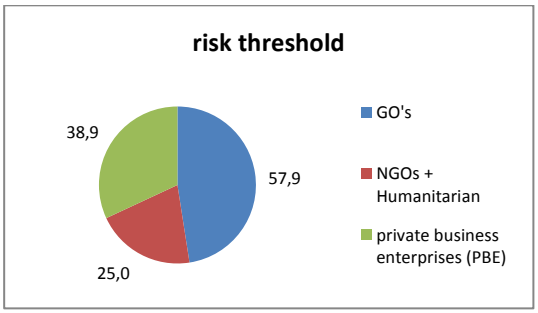

Figure 48

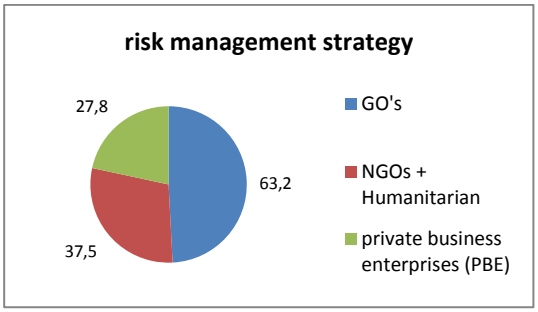

Figure 49

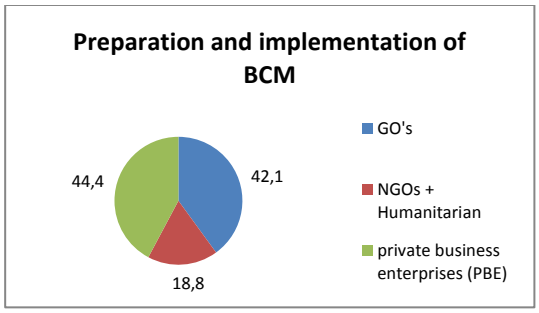

Figure 50

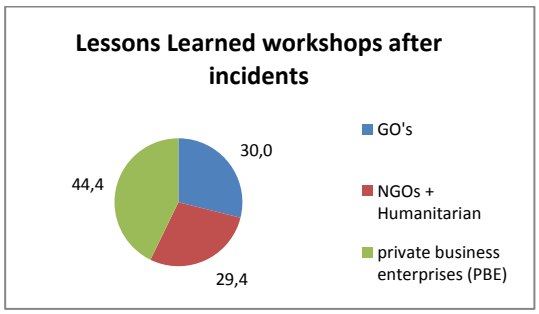

Figure 51

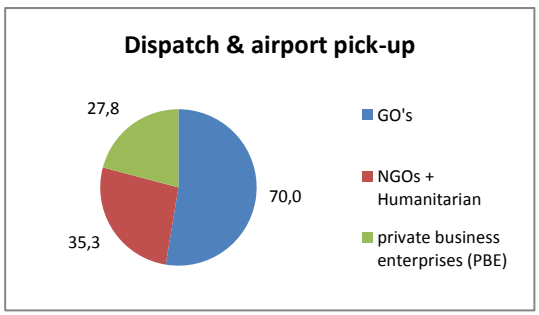

Figure 52

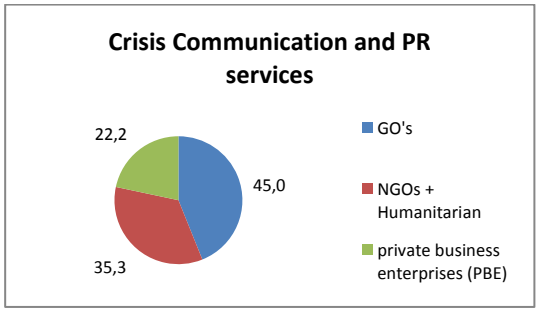

Figure 53

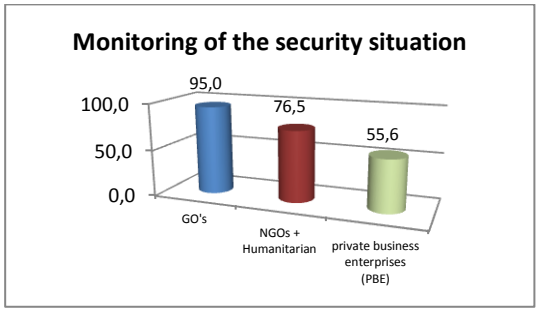

Figure 54

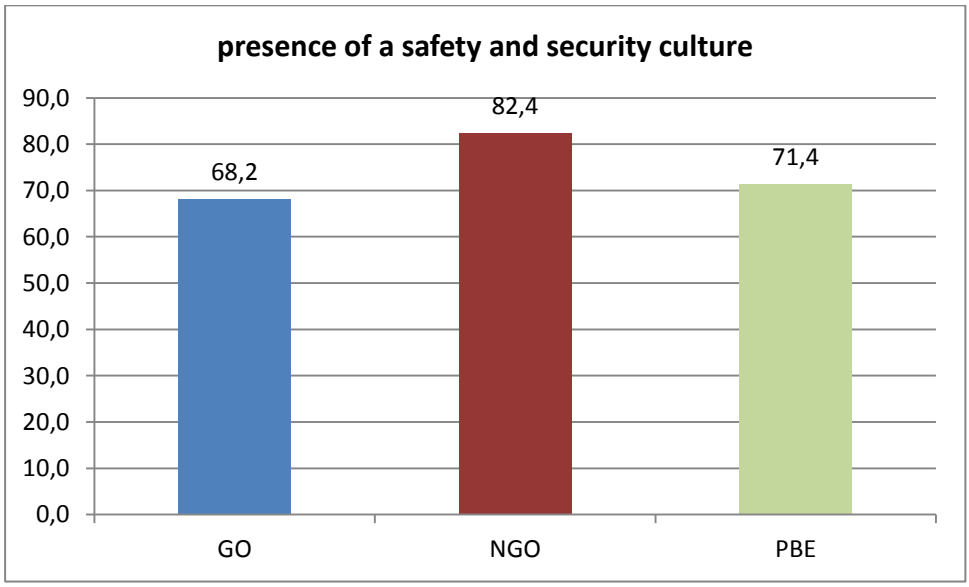

Figure 55

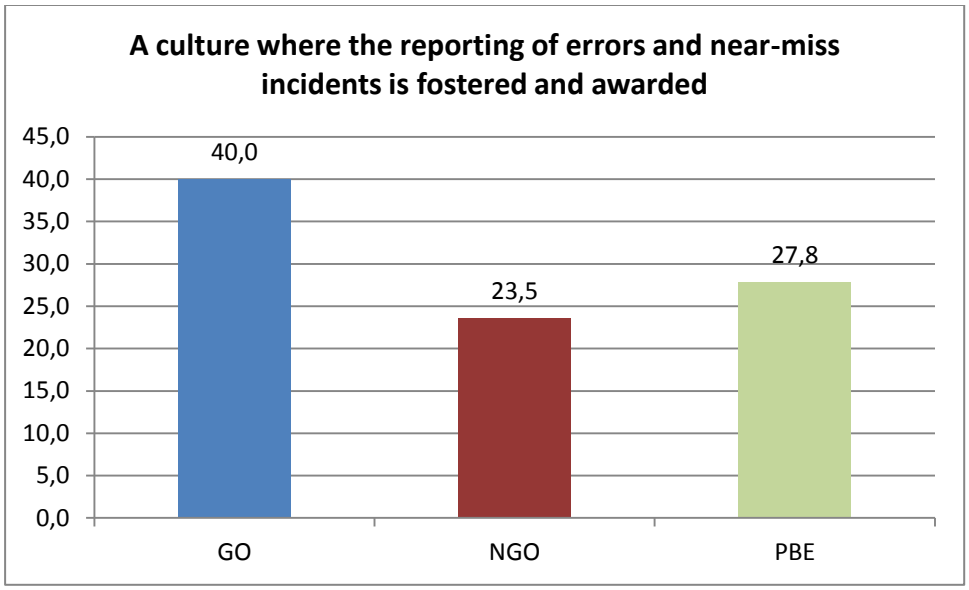

Figure 56

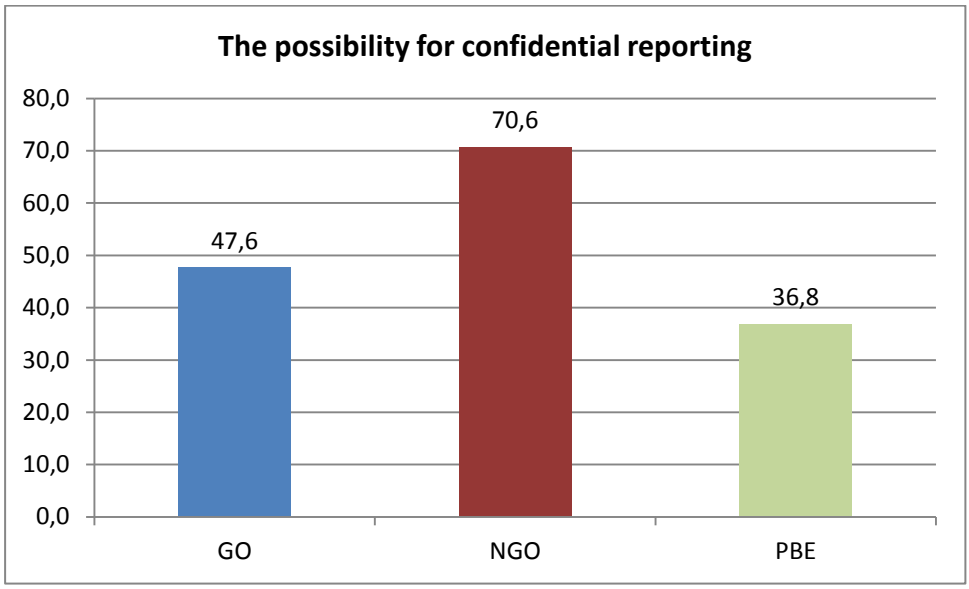

Figure 57

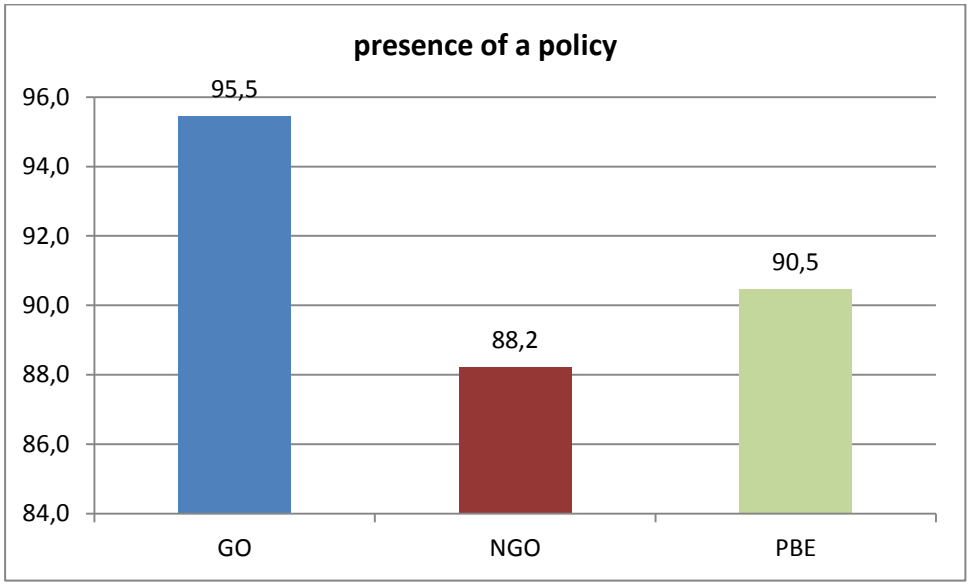

Figure 58

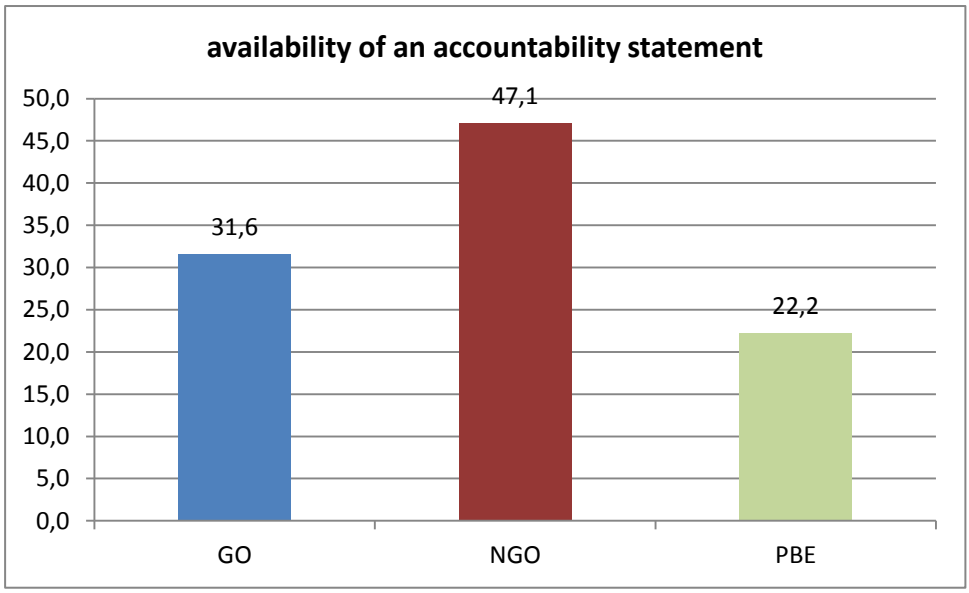

Figure 59

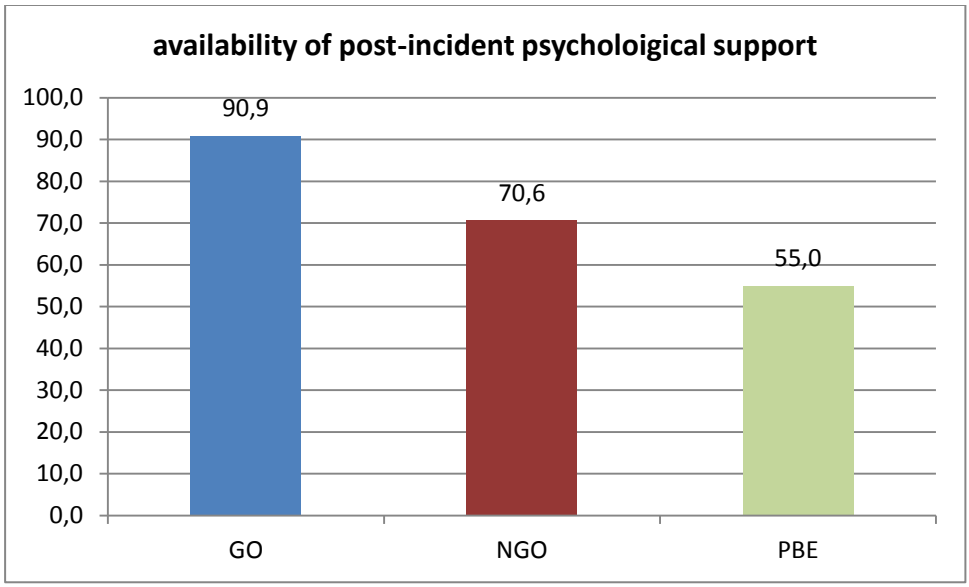

Figure 60

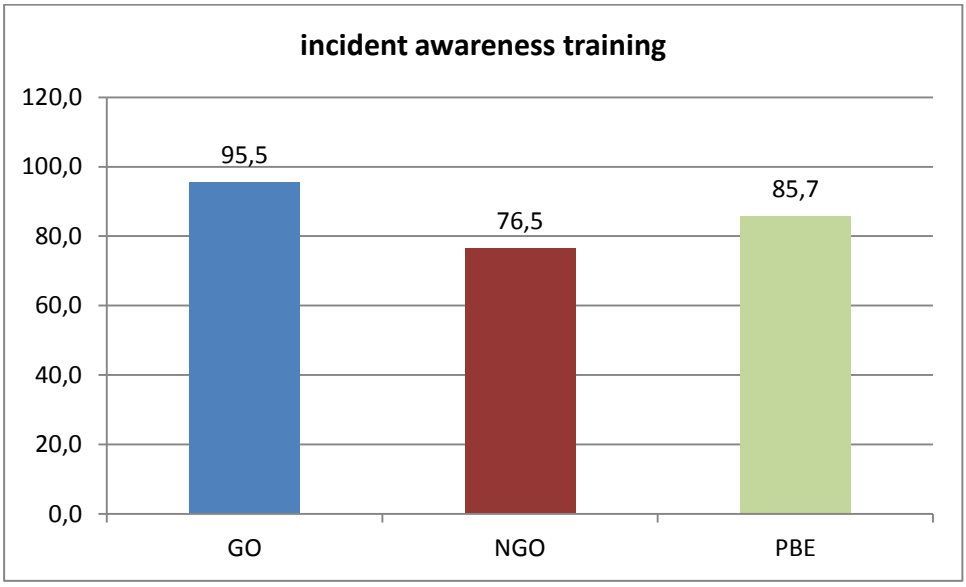

Figure 61

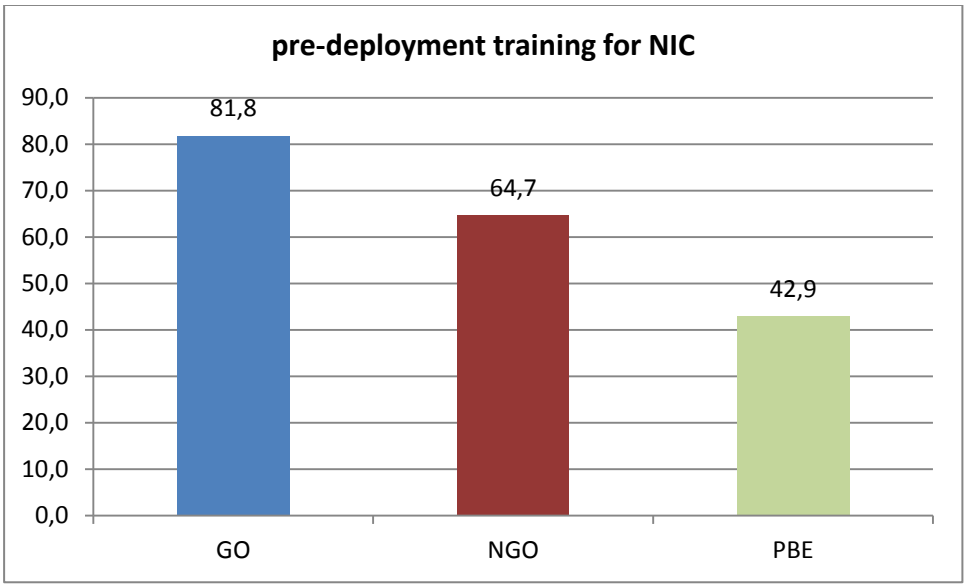

Figure 62

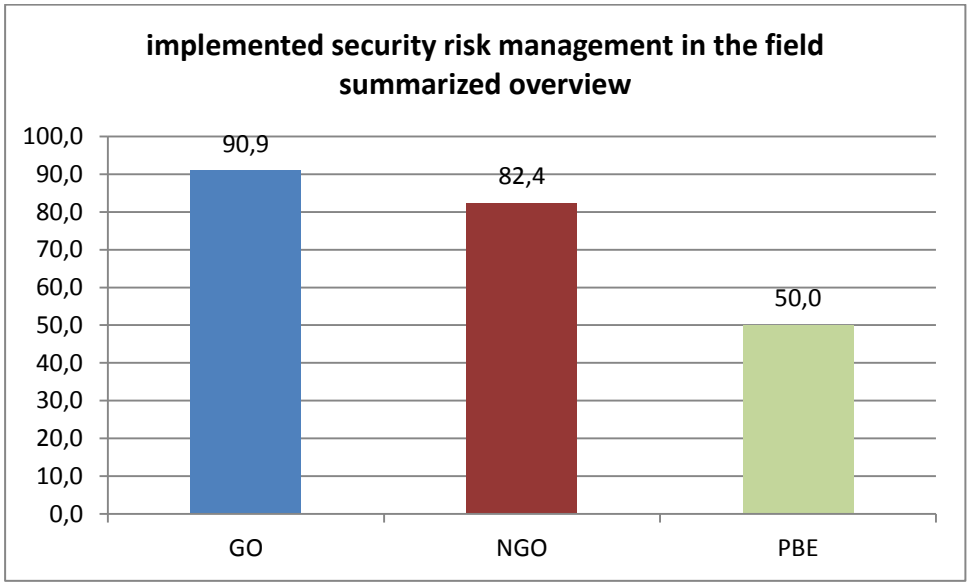

Figure 63

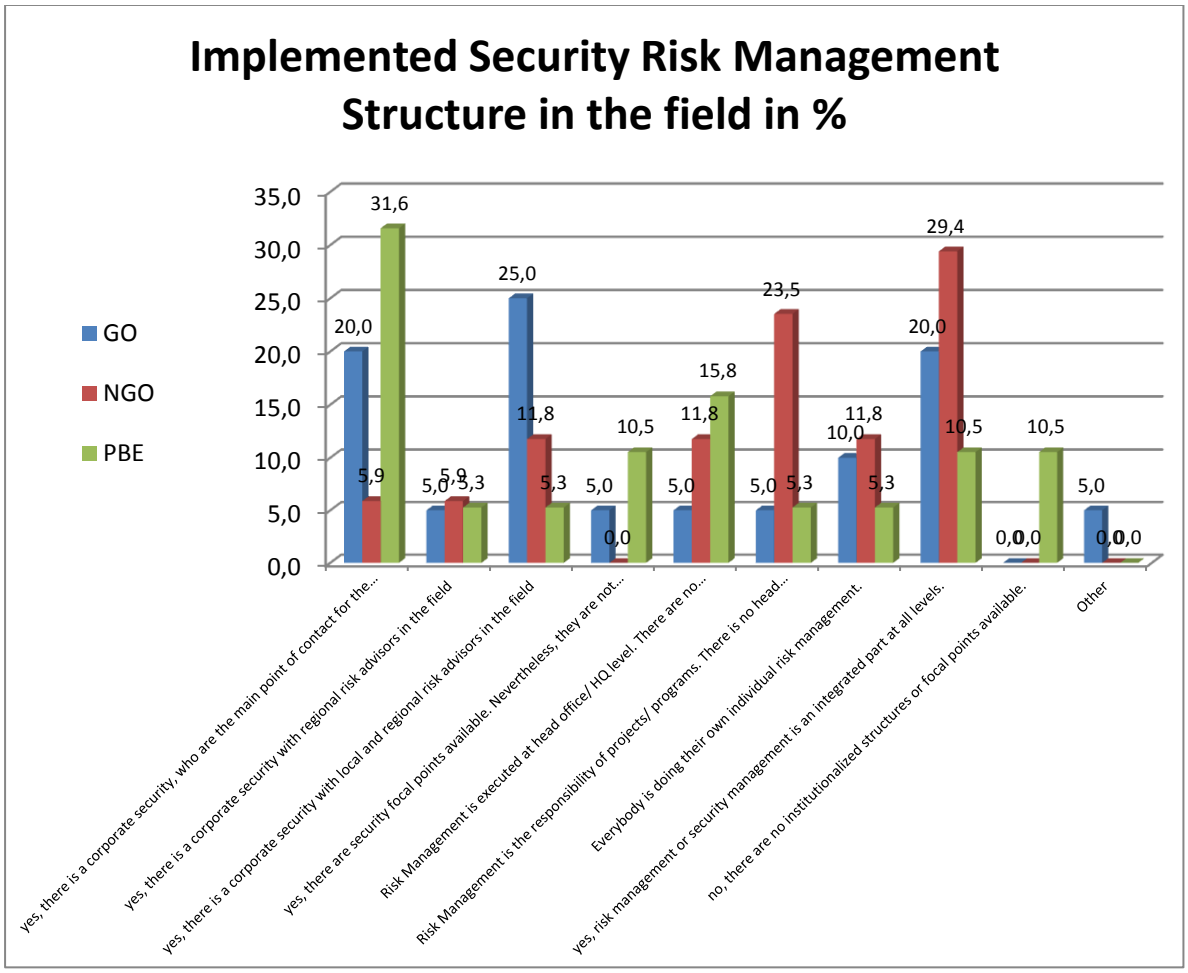

Figure 63.1

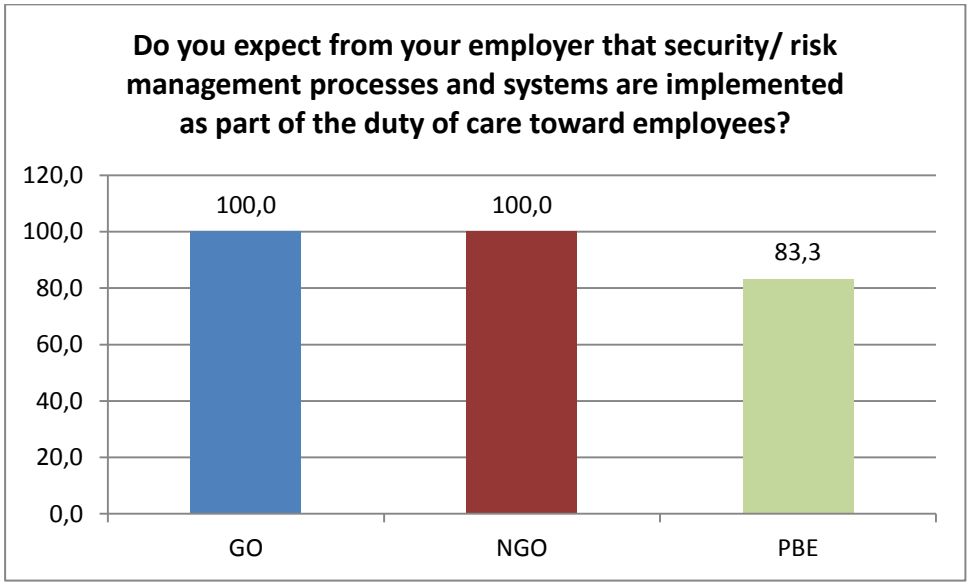

Figure 64

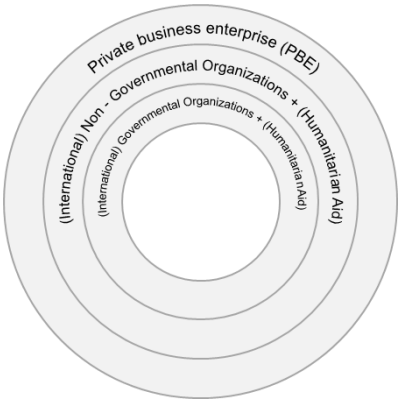

Figure 65

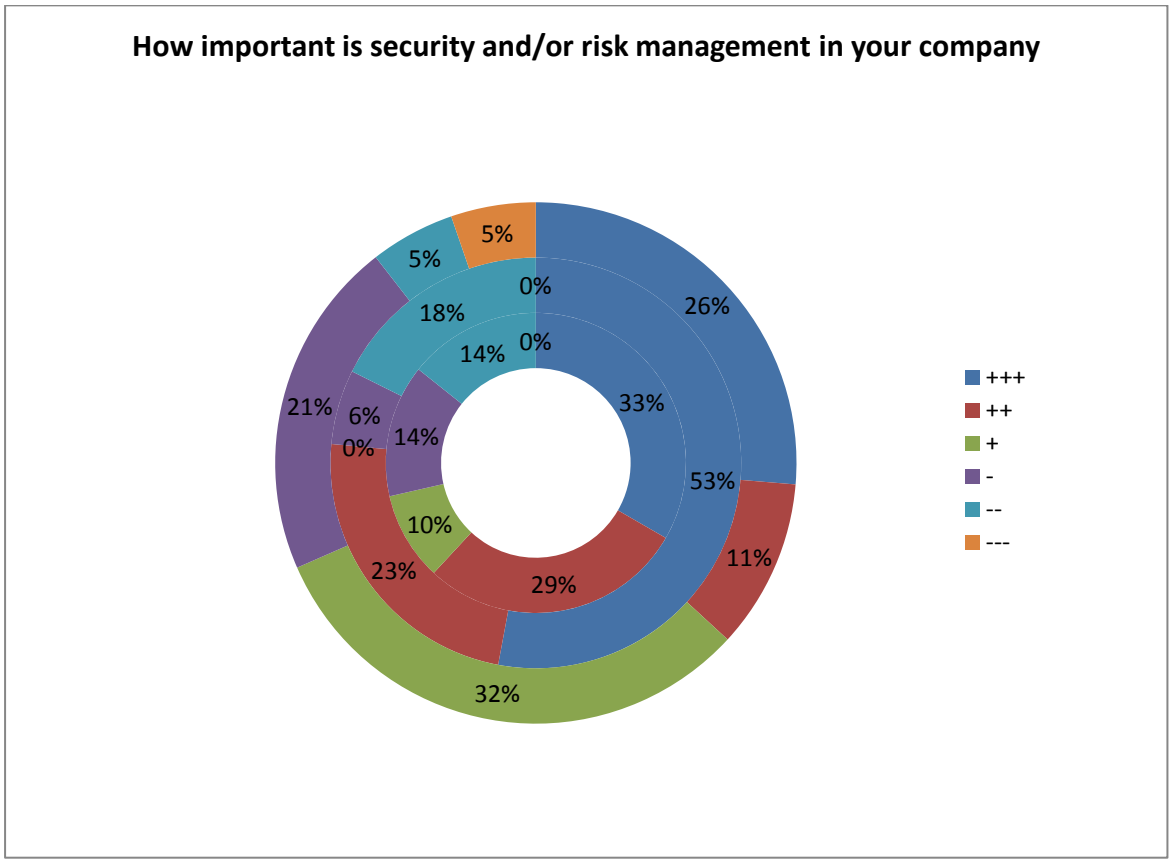

Figure 66

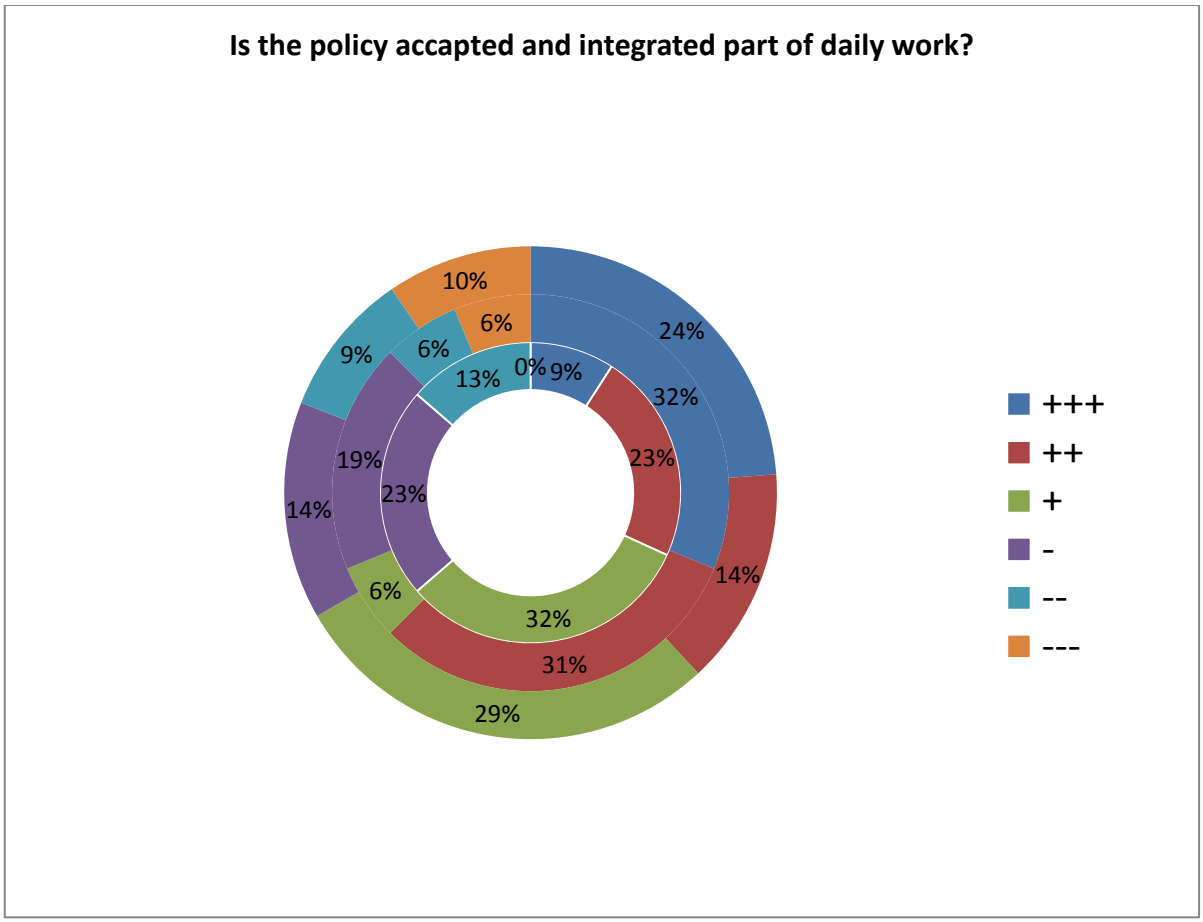
Is the policy accapted and integrated part of daily work?
10%
6%
24%
9%
6%
0%
9%
13%
32%
23%
19%
23%
14%
14%
6%
32%
31%
29%
+++
++
+
-
--

Figure 67

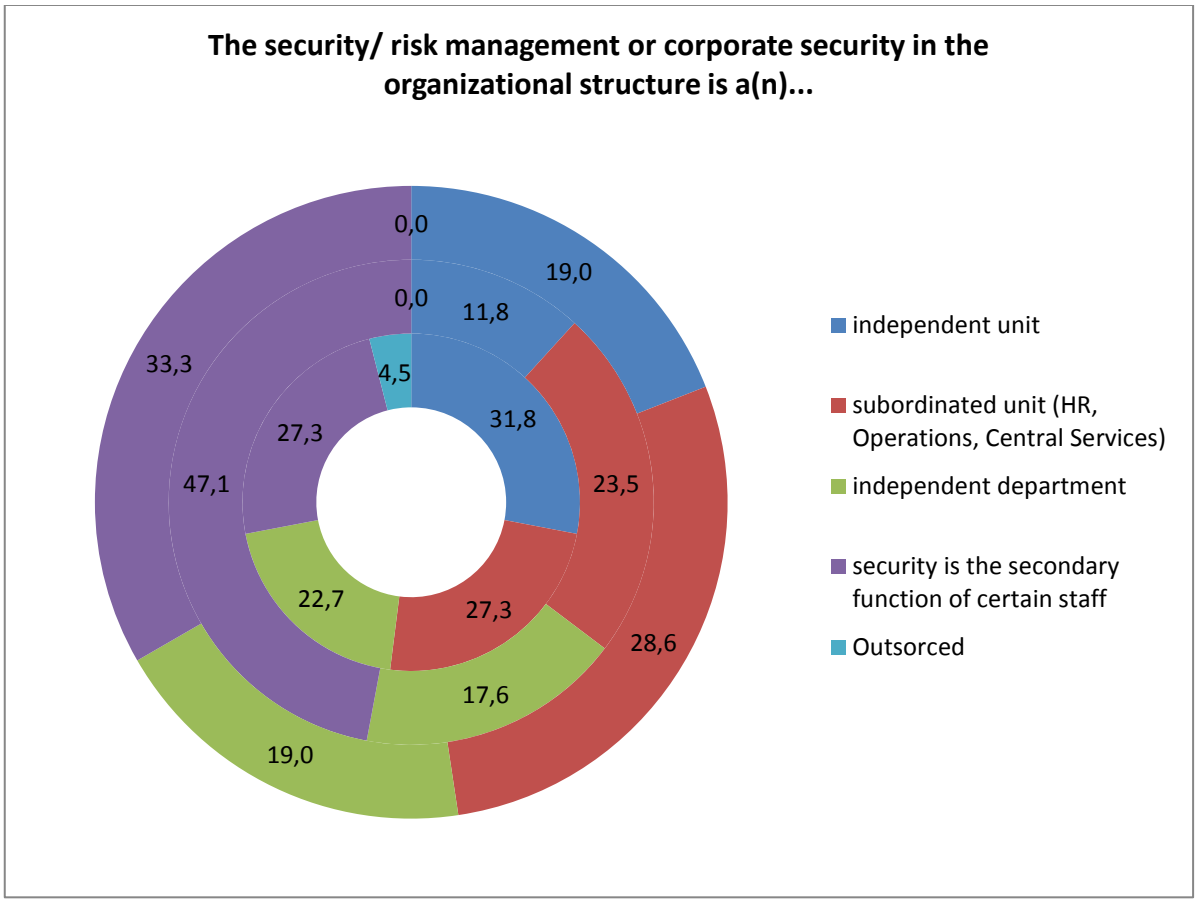

Figure 68

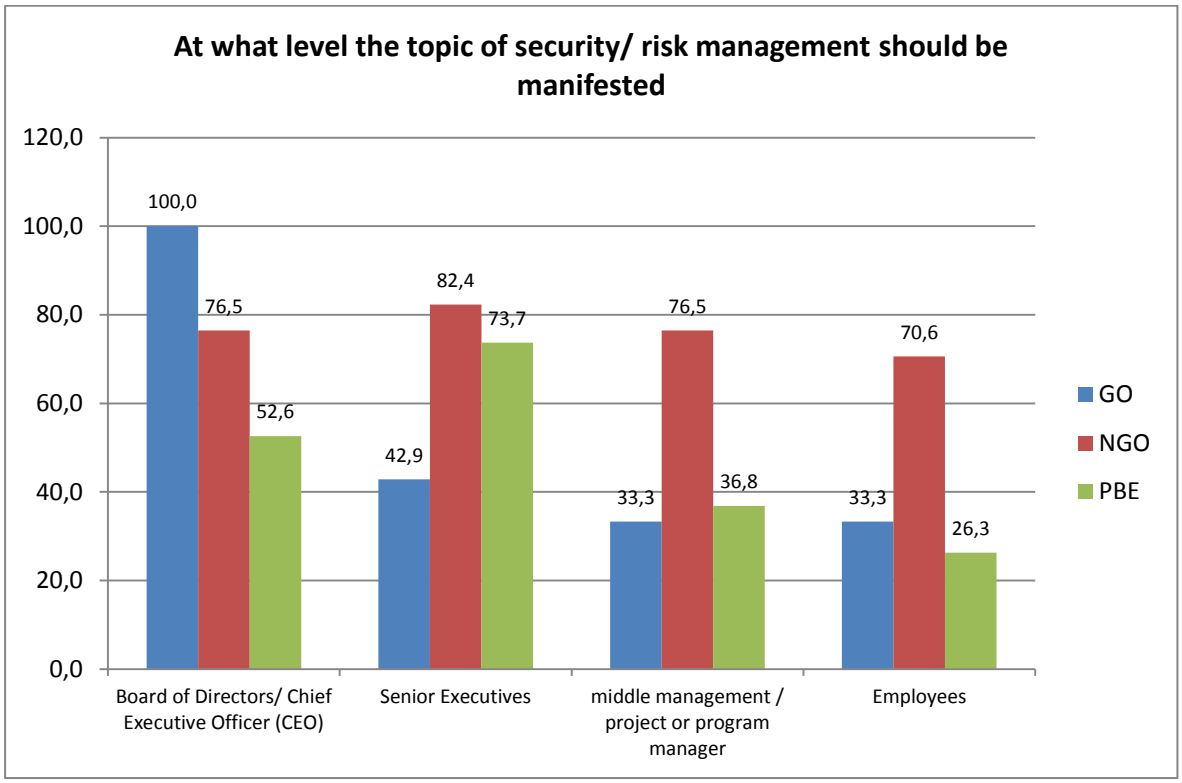

Figure 69

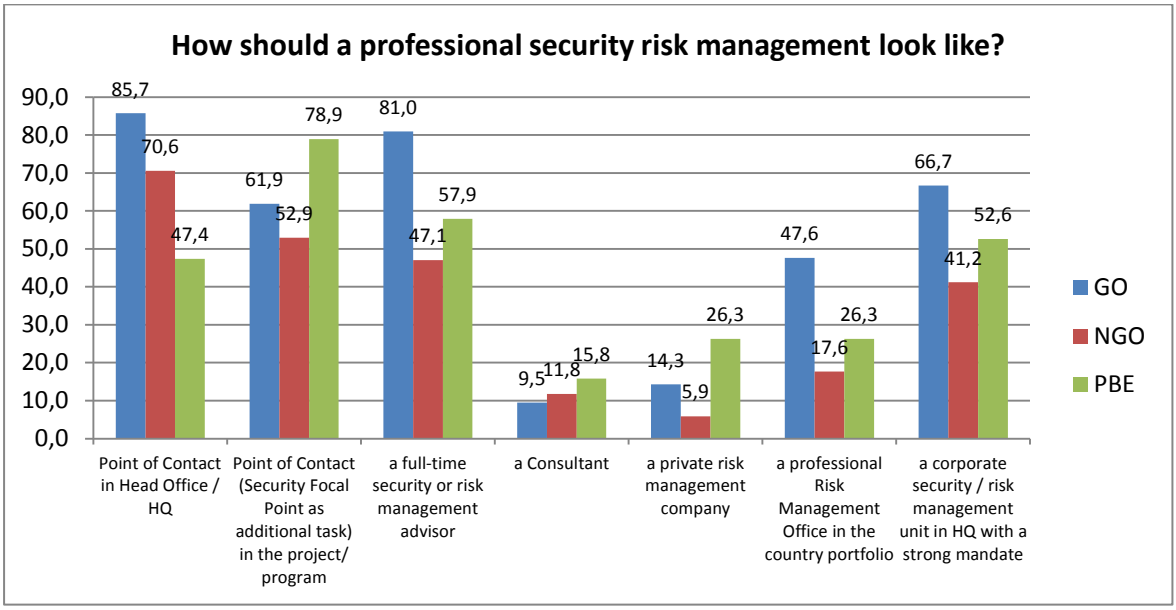

Figure 70

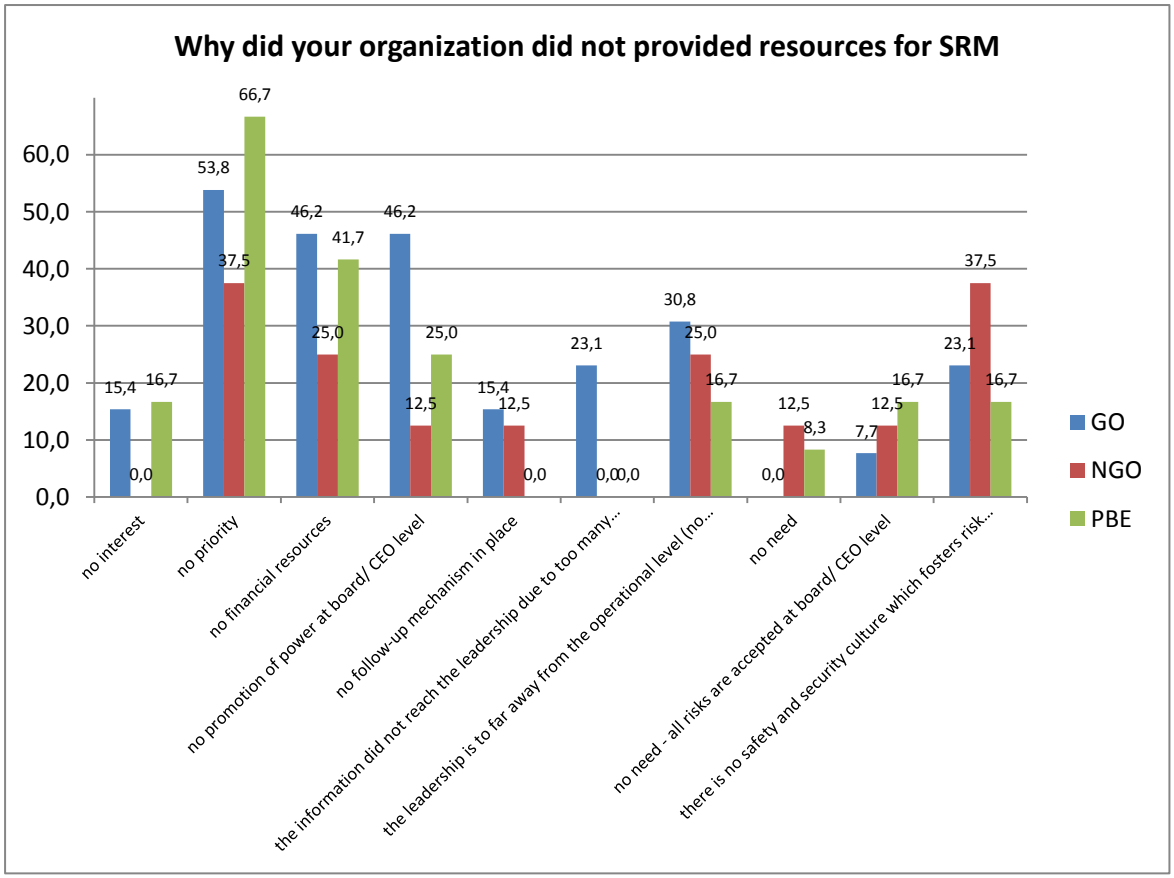

Figure 71

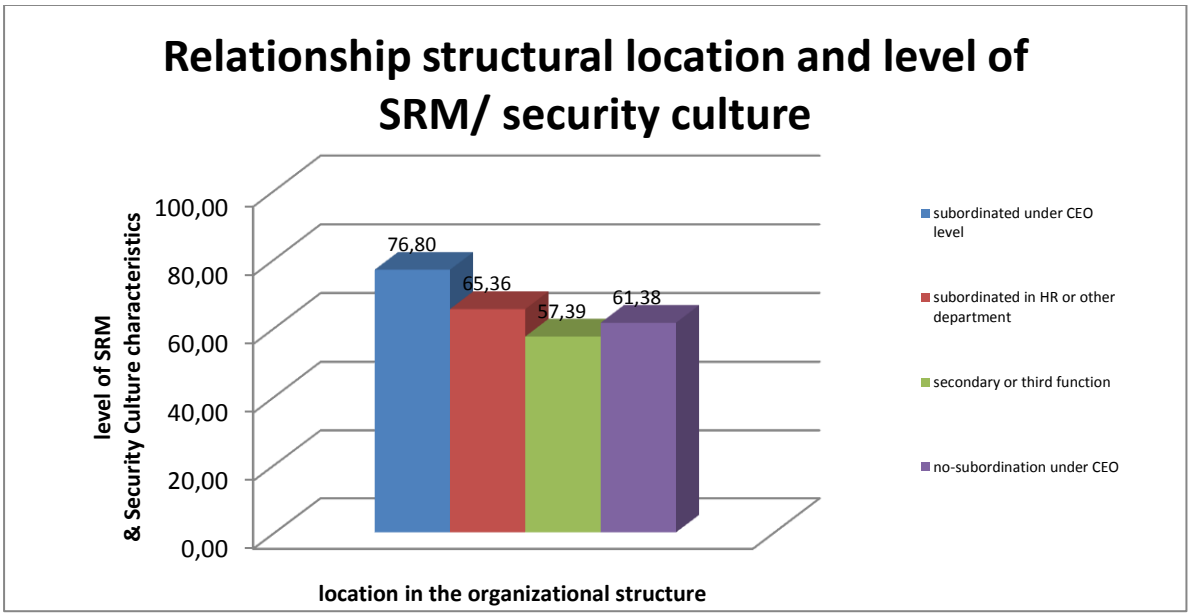
Relationship structural location and level of SRM/ security culture
level of SRM & Security Culture characteristics
100,00
80,00
60,00
40,00
20,00
0,00
76,80
65,36
57,39
61,38
location in the organizational structure
subordinated under CEO level
subordinated in HR or other department
secondary or third function
no-subordination under CEO

Figure 72

Bibliography

Ale, B. J.M. (2009) Risk: An introduction: the concepts of risk, danger and chance, New York: Routledge.

Anderson, M. (1999) Do No Harm: How Aid can Support Peace – or War. Lynne Rienner, Boulder, CO.

Anderson, M.B. (1999) Do No Harm. How aid can support peace- or war, Boulder: Lynne Rienner Publisher Ltd.

Arbeitsschutzgesetz (ArbSchG) (1996) Gesetz über die Durchführung von Maßnahmen des Arbeitsschutzes zur Verbesserung der Sicherheit und des Gesundheitsschutzes der Beschäftigten bei der Arbeit; available online at: http://www.gesetze-im-internet.de/bundesrecht/arbschg/gesamt.pdf; accessed 11 September, 2012.

Aristotle (384-322 BC), in Barnes, J. (1991) *The complete Works of Aristotle*, Princeton: Princeton University Press; available online at: http://recursosdefilosofia.com/[Jonathan_Barnes_(editor)]_The_Complete_Works_of_A(BookFi.org).pdf; accessed 13 June, 2013: 863-864.

Ashkanasy, N. M., Broadfoot, L. E., and Falkus, S. (2000) 'Questionnaire measures of organizational culture', in Ashkanasy, N. M., Wilderom, C. P. M. & M. F. Peterson (Eds.) Handbook of organizational culture and climate, Thousand Oaks, CA: Sage Publications: 131–147.

Asian Development Bank Administrative Tribunal (1995) 'Decision No. 5', Bares v. Asian Development Bank, May 31; available online at: http://www.adb.org/sites/default/files/pub/1995/ADBT0005.pdf; assessed 14 June, 2013.

Ast, S. A. (2010) Managing Security Overseas. Protecting employees and assets in volatile regions, Boca Raton: Auerbach Publications.

Barnett, M. (2009) 'Evolution without progress? Humanitarianism in a world of hurt. International Organization' in Schneiker, A. (2011) Sicherheitskonzepte deutscher Hilfsorganisationen. Zwischen Identitätswahrung und Pragmatismus, Zeitschrift für Außen- und Sicherheitspolitik, November 2011, 4 (4), Hannover; available online at: http://link.springer.com/article/10.1007%2Fs12399-011-0220-9#; accessed 17 March, 2013: 627-644.

Barnett, M., & Weiss, T. G. (2008) 'Humanitarianism. A brief history of the present' in Barnett, M. and Weiss, T. G. Humanitarianism in question. Politics, power, ethics, Ithaca: Cornell University Press: 1-48.

Baruch, Y. (1999) 'Response rate in academic studies – a comprehensive analysis', *Human Relations*, in Hinkin, T.R. and Holtom, B.C. (2009) 'Respose rates and sample representativeness: identifying contextual response drivers' in Buchanan, D.A. and Bryman, A (2009) *Organizational Research Methods*, London: Sage Publications.

Bellamy, C. (2004) Joint Meeting of Executive Boards: UNDP, UNFPA, WFP, and UNICEF on United Nations Staff Safety and Security, January 21; available online at: http://www.unicef.org/about/execboard/files/finalsecuritybriefingregular.pdf; accessed 13 February, 2013.

Bellot, J. (2011) 'Defining and Assessing Organizational Culture', Nursing Forum, January- March 2011, 46 (1); available online at: http://onlinelibrary.wiley.com.ezproxy4.lib.le.ac.uk/doi/10.1111/j.1744-6198.2010.00207.x/pdf; accessed 26 May, 2013: 29-37.

Berwick, D. M. and Leape, L. L. (1999) ´Reducing errors in medicine: It's time to take this more seriously´, British Medical Journal, 319: 136-137.

Beyea, S. C. (2004) ´Creating a just safety culture´, *AORN Journal*, 79.2, February 2004: 412; available online at: http://go.galegroup.com.ezproxy4.lib.le.ac.uk/ps/retrieve.do?sgHitCountType=None&sort=DA-SORT&inPS=true&prodId=EAIM&userGroupName=leicester&tabID=T002&searchId=R1&resultListType=RESULT_LIST&contentSegment=&searchType=AdvancedSearchForm&currentPosition=1&contentSet=GALE%7CA113802523&&docId=GALE|A113802523&docType=GALE&role; accessed 3 March, 2013.

BGB (2013a) §617 Pflicht der Krankenfürsorge; available online at: http://www.gesetze-im-internet.de/bundesrecht/bgb/gesamt.pdf; accessed 13 June, 2013.

BGB (2013a2013b) §618 Pflicht zu Schutzmaßnahmen; available online at: http://www.gesetze-im-internet.de/bundesrecht/bgb/gesamt.pdf; accessed 13 June, 2013.

BGB (2013b2013c) §619 Unabdingbarkeit der Fürsorgepflichten; available online at: http://www.gesetze-im-internet.de/bundesrecht/bgb/gesamt.pdf; accessed 13 June, 2013.

Blyth, M. (2008) Risk and Security Management: Protecting People and Sites Worldwide; available online: http://site.ebrary.com/lib/leicester/docDetail.action?docID=10250290; accessed 15 June, 2013.

BMZ (2013) Entwicklung für Frieden und Sicherheit. Entwicklungspolitisches Engagement im Kontext von Konflikt, Fragilität und Gewalt; available online: http://www.bmz.de/de/publikationen/reihen/strategiepapiere/Strategiepapier328_04_2013.pdf; accessed 03 May, 2013.

Bohne, P. and Peruzzi, W. (2010) ´A Just Culture Supports Patient Safety´, Trustee, April 2010, 63 (3), Ipswich; available online at: http://web.ebscohost.com.ezproxy4.lib.le.ac.uk/ehost/pdfviewer/pdfviewer?sid=f9309e7b-571d-4929-9e3f-b72d68b9f504%40sessionmgr104&vid=2&hid=113; accessed 29 March, 2013: 32.

Bollettino, V. (2008) 'Understanding the security management practices of humanitarian organizations', Disasters, 32 (2): 263-279.

Borodzicz, E. P. (2005) Risk, Crisis & Security Management, West Sussex: England.

Bowers, J., Fodder, M. and Lewis, J. (2007) Whistleblowing: law and practice, New York: Oxford University Press: xxx – xxxii.

Britton, B. (1997) *The learning NGO*. INTRAC occasional papers series, July 1998, 17, Oyford; available online at: http://www.intrac.org/data/files/resources/381/OPS-17-The-Learning-NGO.pdf; accessed 18 February, 2013.

Buchanan, D.A. and Bryman, A (2009) *Organizational Research Methods*, London: Sage Publications.

Bundesministerium der Justiz (BMJ) (2012) *Grundgesetz der Bundesrepublik Deutschland*, Berlin: Bundesrepublik Deutschland: Art. 2 (2).

Claessens, S. (1993) Risk Management in Developing Countries, Washington DC: World Bank Publications.

Claus, L. (2009) 'Duty of Care of Employers for Protecting International Assignees, their Dependents, and International Business Travelers', International SOS White Paper Series; available online at: http://www.internationalsos.com/en/files/Duty_of_Care_whitepaper.pdf; accessed 18 April, 2013: 4.

Cohen, M. R. (2000) ´Why error reporting systems should be voluntary´, British Medical Journal, 18 March 2000, 320 (7237), Austin: 728-729.

Coombs, W. T. and Holladay, S. J (2010) (eds.) The Handbook of Crisis Communication, Blackwell: Oxford.

Cooper, M.D. (2000) 'Towards a model of safety culture', Safety Science, November 2000, 36 (2); available online at: http://www.sciencedirect.com.ezproxy4.lib.le.ac.uk/science/article/pii/S0925753500000357; accessed 12 May, 2013:111-136.

Corporate Manslaughter and Corporate Homicide Act, 2007, (Chapter 19), London: The Stationary Office.

Creswell, J.W. and Plan Clark, V.L. (2007) 'Designing and conducting mixed methods research', in Bryman, A (2009) *Mixed methods in organizational research,* Organizational Research Methods, London: Sage Publications: 516-531.

de Guttry, A. (2012) 'Duty of Care of the EU and its member states towards their personnel deployed in international missions', Studi sull'integrazione Europea, 7; available online at: http://web1.sssup.it/pubblicazioni/ugov_files/374571_De_Guttry_duty%20of%20care%20_2-3_2012.pdf; assessed 14 June, 2013: 263–94.

Deitelhoff, N. and Wolf, K.D. (2010) Corporate Security Responsibility? Corporate Governance Contributions to Peace and Security in Zones of Conflict, Hampshire: Palgrave Macmillan.

Dekker, S. (2008) ´Just Culture: Who gets to draw the line?´, Journal Cognition, Technology and Work, September 2009, 11 (3), London; available online at: http://sunnyday.mit.edu/16.863/JustCultureCTW-1.pdf: accessed 17 March, 2013: 177-185.

Dekker, S. (2012) Just Culture Balancing Safety and Accountability, Hampshire: Ashgate Publishing Limited.

Detert, J.R.; Roger, G., Schröder, R.G., Mauriel, J.J. (2000) 'A Framework for Linking Culture and Improvement Initiatives in Organizations', The Academy of Management Review, 4 October 2000, 25 (4); available online: http://www.jstor.org.ezproxy4.lib.le.ac.uk/stable/259210; accessed 29 July, 2013: 850-863.

Diedenhofen, T. (2008) Fürsorgepflicht des Arbeitgebers bei Dienstreisen – ein häufig vernachlässigtes Thema – mit Folgen!, 27.06.2007, TüV Süd AG - PartnerTag 2008, International SOS; available online at: http://www.tuev-sued.de/uploads/images/1215157801181800150817/6_diedenhofen.pdf; accessed 3 July, 2013.

Dijkzeul, D. (2004). Mapping international humanitarian organisations. Humanitäres Völkerrecht, Informationsschriften, 4: 216–225.

Dijkzeul, D. and Moke, M. (2004) Humanitäre Hilfe – Fluch oder Segen?; available online at: http://www.ageh.de/informationen/con_05/con_1_05/Moke-Dijkzeul-mue-II.pdf; accessed

Donahue A.K. and Tuohy R.V. (2006) 'Lessons we do not learn: A study of the lessons learned of disasters, why we repeat them, and how we can learn them.', Homeland Security Affairs, II(2); available online at :http://www.hsaj.org/?fullarticle=2.2.4; accessed 12 September, 2012: 1-26.

Douglas M. (1992) ´Risk and blame: essays in cultural theory´, in Dekker, S. (2008) ´Just Culture: Who gets to draw the line?', Journal Cognition, Technology and Work, September 2009, 11 (3), London; available online at: http://sunnyday.mit.edu/16.863/JustCultureCTW-1.pdf; accessed 17 March, 2013: 177-185.

Douglas, M. (1994) Risk and blame: essays in cultural theory, London: Routledge.

Edwards, M. (1997). 'Organizational learning in non-governmental organizations: What have we learned?' in Schneiker, A. (2011) ‚Sicherheitskonzepte deutscher Hilfsorganisationen. Zwischen Identitätswahrung und Pragmatismus', Zeitschrift für Außen- und Sicherheitspolitik, November 2011, 4 (4), Hannover; available online at: http://link.springer.com/article/10.1007%2Fs12399-011-0220-9#; accessed 17 March, 2013: 627-644.

European Union (2000) Charter of fundamental rights of the European Union; available online: http://www.europarl.europa.eu/charter/pdf/text_en.pdf; accessed 14 June 2013: 15.

Fielding, N. (1993) ‚Qualitative Interviewing and Ethnography' in Institute of Lifelong Learning (2008) MSc in Risk, Crisis and Disaster Management, Module 3.

Gain (2004) Roadmap to a just culture: Enhancing the safety environment, Global Aviation Information; available online at: http://flightsafety.org/files/just_culture.pdf: accessed 2 April, 2013.

Gheorge, A.V., Masera, M., De Vries, L., Weijnen, M. and Kroger, W. (2006) 'Critical infrastructures: the need for international risk governance', International Journal of Critical Infrastructures 3 (1): 3-19.

Gilpin, D.R. and Murphy, P. (2010) 'Complexity and Crises: A New Paradigm', in Coombs, W.T. and Holladay S.J. (2010) (eds.) The Handbook of Crisis Communication, Blackwell: Oxford: 683-690.

GIZ (2012) Policy for safety and security of staff abroad; Eschborn: 2012.

Graeber, R.C. (2008) Fatigue Risk Management Systems within SMS, 17 June 2008, Vienna; available online at: http://www.faa.gov/about/office_org/headquarters_offices/avs/offices/afs/afs200/media/aviation_fatigue_symposium/GraeberAppComplete.pdf; accessed 13 March 2013.

GTZ (undated) Factsheet zum methodischen Rahmen 'Peace and Conflict Assessment (PCA)', Eschborn: GTZ; available online at: http://www2.gtz.de/dokumente/bib-2011/giz2011-0246de-peace-conflict-assessment.pdf; accessed 3 February, 2010.

Guldenmund, F.W. (2000) 'The nature of safety culture: a review of theory and research', Safety Science, 34 (1-3): 215-257.

Hader, R. (2006) ´A *just culture* proves just right´, Nursing Management, June 2006, 37 (6); available online at: http://www.ncbi.nlm.nih.gov/pubmed/16788362 and http://web.ebscohost.com.ezproxy4.lib.le.ac.uk/ehost/pdfviewer/pdfviewer?sid=e2bc1c0f-f07e-4924-a69f-911de0d360c6%40sessionmgr113&vid=2&hid=113; accessed 23 March 2013: 6.

Hakim, S. and Blackstone, E. A. (2009) (eds.) 'Safeguarding Homeland Security: Governors and Mayors Speak Out', Journal of Homeland Security & Emergency Management, 7 (1): Springer.

Harper, M. L. and Helmreich, R. L. (2011) ´Creating and maintaining a reporting culture´ in Proceedings of the 12th International Symposium on Aviation Psychology, Dayton, OH: The Ohio State University; available online at: http://www.docstoc.com/docs/79852798/Creating-and-Maintaining-a-Reporting-Culture; accessed 25 March, 2013: 496-501.

Hart, C. (2004) Doing Your Masters Dissertation, London: Sage Publications.

HDI (2013) Email to the author, 23, August.

Helmreich, R. L. (2000) ´Culture and error in space: Implications from analog environments´, Aviation, Space, and Environmental Medicine, 71 (9-11), Austin; available online at: http://homepage.psy.utexas.edu/homepage/group/helmreichlab/publications/pubfiles/Pub249.pdf; accessed 1 April 2013: 133-139.

Hofstede, G. (1994) ´Cultures and Organizations: Intercultural Cooperation and its importance for survival´, in Reason, J. T. (1997) Managing the Risks of Organizational Accidents, Aldershot: Ashgate :194.

Houben, M. (2012) The price of anything. Part 2; available online at: http://www.youtube.com/watch?v=db2ZffeQ2_8; accessed 2 September, 2013.

Humanitarian Outcomes (2013a) Humanitarian Outcomes website; available online at: http://www.humanitarianoutcomes.org/home; accessed 10 November 2013.

Humanitarian Outcomes (2013b) Aid Worker Security Report 2013 Preview Figures at a glace, 19 August 2013; available online at: https://aidworkersecurity.org/sites/default/files/AidWorkerSectyPreview_0819.pdf; accessed 23 August, 2013.

ICRC (2004) 'Humanitarian security: a matter of acceptance, perception, behaviour...', 31 March 2004, Statement; available online: http://www.icrc.org/eng/resources/documents/misc/5xsgwe.htm; accessed 26 July, 2013.

INGO Accountability Charta (2005) International Non-Governmental Organizations Accountability Charta; available online: http://www.ingoaccountabilitycharter.org/wpcms/wp-content/uploads/INGO-Accountability-Charter.pdf; accessed 6 August, 2013.

Institute of Lifelong Learning (2008) MSc in Risk, Crisis and Disaster Management, Module 3.

Institute of Medicine (IoM) (1999) To err is human: shaping the future of health, 2000, Washington, National Academy of Science; available online at: http://www.iom.edu/~/media/Files/Report%20Files/1999/To-Err-is-Human/To%20Err%20is%20Human%201999%20%20report%20brief.pdf; accessed 1 April, 2013.

International Court of Justice (ICJ) (1949) Reparation for injuries suffered in the service of the United Nations; available online: http://www.icj-cij.org/docket/files/4/1835.pdf; accessed: 14 June, 2013: 13.

International Labour Organization (ILO) (2000) 'Forty-third ordinary session', In re Grasshoff, Judgement No. 402, Geneva; available online at: http://www.ilo.org/dyn/triblex/triblexmain.fullText?p_lang=en&p_judgment_no=402&p_language_code=EN; accessed 14 June, 2013: 4.

International Standardization Organization (2009a) ISO 31000 Risk Management – Principles and Guidelines, Genf: ISO Copyright Office.

International Standardization Organization (2009b) ISO/IEC 31010 Risk Management – Risk Assessment Techniques, Genf: ISO Copyright Office.

Irish Aid (2013) *Irish Aid Guidelines for NGO Professional Safety and Security Risk Management*; available online:

http://www.irishaid.ie/media/irishaid/allwebsitemedia/20newsandpublications/irish-aid-guidelines-for-ngo-professional-safety-and-security-risk-management.pdf; accessed 6th August, 2013.

Johnston, N. A. (2005) ´Blame, Punishment and Risk Management´, in Hood, C. and Jones, D. K. C. (eds) Accident and Design: contemporary debates in risk management, Abington: UCL Press: 72-83.

Knapp, K.J., Marshall, T.E., Rainer, R.K. and Ford, F.N. (2006) 'Information security: management's effect on culture and policy', *Information Management & Computer Security*, 14 (1), available online at: http://www.emeraldinsight.com.ezproxy4.lib.le.ac.uk/journals.htm?articleid=1541496&show=abstract#sthash.06QqvJym.dpuf; accessed 24 May, 2013: 24-36.

Koh, H.C., Johnson, S.D. and Killough, L.N. (2009) 'Organizational and Occupational Culture and the Perception of Managerial Accounting Terms: An Exploratory Study Using Perceptual Mapping Techniques', Contemporary Management Research, December 2009, 5 (4); available online at: http://www.google.de/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=2&cad=rja&ved=0CDoQFjAB&url=http%3A%2F%2Fwww.cmr-journal.org%2Farticle%2Fdownload%2F1931%2F3601&ei=WTwjUt6vHI_IswadjoH4AQ&usg=AFQjCNEz-W2g8hx5l7JtGoc9gqUSf5LdJA&sig2=Et3_3UdXMt0KRAsPeTGMgQ&bvm=bv.51495398,d.Yms; accessed 24 March, 2013: 317-342.

Krähenbühl, P. (2004) 'The ICRC's approach to contemporary security challenges: A future for independent and neutral humanitarian action', ICRC, IRRC, September 2004, 86 (855); available online at: http://www.961.ch/eng/assets/files/other/irrc_855_krahenbuhl.pdf; accessed 26 July, 2013.

Krimsky, S. (2007) 'Risk communication in the internet age: The rise of disorganized scepticism', Environmental Hazards, 7: 157-164.

Krimsky, S. and Golding D. (1992) 'Reflections' in Krimsky, S. and Golding, D. (1992) (eds.) Social Theories of Risk, Westport: Praeger.

Kruk, G. (2008) Peace and Conflict Assessment, A methodological framework for the conflict- and peace-oriented alignment of development programmes Eschborn: GTZ; available online at: http://www.forumzfd-akademie.de/files/va_media/nid2214.media_filename.pdf: accessed 25 May, 2011.

Leape L. L. and Berwick D. M. (1999) ´Reducing errors in medicine: It's time to take this more seriously´, British Medical Journal, Vol. 319: 136- 137; in Harper, M. L. and Helmreich, R. L. (2011) ´Creating and maintaining a reporting culture´ In Proceedings of the 12th International Symposium on Aviation Psychology, Dayton, OH: The Ohio State University; available online at: http://www.docstoc.com/docs/79852798/Creating-and-Maintaining-a-Reporting-Culture; accessed 25 March, 2013: 496-501.

Lekka C. (2011) High reliable organizations: A review of literature, HSE Books, Derbyshire: Crown.

Lewin, K., Lippitt, R. and White, R.K. (1939a) 'Patterns of aggressive behaviour in experimentally created 'social climates'', Journal of Social Psychology, 1 May 1939, 10; available online at: http://search.proquest.com.ezproxy4.lib.le.ac.uk/pao/docview/1290670609/1403BD1FE0D6BF36B85/1?accountid=7420; accessed 26 May, 2013: 271-299.

Lewin, K., Lippitt, R. and White, R.K. (1939b) 'Patterns of aggressive behaviour in experimentally created 'social climates'', in Bellot, J. (2011) 'Defining and Assessing Organizational Culture', Nursing Forum, January- March 2011, 46(1), Thomas Jefferson University, PA; available online at: http://onlinelibrary.wiley.com.ezproxy4.lib.le.ac.uk/doi/10.1111/j.1744-6198.2010.00207.x/pdf; accessed 26 May, 2013: 29-37.

Martin, J. and Siel, C. (1983) 'Organizational culture and counterculture: An uneasy symbiosis', Organizational Dynamics, Autumn 1983, 12 (2); available online at: http://www.sciencedirect.com/science/article/pii/0090261683900335; accessed 14 May 2013: 52-64.

Marx D. (2001) Patient safety and the 'just culture': a primer for health care executives, New York: Columbia University.

Merkelbach, M. and Daudin, P. (2011) From Security Management to Risk Management. Critical Reflections on Aid Agency Security Management and the ISO Risk Management Guidelines, Discussion Paper; Geneva: Security Management Initiative.

Mitroff, I., Pearson, C. (1993) Diagnostic Guide for improving your organization's crisis preparedness, San Francisco: Jossey-Bass: 13.

Morgan, G. (1986) 'Images of Organization', in Buchanan, D.A. and Bryman, A. (2011) The Sage Handbook of Organizational Research Methods, Sage: London: 128-129.

Mowday, R.T. and Sutton, R.I. (1993) *Organizational behavior: linking individuals and groups to organizational contexts. Annual Review of Psychology*, 44; available online at: http://www.annualreviews.org/doi/abs/10.1146/annurev.ps.44.020193.001211; accessed 11 April, 2013: 195–230.

Muhwezi, J., Kamugisha, A., Kaboyo, A. (2013) 'ALGERIA: Deadly Hostage Crisis', Africa Research Bulletin: Political, Social and Cultural Series, February 2013, 50(1); available online at: http://onlinelibrary.wiley.com.ezproxy4.lib.le.ac.uk/doi/10.1111/j.1467-825X.2013.04899.x/pdf; accessed 27 July, 2013: 19563A–19565C.

Nachmias, D. and Nachmias, C. (1981) *Research Methods in Social Science* in Institute of Lifelong Learning (2008) MSc in Risk, Crisis and Disaster Management, Module 3.

Nalla, M.K., Christian, K.E., Morash, M.A., Schram, P.J. (1996), Journal of Criminal Justice Education, 7(1), 18 August 2006, Michigan; available online at: http://www.tandfonline.com/doi/pdf/10.1080/10511259600083611: accessed 11 January, 2014: 79-97.

Nosworthy J. (2000) 'Implementing information security in the 21st Century – do you have the balancing factors?', Computers and Security, 2000, 19(4): 337–347.

O'Neill, M. (2008) 'Acceptance: An Approach to Security as if People Mattered', Monday Developments, Save the Children, February 2008; available online at: http://www.google.de/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=3&cad=rja&ved=0CE0QFjAC&url=http%3A%2F%2Fwww.eisf.eu%2Fresources%2Fdownload.asp%3Fd%3D1539&ei=ndryUf-QKsfXtAb1sYHYAw&usg=AFQjCNHfoeIiW7pnKIpIb6-Ao2LEXLPSA&sig2=lKuffc-Q_5pGw5-Er2wPug&bvm=bv.49784469,d.Yms; accessed 26 July, 2013.

OCHA (2012) OCHA Message: Humanitarian Principles, OCHA: Protection and Displacement Section; available online at: https://ochanet.unocha.org/p/Documents/OOM-humanitarianprinciples_eng_June12.pdf; accessed 20th August, 2013.

OECD (2012) Fragile States 2013: Resource flows and trends in a shifting world, OECD Publishing; available online at: http://www.oecd.org/dac/incaf/FragileStates2013.pdf; accessed 28 August, 2013.

OECD (2012a) *Managing Risks in Fragile and Transitional Contexts: The Price of Success?*, Conflict and Fragility, OECD Publishing; available online at: http://www.keepeek.com/Digital-Asset-Management/oecd/development/managing-risks-in-fragile-and-transitional-contexts_9789264118744-en; accessed 25 July, 2013.

OECD Nuclear Agency. (1987) 'Chernobyl and the Safety of Nuclear Reactors' in OECD Countries. Paris: OECD.

Oxford Dictionaries (2013) ´Definition Confidential ´; available online at http://oxforddictionaries.com/definition/english/confidential; accessed 4 February 2013.

Parker, M. (2000) Organizational culture and identity, London: Sage Publications.

People in Aid (1997) code of good practice in the management and support of aid personnel, London: People in Aid.

People in Aid (2003) code of good practice in the management and support of aid personnel, London: People in Aid.

Perrow, C. (1999) Normal accidents: living with high-risk technologies, Princeton, N.J., Princeton University Press: 5.

Pettigrew, A. M. (1979) 'On studying organizational cultures', Administrative Science Quarterly, 24: 570-581.

Phelan, K. (2010) 'Review of Managing Security Overseas: Protecting Employees and Assets in Volatile Regions', Journal of Homeland Security and Emergency Management, 7 (1), Art. 9; available online at: http://www.degruyter.com.ezproxy3.lib.le.ac.uk/view/j/jhsem.2010.7.1/jhsem.2010.7.1.1714/jhsem.2010.7.1.1714.xml; accessed 15 June 2013.

Pidgeon, N. and O'Leary, M. (2000) 'Man-made disasters: why technology and organizations (sometimes) fail', Safety Science, 34: 15-30.

Pidgeon, N., Hood, C., Jones, D., Turner, B. and Gibson, R. (1992) 'Risk Perception', in The Royal Society Report (1992) Risk: Analysis, Perception and Management, London: Royal Society, 89-134.

Pidgeon, N.F. (1991) 'Safety Culture and Risk Management in Organizations', Journal of Cross-Cultural Psychology, 22 (1): 129-140.

Porter, M. (1994) '"Second Hand Ethnography": Some Problems in Analysing a Femenist Project' in Institute of Lifelong Learning (2008) MSc in Risk, Crisis and Disaster Management, Module 3.

Prasad, P and Prasad A. (2009) 'Endless Crossroads: Debates, Deliberations and Disagreements on Studying Organizational Culture', in Buchanan, D.A. and Bryman, A. (2011) The Sage Handbook of Organizational Research Methods, Sage: London: 128-129.

Provera, B., Montefusco, A. and Canato, A. (2008) ´A 'no blame' approach to organizational learning´, British Journal of Management, December 2010, 21 (4); available online at: http://onlinelibrary.wiley.com/doi/10.1111/j.1467-8551.2008.00599.x/abstract; accessed 23 March, 2013: 1057-1074.

Reason, J. T. (1997) Managing the Risks of Organizational Accidents, Aldershot, U.K.: Ashgate.

Reason, J. T. (2000) 'Human error: Models and management', British Medical Journal, 320 (7237); available online at: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1117770/?tool=pmcentrez&rendertype=abstract ; accessed 12 March, 2013: 768-770.

Roper, C. A., (1999) Risk Management for Security Professionals, Burlington: Butterworth Heinemann.

Rose, G. (1982) *Deciphering Sociological Research* in Institute of Lifelong Learning (2008) MSc in Risk, Crisis and Disaster Management, Module 3.

Ruighaver, A.B., Maynard, S.B. and Chang, S. (2007) 'Organizational security culture: Extending the end-user perspective', Computers & Security, February 2007, 26 (1); available online at: (http://www.sciencedirect.com/science/article/pii/S016740480600157X); accessed 14 May, 2013: 56-62.

Saari, J. (1998) 'Safety interventions: international perspectives', in Feyer, A.M. and Williamson, A. (Eds.). Occupational Injury, Risk, Prevention and Intervention, London: Taylor and Francis: 179-194.

Schein, E. (2004) (3rd ed.) Organizational Culture and Leadership, San Francisco, CA: Jossey Bass.

Schein, E.H. (1996) 'Three Cultures of Management: The Key to Organizational Learning', *Sloan Management Review,* Fall 1996, 38 (1), Massachusetts; available online at: http://sloanreview.mit.edu/article/three-cultures-of-management-the-key-to-organizational-learning/; accessed 12 August, 2013.

Schneiker, A. (2011) ‚Sicherheitskonzepte deutscher Hilfsorganisationen. Zwischen Identitätswahrung und Pragmatismus', Zeitschrift für Außen- und Sicherheitspolitik, November 2011, 4 (4), Hannover; available online at: http://link.springer.com/article/10.1007%2Fs12399-011-0220-9#; accessed 17 March, 2013: 627-644.

Security Management Initiative (SMI) (2013) 'The price of anything' campaign; available online at: http://www.securitymanagementinitiative.org/; accessed 30 August, 2013.

Sennewald, C. A. (2003) Effective Security Management, Burlington: Elsevier Science.

Shedden, P., Ahmad, A., Ruighaver, A.B. (2006) 'Risk management standards– the perception of ease of use'; available online at: http://www.isy.vcu.edu/~gdhillon/Old2/Old/secconf/pdfs/39.pdf; accessed 17 April, 2013.

Sheik, M., Gutierrez, M.I., Bolton, P., Spiegel, P., Thieren, M. and Burnham, G. (2000) 'Deaths among humanitarian workers', British Medical Journal, 2000, 321; available online at: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1118167/pdf/166.pdf; accessed 14 June, 2013: 166-168.

Shrivastava, P. (1987) (2nd ed.) Bhopal: Anatomy of a Crisis, London: Paul Chapman.

Slim, H (1996) Planning between danger and opportunity: NGO situation analysis in conflict related emergencies, 16 January 1996; available online at: http://www.google.de/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=2&cad=rja&ved=0CDkQFjAB&url=http%3A%2F%2Fwww.securitymanagementinitiative.org%2Findex.php%3Foption%3Dcom_docman%26task%3Ddoc_download%26gid%3D62%26Itemid%3D&ei=6NjfUfvYHMXUswb9vIBo&usg=AFQjCNHgPzLH0fa-7O5Ao3jfIquUPG2Y7Q&sig2=IAI5exPNFitEyuJDs1jR3Q; accessed 12 July, 2013.

Slim, H (1996a) 'Planning between danger and opportunity: NGO situation analysis in conflict related emergencies', in VENRO (2003) Mindeststandards für die Personalsicherheit in der humanitären Hilfe; available online at: http://www.entwicklungsdienst.de/fileadmin/Redaktion/Publik_ext/Venro_Mindeststandard_HH.pdf; accessed 1 July 2013.

Slovic, P. (1987) 'Perception of Risk'. Science New Series, 26 (4799): 280-285.

Smallman, C. (1996) 'Challenging the orthodoxy in risk management', Safety Science, 22 (1): 245-262.

Smilie, L. and Minear, L. (2004) The charity of nations. Humanitarian action in a calculating world, Bloomfield: Kumarian Press.

Smith, D. and Irwin, A. (2006) 'Complexity, Risk and Emergence: elements of a *management* dilemma', Risk Management, 8 (4): 221-226.

Stoddard, A. (2013) 'Why Aid Workers are targets', The Globalist, May 14; available online at: http://www.theglobalist.com/storyid.aspx?StoryId=9991; accessed18 May, 2013.

Stoddard, A., A. Harmer and K. Haver (2011). Aid Worker Security Report 2011: Spotlight on Security for National Aid Workers: Issues and Perspectives. Humanitarian Outcomes; available online at: http://www.humanitarianoutcomes.org/sites/default/files/resources/AidWorkerSecurityReport20121.pdf; accessed 5 January, 2013.

Stoddard, A., Harmer, A. and Hughes, M. (2012) 'Aid Worker Security Report 2012 Host states and their impact for humanitarian operations', Humanitarian Outcomes, New York; available online at: http://www.humanitarianoutcomes.org/sites/default/files/resources/AidWorkerSecurityReport20126.pdf; accessed 1st April, 2013.

The Royal Society Report (1992) Risk: Analysis, Perception and Management, London: Royal Society.

The Sphere Project (2011) (5th ed.) Humanitarian Charter and Minimum Standards in Humanitarian Response, Northampton: Belmont Press Ltd; available online: http://www.sphereproject.org/resources/download-publications/?search=1&keywords=&language=English&category=22; accessed 6 August, 2013: 78-80.

Thoreau, H.D. (1817 – 1862) *Walden*; available online at: http://www.gurteen.com/gurteen/gurteen.nsf/id/X00228226/; accessed 28 August, 2013.

Thürer, D. (1999) The failed State and international law, *International Review of the Red Cross*, 836; available online at: http://www.icrc.org/eng/resources/documents/misc/57jq6u.htm; accessed 3 August, 2013.

Toft, B. and Reynolds, S. (2006) ´Learning from Disasters: a management approach´, Palgrave Macmillan: 48-49.

Unfallkasse des Bundes (2008) *Arbeits- und Gesundheitsschutz bei Auslandseinsätzen. Informationen und Mindeststandards zum Schutz von Sicherheit und Gesundheit des im Ausland eingesetzten* Personals, August 2008, Berlin: Bundesministerium des Inneren.

United Nations (1966) International Covenant on Economic, Social and Cultural Rights; available online: http://www.ohchr.org/Documents/ProfessionalInterest/cescr.pdf; accessed 14 June, 2013: 3.

Van Brabant, K. (2000) Operational Security Management in Violent Environments. London: HPN/ODI.

Van Brabant, K. (2001) HPG Briefing Mainstreaming Safety and Security Management in Aid Agencies, Humanitarian Policy Group, Overseas Development Institute, Number 2, London; available online at: http://www.odi.org.uk/sites/odi.org.uk/files/odi-assets/publications-opinion-files/369.pdf; accessed 30 April, 2013.

Van Brabant, K. (2010) (new ed.) HPN Good Practice Review. Operational Security Management in violent environments, Humanitarian Practice Network, Overseas Development Institute, Number 8, London; available online at http://www.odihpn.org/download/gpr_8_revised2pdf; accessed 03 September, 2012.

Van Brabant, K. (2011) (new ed.) HPN Good Practice Review. Operational Security Management in violent environments, Humanitarian Practice Network, Overseas Development Institute, Number 8, London: ODI.

Vaughn, J. (2009) 'The unlike securitizer: Humanitarian organizations and the securitization of indistinctiveness', in Schneiker, A. (2011) ‚Sicherheitskonzepte deutscher Hilfsorganisationen. Zwischen Identitätswahrung und Pragmatismus', Zeitschrift für Außen- und Sicherheitspolitik, November 2011, 4 (4), Hannover; available online at: http://link.springer.com/article/10.1007%2Fs12399-011-0220-9#; accessed 17 March, 2013: 627-644.

Vellani, K.H. (2009) Strategic Security Management. A Risk Assessment Guide for Decision Makers, Oxford: Butterworth-Heinemann: 109-119.

VENRO (2003) Mindeststandards für die Personalsicherheit in der humanitären Hilfe, Bonn: VENRO.

Waring, A. and Glendon, A.I. (1998) Managing Risks – Critical issues for survival and success into the 21st century, London: Thomson Learning.

Weik, K. E. and Sutcliffe, K. M. (2007) (2nd ed.) Managing the Unexpected: Resilient Performance in an Age of Uncertainty, San Francisco: Jossey-Bass.

Williamson, C. (2010) 'Personnel Management and security', Humanitarian Exchange, 47, HPN, London; available online at: http://www.odihpn.org/documents/humanitarianexchange047.pdf; accessed 14 June, 2013: 14-17.

Zimmer, M. (2010) 'Oil Companies in Nigeria: emerging good practice or still fuelling conflict?', in Deitelhoff, N. and Wolf, K. (2010) Corporate Security Responsibility? Corporate Governance contributes to peace and security in zones of conflict, Hampshire: Palgrave Macmillan: 58-84.