AAMEG

Australia-Africa Minerals & Energy Group

RISK SURVEY REPORT
Compiled on behalf of AAMEG

By

Risk 2 Solution

INTEGRATED RISK PROFESSIONALS

November 2015

Considerations:

- This document is intended for use by AAMEG (the Client) and its members. Upon handover of this completed document to the Client, Risk2Solution takes no further responsibility for the safe storage or distribution of the contents of this report by any of the client's employees, contractors or any other person associated with the client.
- This report is current as of the date on the cover page. Due to changes in the threat and risk environment, technological improvements and related factors, it should be noted that these recommendations may not be applicable or there may be alternative solutions or improvements based on technological and legislative changes.
- Risk2Solution Group takes no responsibility for the consequences of the client's, its members and/or associates or any other party's action or inaction based on recommendations and suggestions included in this document.
- The methodology, layout and structure remain the intellectual property of Risk2Solution Group.
- The preparation of this report is based on the responses from AAMEG members to the survey. Risk2Solution Group, its Directors, assessors or staff cannot be held liable for recommendations or findings based on limitations that may be attributed to the responses from the target audience base.

AUTHORS PROFILES:

This report was compiled for AAMEG by Risk2Solution Group. More information on the Group can be found at www.risk2solution.com or please email info@risk2solution.com.

The following personnel provided input into this report:

Dr Gavriel Schneider

- Doctor of Criminology degree with specialisation in security management (Dlitt et Phil Crim – Sec man)
- Master of Technology degree in Security Risk Management (MTSEC)
- Bachelor of Business Administration degree majoring in Security Risk Management (BBA)
- Advanced Diploma in Integrated Risk Management
- Advanced Diploma in Occupational Health Safety (OHS) and WHS
- Advanced Diploma in Project Management
- Diploma in Quality Auditing
- ASIS Certified Protection Professional (CPP)
- Fellow and member of the Board of Governors of the South African Institute of Security (SAIS)
- Fellow of the Australian institute of Management (FAIM)
- Licensed Security Advisor
- Aviation Security Qualified
- Port Facility Security Officer
- Assessor, Moderator and Verifier (SASSETA**)**

Professor Anthony Minnaar:

- Professor of Criminal Justice Studies
- Programme Head: Security Management
  Department of Criminology & Security Science
  School of Criminal Justice, College of Law
  University of South Africa (UNISA)

Natasha Lutchmarin:

- Magister Technologiae: Security Risk Management (Research Master's Degree (University of South Africa))
- Bachelor of Criminology honours (University of KwaZulu-Natal)
- Bachelor of Criminology (University of KwaZulu-Natal)
- Advanced Short Course in Outcomes-Based Assessment in Higher Education and Open Distance Learning (University of South Africa)
- Certificate Short Course: Security Risk Management (University of South Africa)
- Former role as lecturer at the University of South Africa (Program: Security Risk Management). Subject head for specialisation stream Security Technology and Information Security.

1. EXECUTIVE SUMMARY:

Risk2Solution on behalf of AAMEG conducted a survey to benchmark the current base line realities and gap areas of its member base. The survey of 19 questions focused on non-technical risk including safety, security, emergency response and related fields which are often referred to as ‘Hard Risk’. The target population included senior executives or board members of AAMEG and was sent out to approximately 100 members with a completed response rate of 19 surveys being returned. Whilst this is slightly lower than anticipated, it has provided for a base level analysis of market trends and requirements in this area. For ease of review each question has been structured into a core output point. These points are as follows:

1. ***Respondents have indicated that there is a medium to high Hard Risk exposure for their organisations.***
2. ***Respondents have indicated that the effectiveness of Hard Risk Management activities only seem to be achieved by approximately 50% of its members.***
3. ***84% of the respondents believe the directors and senior officers have a Duty of Care responsibility to employees, consultants and contractors and have been implementing mitigation measures as effectively as possible.***
4. ***28% of respondents have had to claim on insurance or pay out a sum of money as a result of a foreseeable risk actually occurring. This indicates a potential weakness in the Risk minimisation and management areas.***
5. ***37% of respondents have made an insurance claim or paid out a sum of money as a result of an unforeseeable risk actually occurring. This indicates a potential weakness in the Risk Identification and Assessment areas.***
6. ***There is a significant gap with regard to awareness, uptake and implementation of the Voluntary Principles of Security and Human Rights.***
7. ***Traveller safety and associated risk is an area of concern for the respondent base.***
8. ***Respondents appear to be satisfied with their risk management, security, safety and emergency response service providers. There are however aspects and areas of delivery and supply that could be improved.***
9. ***Based on the respondents correlated risk concern areas, Bribery and Corruption appears to be the most concerning risk factor for CEO and senior executives.***
10. ***The majority (75%) of the respondents include Risk management as a core strategic activity. Over 30% did not include it or felt that it was a hindrance to core business.***
11. ***Less than 50% of respondents would recommend their current risk, safety and security providers which may indicate a lack of confidence in service provisions.***
12. ***The majority of respondents believe that they have an understanding of the risk management process and its intricacies.***
13. ***There is a 50/50 division among respondents to risk management with regards to their risk altitudinal leaning. Over half feel it’s a necessary activity but do not apply a proactive and preventative approach.***

14. ***Key benefits and features of a robust risk management system have a broad range but hinge on aspects such CEO and board experience as well as regular review and updates.***
15. ***Based on respondent feedback there are numerous areas for improvement and enhancement of risk management that need to be addressed.***
16. ***Based on respondent feedback it would appear that respondents agree with the need to have robust risk management systems in place to attract investors and capital.***
17. ***There are numerous frustrations that reflect both internal and external realities including culture, behaviour and political issues.***
18. ***As an indicative sample just over half of the respondents are utilising professional training and development expertise to upskill themselves and their staff in the field of risk management.***
19. ***Time allocation to risk activities is a critical consideration and based on respondent's feedback there is potential to better apply time spend in a proactive manner.***

This report, together with workshops and roundtable sessions, will be used a tool to develop and address issues of concern and importance in the risk management field. Whilst Risk2solution have created revolutionary new models to identify and mitigate critical hard risk concerns, the file is an evolving one, as are the related legislative considerations, threat and risk issues as well as political and societal issues. As such, this report should be viewed as a snapshot of the current situation with a need to be updated and addressed on an ongoing basis.

TABLE OF CONTENTS

2. BACKGROUND

AAMEG conducted a benchmark risk and related issues survey during September and October of 2015. The primary aim of the survey was to ascertain what issues are causing concern and determine a base starting point for AAMEG to explore opportunities for enhanced risk related identification and support for its membership base. The core goal of this initiative is to create a base starting point of what is needed in order to help member companies reduce overall risk to themselves, staff and operations. By adopting an established, robust and integrated risk approach it may be possible to assist in mitigating the impact of any unforeseen incidents/circumstances which may occur in the future.

The focus of this survey is directed towards non-technical risks such as safety, security, emergency response, business continuity, natural disasters, etc. For ease of explanation these risks will be referred to in this report as **'Hard Risk'**. The slant towards Hard Risk was based on indicative market request to focus in this area as well as the direction from AAMEG that technical risks were for the most part well addressed by members and supporting organisations. Accordingly, technical risks were excluded from the research survey.

This survey was compiled and distributed via an online portal. The self-administered questionnaire was directed at senior executives or board members and participation was voluntary. Responses were structured to be confidential and anonymous i.e. no participant's identities needed to be supplied for the survey to be completed.

3. PRESENTATION OF DATA

In this section of the report the findings of each question will be provided with a base analytical overview. The univariate analysis process was applied to the collected data in order to quantitatively analyse and interpret the data collected from the self-administered questionnaire survey. The data is presented in the form of frequency distributions within pie chart graphs and tables. A base analysis has also been provided. It should be noted that this report is structured as an analytical overview as opposed to an in-depth analysis.

It needs to be noted that the distribution pool for the survey was approximately 100 possible respondents with only 19 respondents completing the survey. Some of the 19 responses were also incomplete. This creates the potential for a statistical skewing of results but in consultation with AAMEG, it was decided that a base of approximately 20% as a response rate would be sufficient to draw out the required data. The number of respondents is not highlighted in each question unless there was a smaller response pool than 19.

Note: Where applicable in certain locations for ease of reading and explanation, percentages have been rounded up to the nearest 0.5%.

3.1. Question 1

In terms of non-technical risk (Hard Risk), how would you rate your company's overall risk exposure?

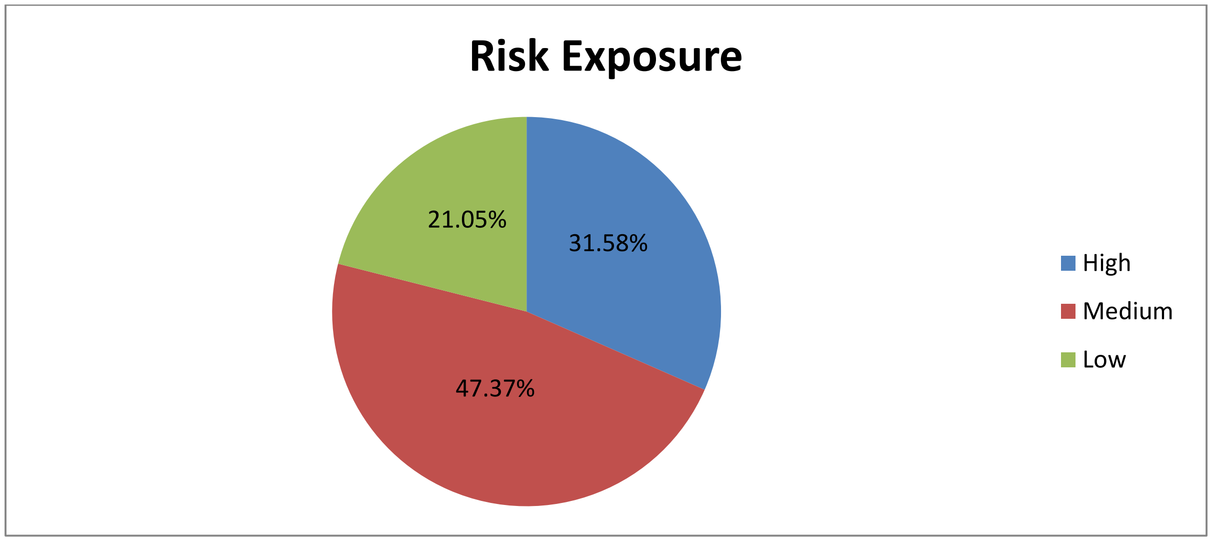

Figure 1: Risk Exposure

The majority of the respondents, 78.95%, indicated that their company or organisation either had a medium or high risk exposure level. This indicates that there is a possibility that improvements can be made in terms of risk management processes and this should be investigated further. An integrated and proactive stance should be assessed as a collective. Joint initiatives to enhance security, safety and emergency response may assist cost effectiveness and reduce risk exposure. Managing an event or incident from a reactive posture can lead to unnecessary, increased losses.

Core finding – AAMEG members have indicated that there is a medium to high Hard Risk exposure for their organisations.

3.2. Question 2

Are the following activities conducted effectively in your company?

Effectiveness of activities	Ineffective	Average	Effective	Sample size
Risk identification	15.79% (3)	26.32% (5)	57.89% (11)	19
Evaluating and measuring of risk using a system	31.58% (6)	21.05% (4)	47.37% (9)	19
Determining appropriate risk mitigation/management measures	21.05% (4)	26.32% (5)	52.63% (10)	19
Implementing and applying risk mitigation measures	23.53% (4)	23.53% (4)	52.94% (9)	17
Monitoring and evaluation of changes and risk mitigation measures on an ongoing basis	26.32% (5)	31.58% (6)	42.11% (8)	19

Table: Effectiveness of activities

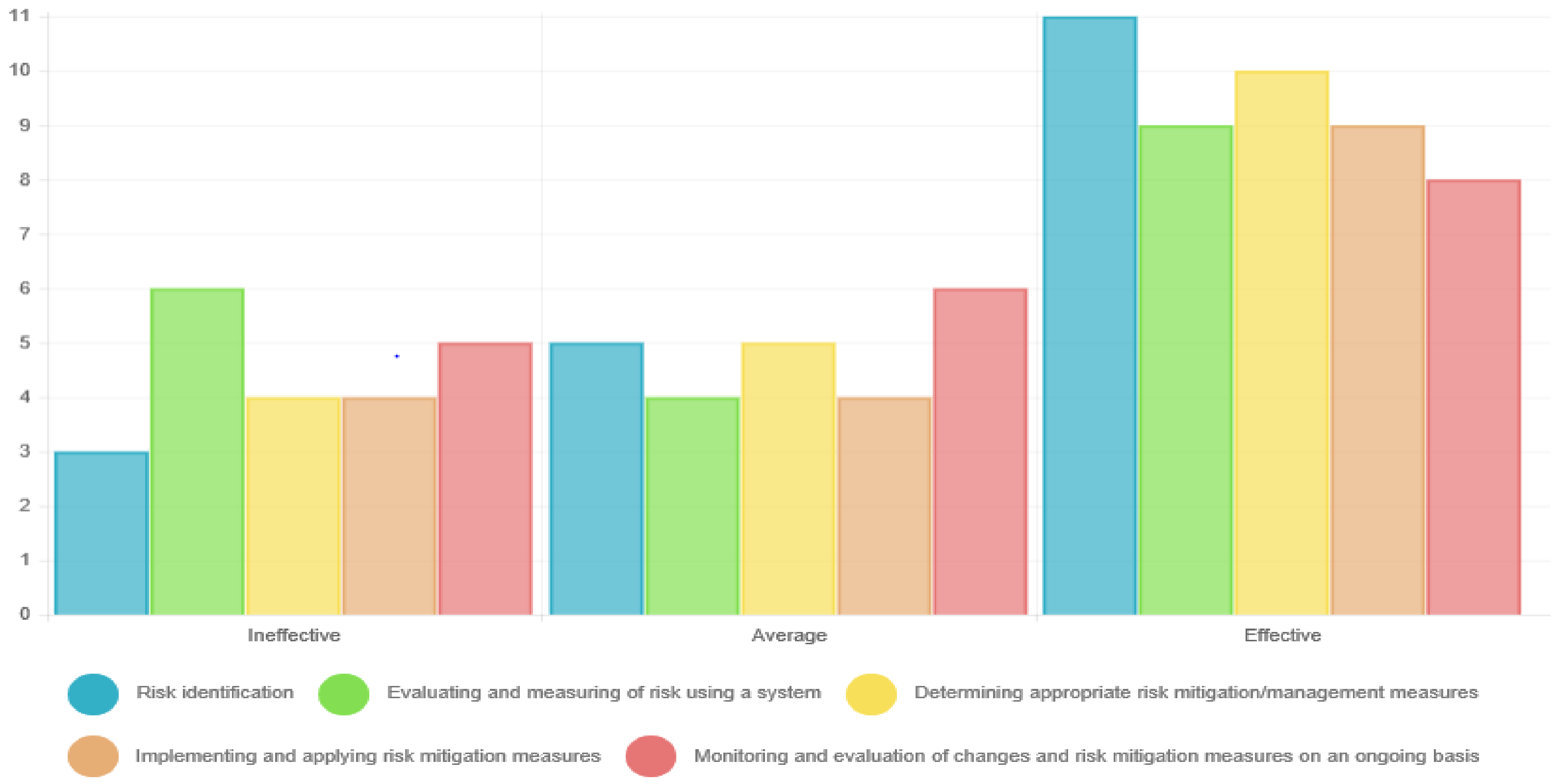

Figure: Effectiveness of activities

The responses received from the previous question indicated that risk exposure levels were medium/high. This question was designed to assess whether the effectiveness of activities was commensurate with the risk exposure levels. It is a potentially worrying indicator that approximately only 50% of respondents believed that their Hard Risk processes were Effective.

Core finding – Respondents have indicated that the effectiveness of Hard Risk Management activities only seems to be achieved by approximately only 50% of its members.

3.3. Question 3

As a senior executive or company director you may be held personally accountable for the death or injury of a member of company staff. Which of the statements below best reflects your feelings?

Death or injury of staff	Frequency	% of cases
I do not worry about this at all and no solutions and mitigations are being implemented as they are too costly and not a current priority	1	5.26%
I occasionally worry about this but find it challenging to implement solutions and mitigations as they are too costly and not a current priority	2	10.53%
I am aware that directors and senior offices have a Duty of Care responsibility to employees, consultants and contractors and have been implementing mitigation measures as effectively as possible	16	84.21%

Table: Deaths or injury to staff

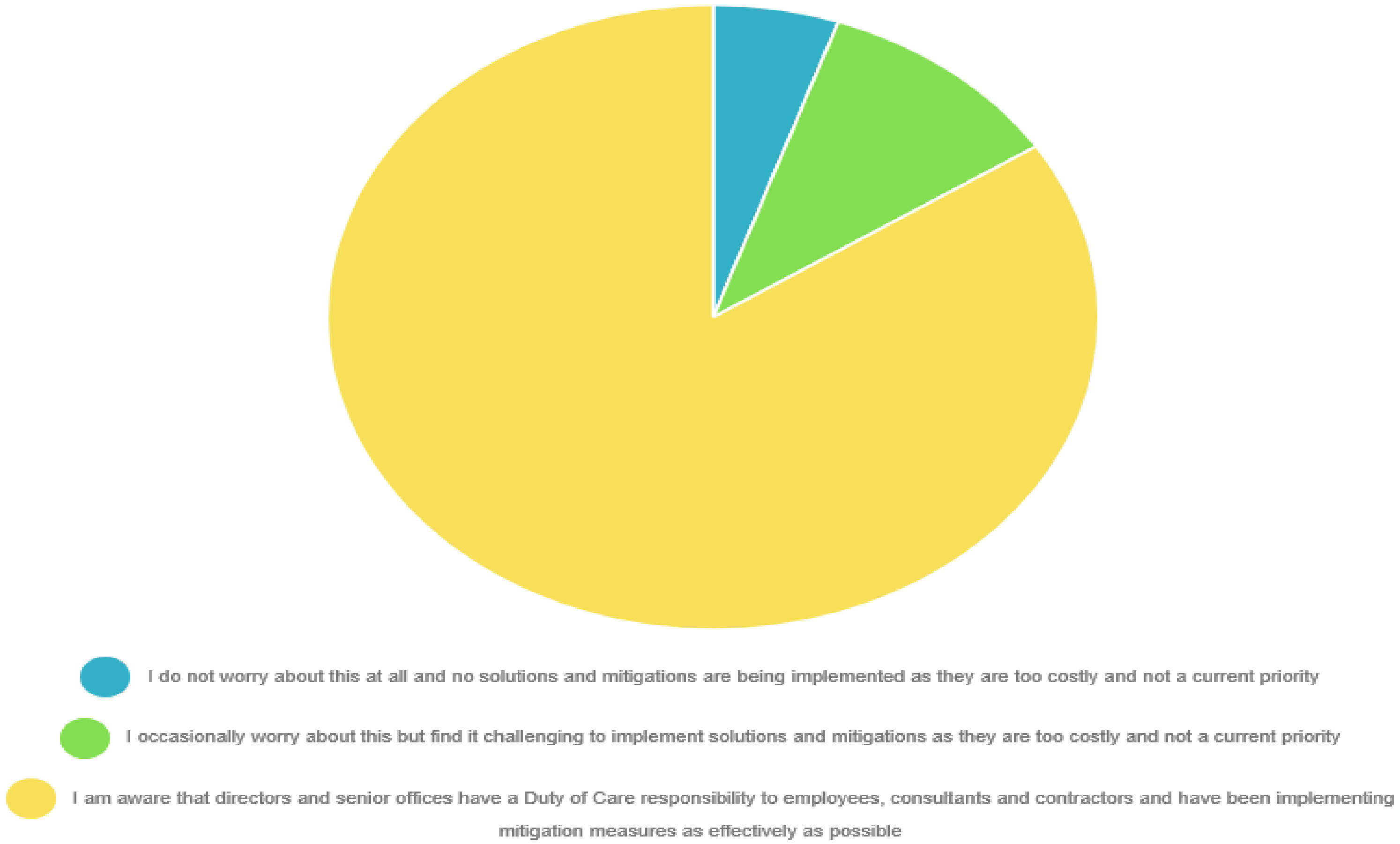

Figure: Deaths or injury to staff

With the exception of 15.79% respondents, the other 84.21% respondents returned a positive response demonstrating an acknowledgment of the seriousness of managing hard risk. Based on the previous feedback where approximately only 50% of respondents identified that their risk management approaches were effective, this indicates a discrepancy in the application of Hard Risk management approach compared to the seriousness, understanding and acceptance of the respondents.

Core finding – 84% of the respondents believe that they are aware that directors and senior offices have a Duty of Care responsibility to employees, consultants and contractors and have been implementing mitigation measures as effectively as possible.

3.4. Question 4

Have you ever had to claim from insurance or had to pay out a sum of money without claiming, in reference to an incident or event, as a result of foreseeable risk?

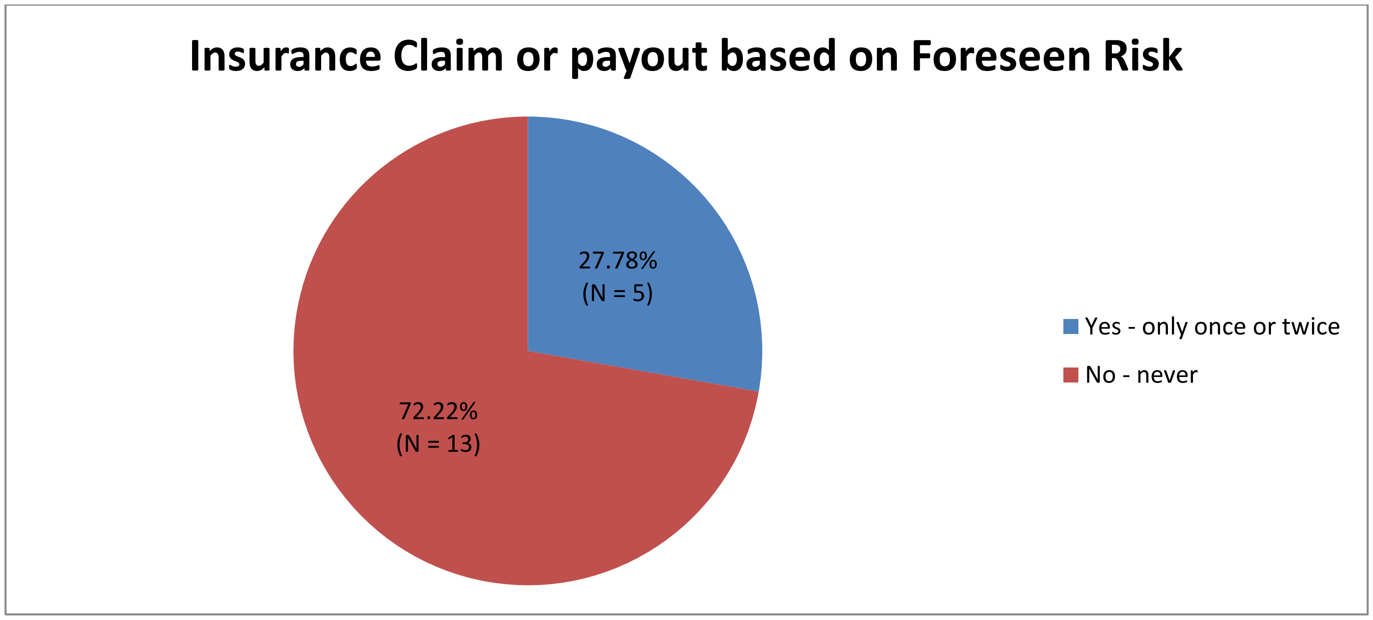

Figure 4: Foreseen risks

72.22% of the respondents specified that they have never had to claim from insurance or had to pay out a sum of money without claiming, in reference to the occurrence of an incident or event as a result of a foreseeable risk. However, a significant proportion of respondents, 27.78%, indicated that they have experienced a foreseen risk and the resulting financial consequences and viewed this as one of the many facets of risk. This indicates that risk exposure indicators are real and that incidents do actually occur even if they are foreseen. It further indicates a potential weakness in risk minimisation and management.

Core finding – 28% of respondents have had to claim on insurance or pay out a sum of money as a result of a foreseeable risk actually occurring. This indicates a potential weakness in the Risk minimisation and management areas.

3.5. Question 5

Have you ever had to claim from insurance or had to pay out a sum of money without claiming, in reference to an incident or event, as a result of unforeseeable risk?

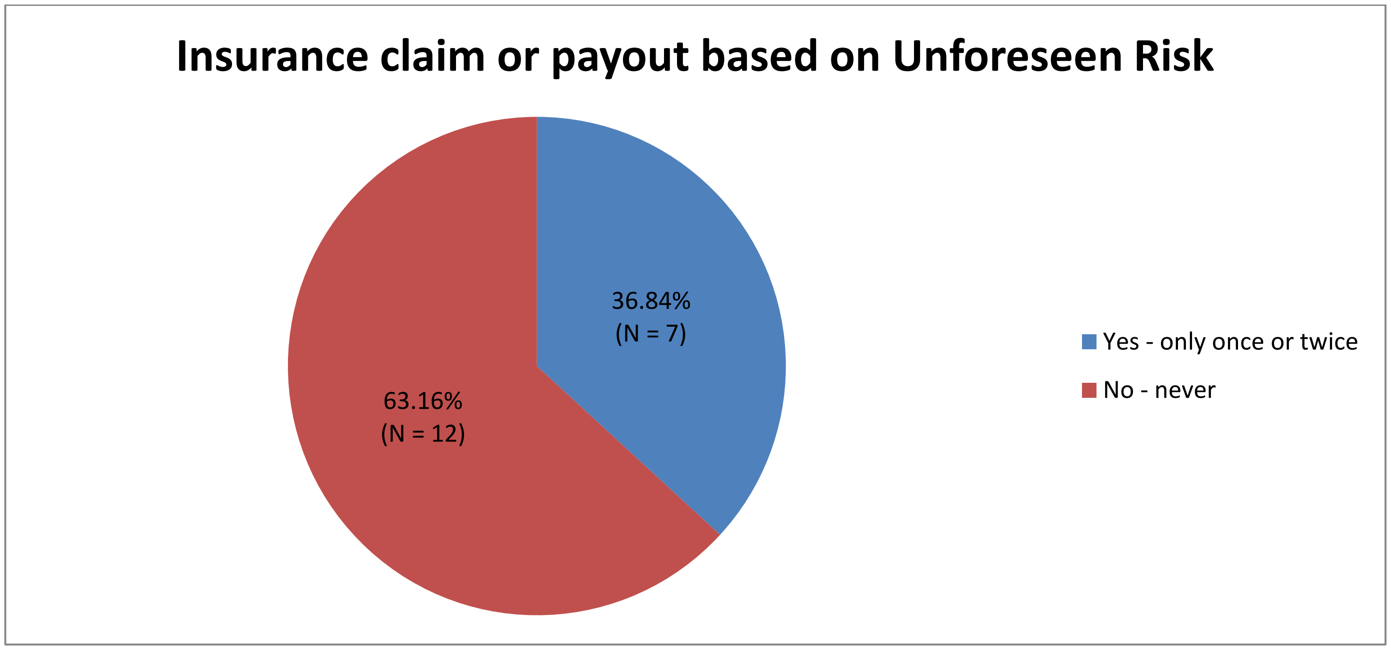

Figure: Unforeseen risk

63.16% of the respondents specified that they have never had to claim from insurance or had to pay out a sum of money without claiming, in reference to the occurrence of an incident or event as a result of an unforeseeable risk. However, a significant proportion of respondents, 36.84%, indicated that they have experienced unforeseen risk and the resulting financial consequences as one of the many facets of risk. This indicates a potential weakness in risk identification.

Core finding – 37% of respondents have had to claim on insurance or pay out a sum of money as a result of an unforeseeable risk actually occurring. This indicates a potential weakness in the Risk Identification and Assessment areas.

3.6. Question 6

Does your company understand and apply the Voluntary Principles of Security and Human Rights?

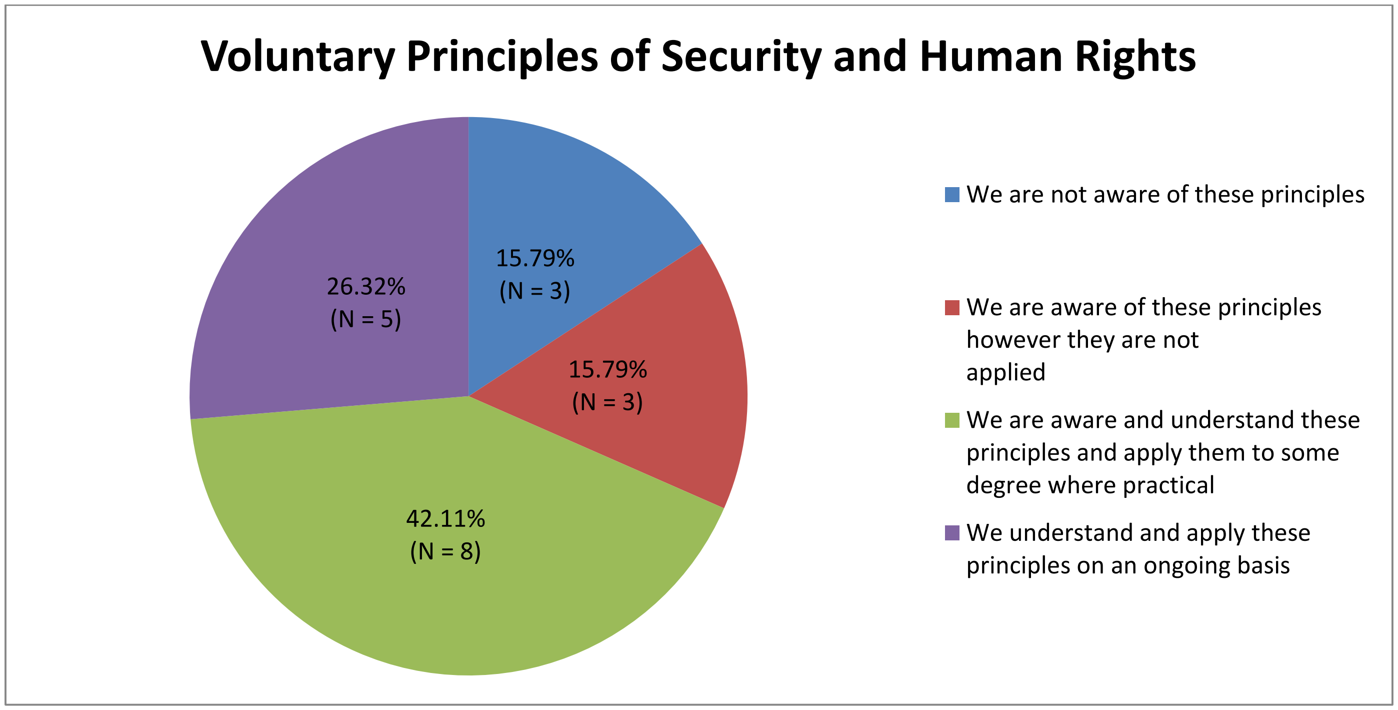

Figure: Voluntary Principles of Security and Human Rights

With only 26% of respondents indicating that they understand and apply Voluntary Principles on Security and Human Rights on an ongoing basis, consideration should be given to this as they are a set of non-binding principles created to assist extractive companies to balance security concerns with human rights. 32% indicated that they are either not aware of the principles or are aware but do not apply them at. This indicates that there is a requirement for education and support in this area.

Core finding – there is a significant gap with regards to awareness, uptake and implementation of the Voluntary Principles of Security and Human Rights.

3.7. Question 7:

Which statement below reflects the way your organisation manages traveller and expat safety risk?

Traveller and expat safety risk	Frequency	% of cases
We manage traveller and expat safety risk extremely well and I would have no concern if an incident occurred and we were held to account	3	15.79%
We manage traveller and expat safety risk adequately however I would have some concern if an incident occurred and we were held to account	12	63.16%

We have limited resources and rely on the individual traveller and/or expat to manage their own risk	2	10.53%
We only travel to safe locations and do not perceive traveller or expat safety as being a risk in our operation	2	10.53%

Table: Traveller and expatriate safety risk

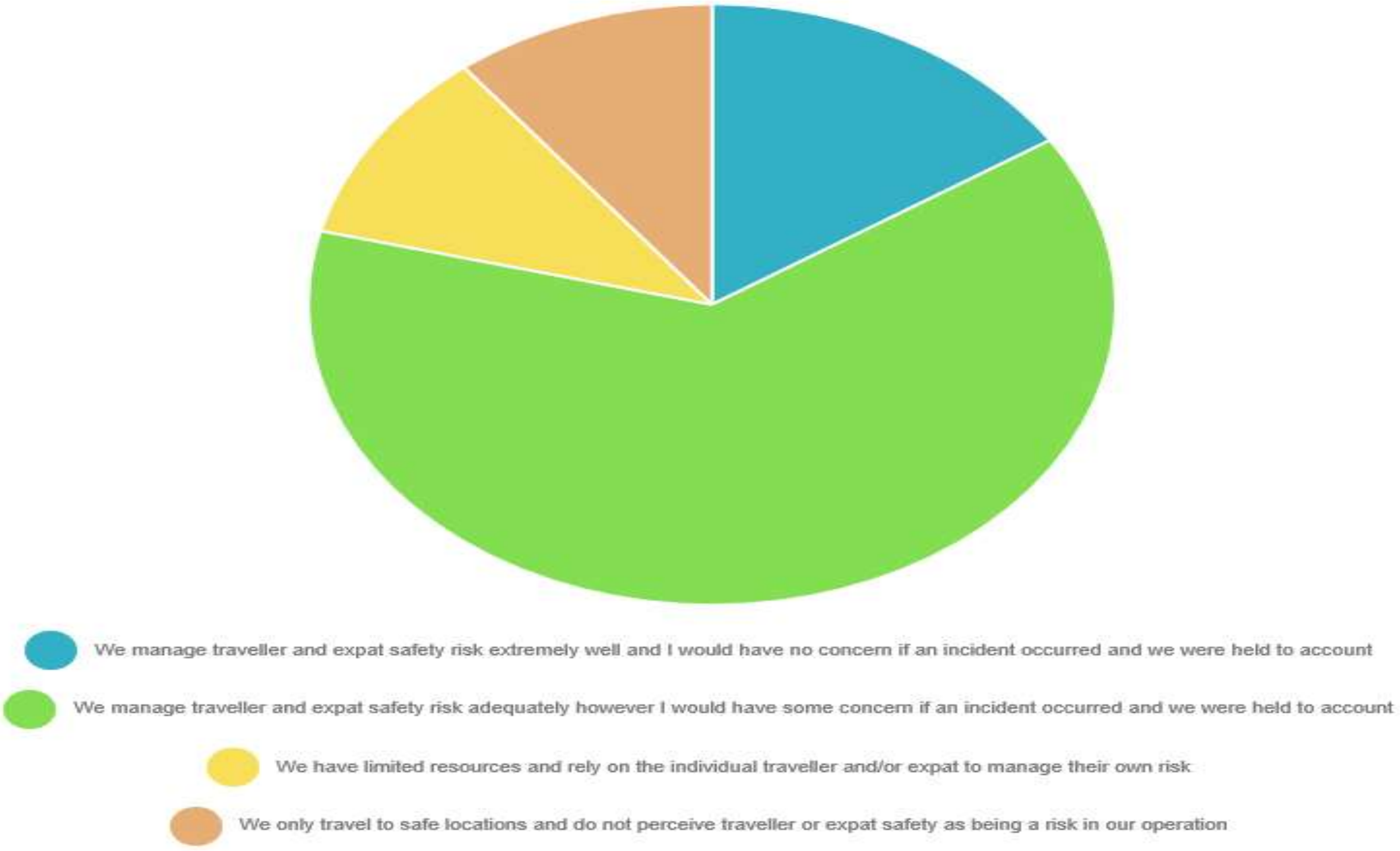

Figure: Traveller and expatriate safety risk

With 74% of respondents indicating that they have some concerns in this area or are forced to rely on the individual to manage their own risk, this is clearly an area of significant concern. An employee or employees working in foreign countries is/are not a new phenomenon, however, this often exposes these individuals to safety risks which could include aspects such as crime, terrorism, or health issues. With only 16% indicating that they manage travel risk very well there is a definite requirement for the broader base of AAMEG members to better address this area.

Core finding – Traveller safety and associated risk is an area of concern for the respondent base.

3.8. Question 8:

Please rate your level of satisfaction in reference to risk management, security, safety and emergency response service providers.

The following were the options provided from which respondents had to choose a rating for each ranging from ‘poor’, ‘average’ ‘good’ to ‘excellent’.

Option 1	Solutions are simple and easy to source
Option 2	Solutions are simple and easy to implement and manage
Option 3	Solutions are cost effective
Option 4	Providers understand the reality of limited budgets whilst needing a solution
Option 5	Solutions are flexible and can be scaled up and down as required
Option 6	Solutions are proactive and usually purpose us to be able to manage the unexpected and align with my organisational objectives

Service providers	Unsatisfactory	Poor	Average	Good	Excellent	Sample size
Option 1	0	11.11% (2)	38.89% (7)	44.44% (8)	5.56% (1)	18
Option 2	0	11.76% (2)	47.06% (8)	41.18% (7)	0	17
Option 3	11.11% (2)	11.11% (2)	55.56% (10)	22.22% (4)	0	18
Option 4	5.56% (1)	16.67% (3)	33.33% (6)	44.44% (8)	0	18
Option 5	0	22.22% (4)	33.33% (6)	44.44% (8)	0	18
Option 6	5.56% (1)	22.22% (4)	38.89% (7)	33.33% (6)	0	18

Table: Service providers

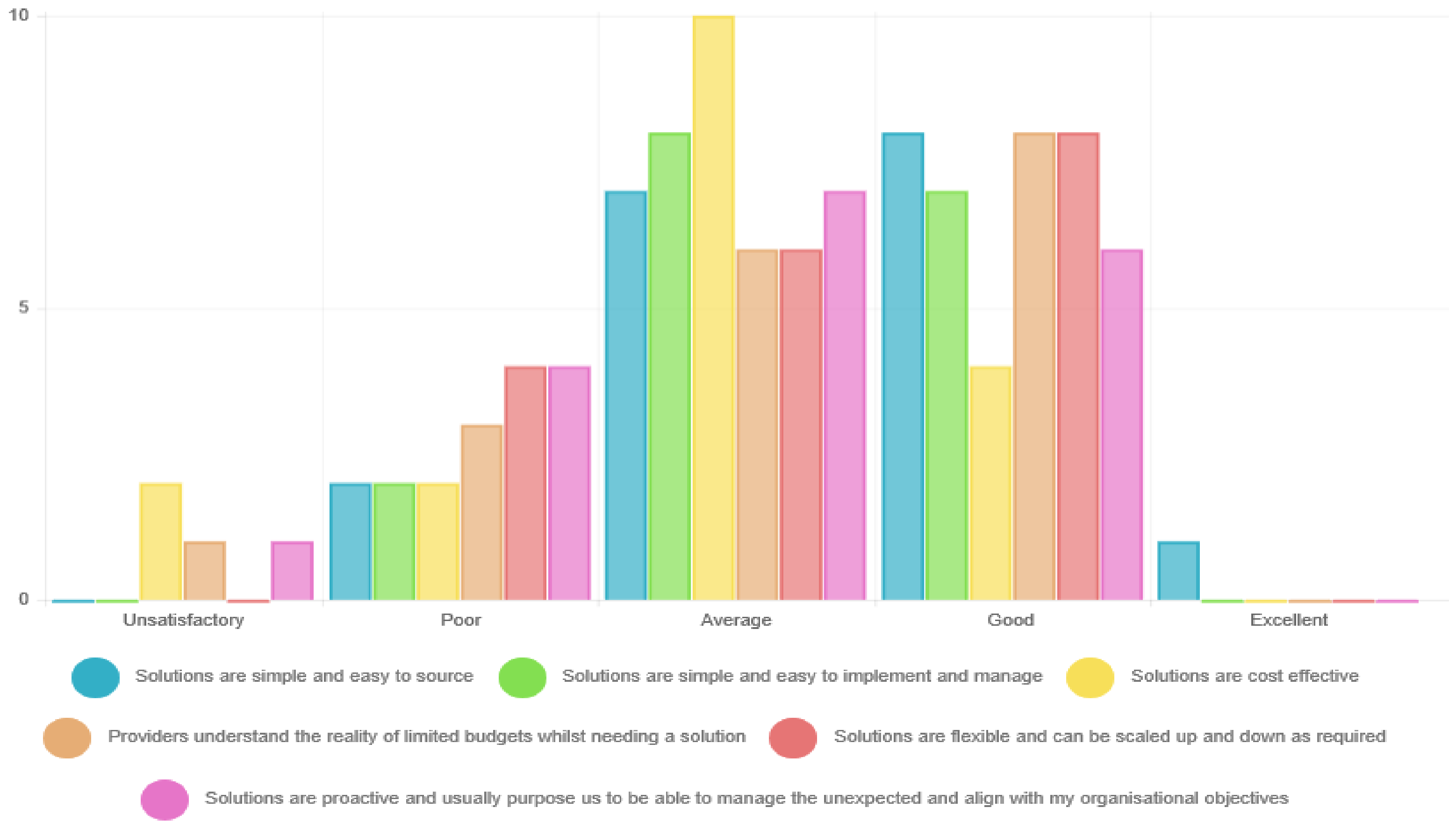

Table: Service providers

This is a multiple response question. Most of the respondents rated their service providers as 'Average' or 'Good'. Therefore the majority of the respondents were satisfied with the produces delivered by their service providers in terms of risk management, security, safety and emergency response. As a point of reference the following three options all rated with between 20 and 30% ratings in the poor and unsatisfactory columns which indicated the potential for improvement in these aspects:

Option 4 Providers understand the reality of limited budgets whilst needing a solution

Option 5 Solutions are flexible and can be scaled up and down as required

Option 6 Solutions are proactive and usually purpose us to be able to manage the unexpected and align with my organisational objectives

Core finding – Respondents appear to be satisfied with their risk management, security, safety and emergency response service providers. There are however aspects and areas of delivery and supply that could be improved.

3.9. Question 9

Please rank the following risk exposure, from the perspective of a CEO in terms of non-technical risks, from the highest to the lowest. Click on option and drag.

Seventeen respondents provided a response to this question. Option descriptions are provided below:

Option 1	People and personnel safety -
Option 2	Political risk
Option 3	Financial and associated risk (including cash flow, process costs, etc.)
Option 4	Reputational risk to directors and senior executives
Option 5	Sovereign risk including expropriation nationalisation
Option 6	Road transport risk
Option 7	Social risk
Option 8	Cyber risks and data protection
Option 9	Reputational risk for the organisation
Option 10	Compliance and legislative risks (including bribery and corruption)
Option 11	Health and medical risks
Option 12	Bribery and corruption risk
Option 13	Environmental risk
Option 14	Armed forces risk
Option 15	Public and security risks (including theft and fraud)
Option 16	Air travel risk

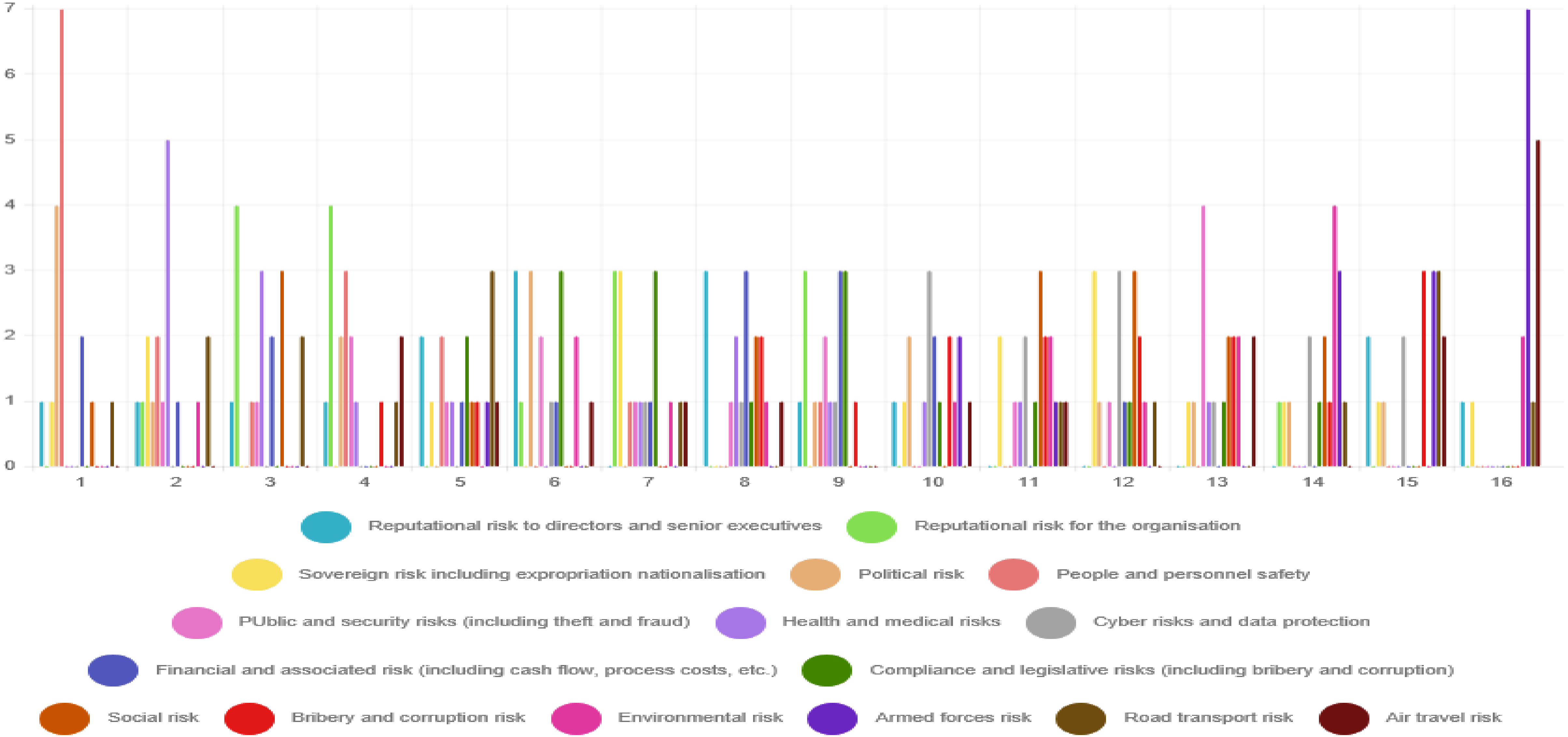

Figure: Feedback Risk Priority Rating

Feedback of risk priority	Aggregated Weighting
Bribery and corruption risk	13.82
Environmental risk	11.24
Armed forces risk	11.12
Road transport risk	11
Air travel risk	10.88
Reputational risk to directors and senior executives	9.24
Reputational risk for the organisation	9.06
Sovereign risk including expropriation nationalisation	8.47
Political risk	8.12
People and personnel safety	7.94
Public and security risks (including theft and fraud)	7.47
Health and medical risks	6.76
Cyber risks and data protection	6.53
Financial and associated risk (including cash flow, process costs, etc.)	5.76
Compliance and legislative risks (including bribery and corruption)	5.53
Social risk	3.06

Table: Feedback Risk Priority Rating

Core finding – based on the respondents correlated risk concern areas Bribery and Corruption appears to be the most concerning risk factor for CEO and senior executives.

3.10. Question 10

Do you include risk identification and mitigation/management as a fundamental element of corporate strategy?

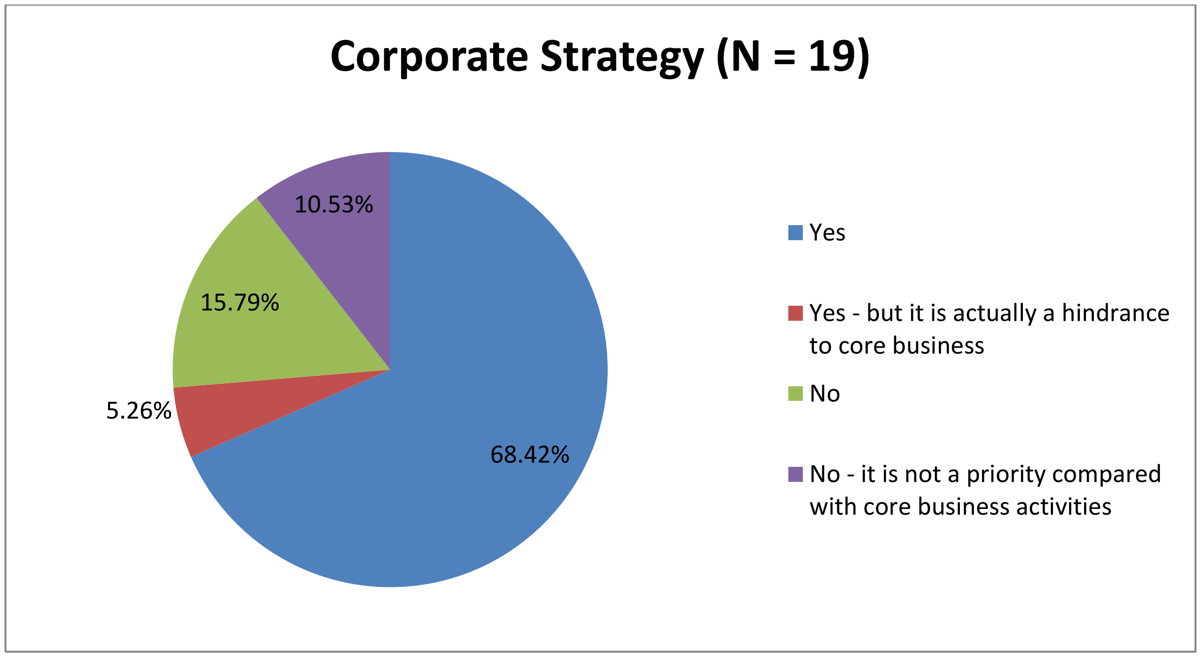

Table: Corporate strategy

Fourteen (73.68%) respondents indicated that risk identification and mitigation/management is included as a fundamental element of corporate strategy. Incorporating risk management as part of corporate strategy is essential and beneficial. This not only allows for and promotes accountability through good governance and robust business practices; it also contributes to strategic objectives such as creating a capable, agile and sustainable organisation and is a critical component of professional performance. The fact that over 25% of respondents did not include risk management as a core aspect of corporate strategy is a major point of concern

Core finding – the majority (75% of the respondents include Risk management as a core strategic activity. Over 30% did not include it or felt that it was a hindrance to core business.

3.11. Question 11

How likely is it that you would recommend your security, safety and risk providers to a friend or colleague? (N = 19)

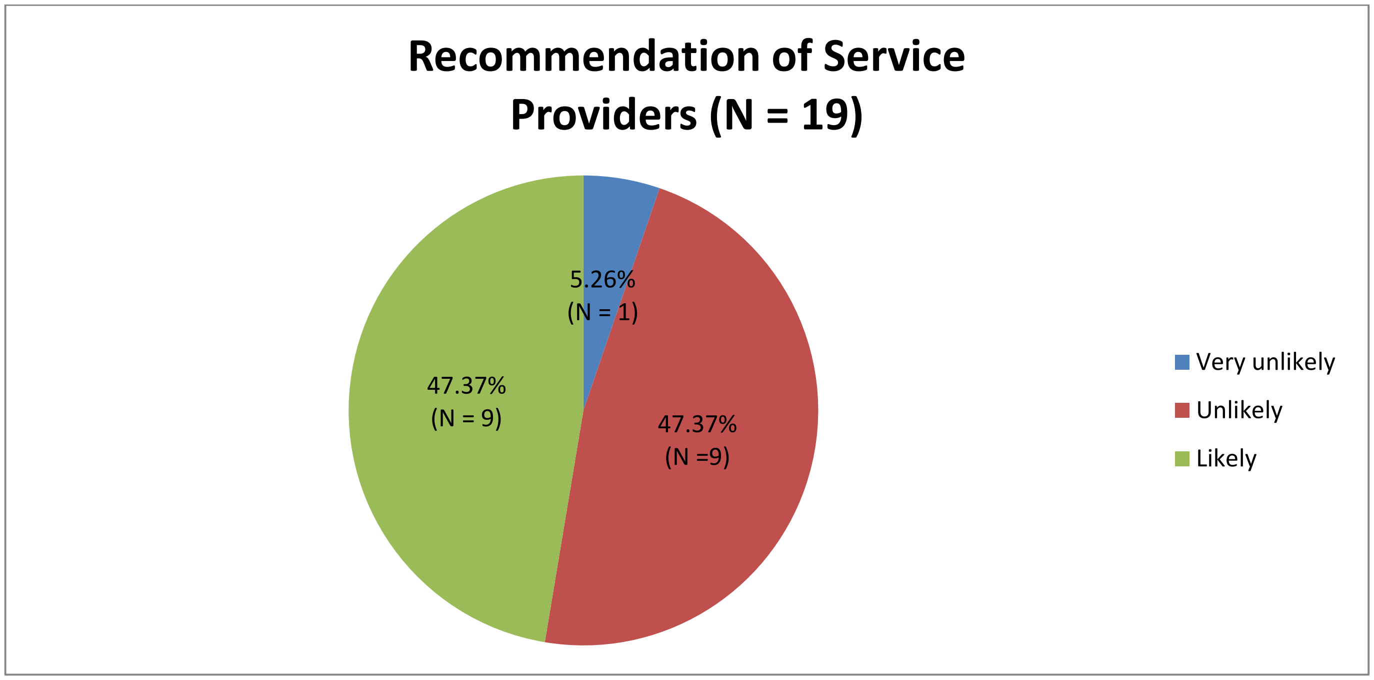

Figure: Recommendation of service

Nine (47.37%) of the respondents demonstrated a level of confidence, trust and satisfaction in their service providers and systems as opposed to the other ten (52.63%) respondents who stated that it is 'Unlikely' and 'Very unlikely' that they would recommend their service providers. This indicates that potentially over 50% of the respondents may have some concerns with their hard risk providers. This response indicates a slight discrepancy between the findings of question 8. A base interpretation of this appears that whilst service levels may be at an acceptable risk, providers are not considered worth recommending.

Core finding – less than 50% of respondents would recommend their current risk, safety and security providers which may indicate a lack of confidence in current hard risk service provisions.

3.12. Question 12

Please rate your level of understanding and comfort with regards to the following concepts of:

Option 1	Risk identification and the consequences thereof
Option 2	Acceptance of an identified risk as something you are willing to manage in house
Option 3	Risk mitigation and the consequences thereof
Option 4	Risk reduction and the consequences thereof
Option 5	Risk transfer/sharing and the consequences thereof
Option 6	Risk mitigation and the consequences thereof
Option 7	Consequence reduction
Option 8	Likelihood of occurrence reduction

Level of understanding	Don't understand	Basic	Average	Good	Frequency
Option 1	0	16.67% (3)	16.67% (3)	66.67% (12)	18
Option 2	5.56% (1)	16.67% (3)	33.33% (6)	44.44% (8)	18
Option 3	0	22.22% (4)	33.33% (6)	44.44% (8)	18
Option 4	0	17.65% (3)	41.18% (7)	41.18% (7)	17
Option 5	5.56% (1)	22.22% (4)	44.44% (8)	27.78% (5)	18
Option 6	5.56% (1)	16.67% (3)	27.78% (5)	50% (9)	18
Option 7	5.56% (1)	16.67% (3)	33.33% (6)	44.44% (8)	18
Option 8	5.56% (1)	16.67% (3)	27.78% (5)	50% (9)	18

Table: Level of understanding

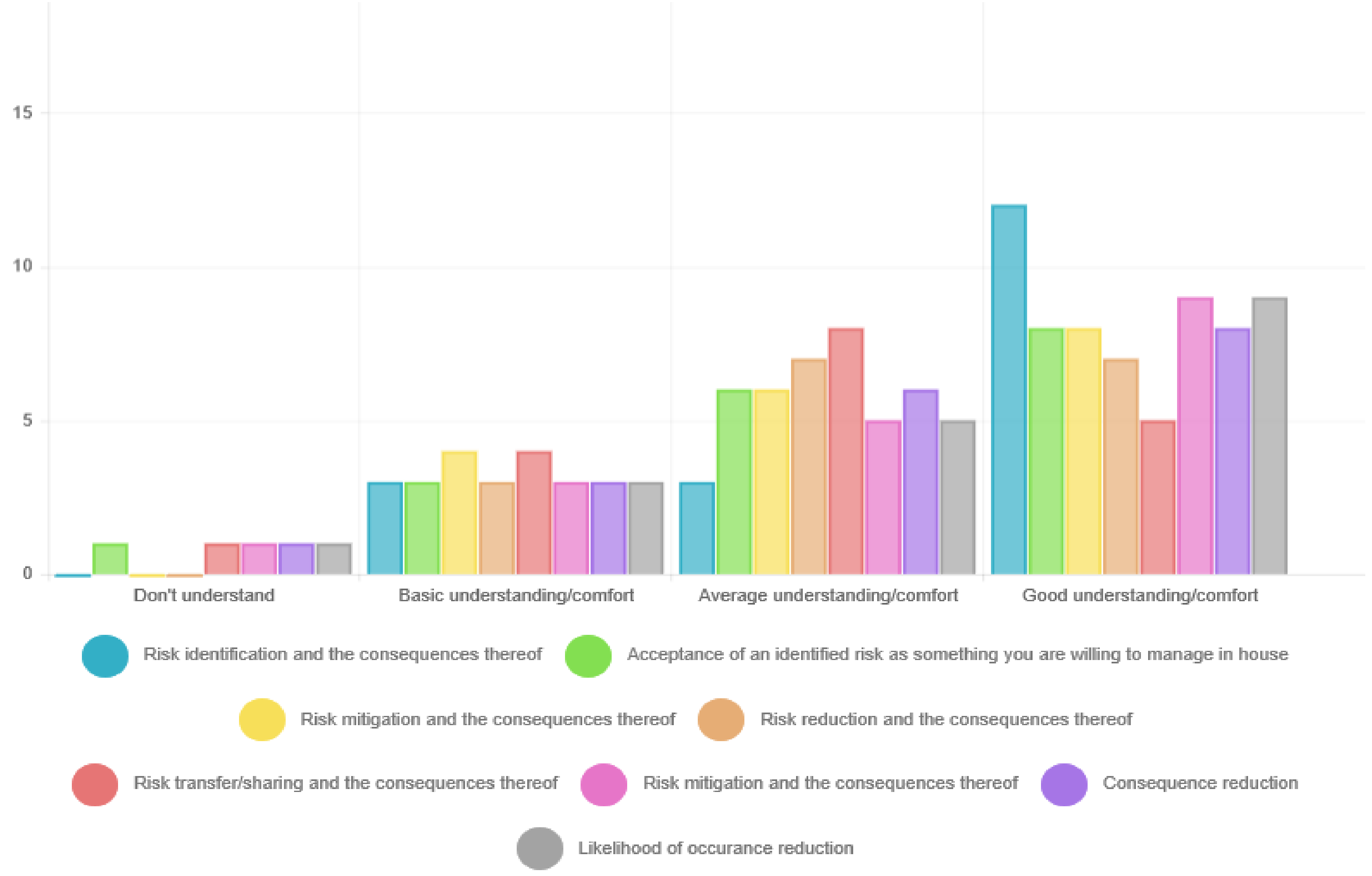

Figure: Level of understanding

This is a multiple response question. It was designed to gauge an understanding of the respondent's knowledge of the risk management process. The majority of respondents had either an 'Average' or a 'Good' understanding and comfort of the concepts listed. This indicates knowledge has been circulated within the company and been acquired. Accordingly it is surmised that an effort is being made to critically engage with the information provided.

Core finding – The majority of respondents believe that they have an understanding of the risk management process and its intricacies.

3.13. Question 13

My approach to managing risk could best be described as:

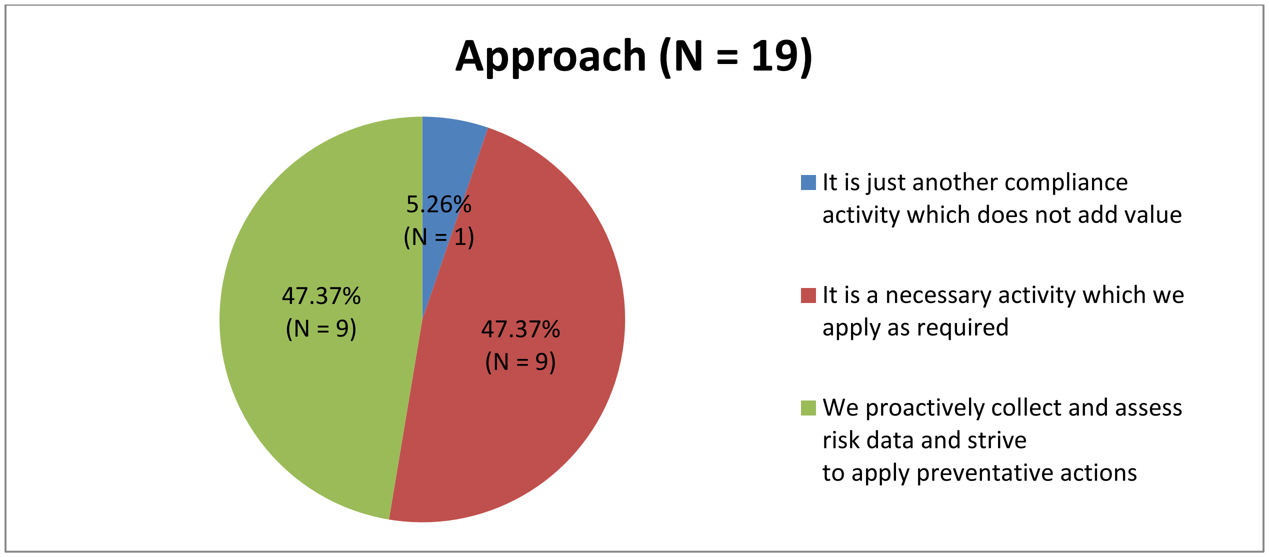

Figure: Attitudinal approach to risk management

This question was designed to scope the attitudinal leaning of the respondent's towards risk management. The three response options allowed for an illustration of perception and application of risk management. In this case it is clear, based on the equal response to the options of including risk management as a necessary activity or the next iteration which is centred on utilising risk management as a proactive tool to add value to operations. In order to achieve effective risk management, focus should be steered towards being proactive rather than reactive. For many businesses, risk management is fast developing into a more forward looking and thinking, integrated corporate approach. An effective risk management process that is based on proactive risk identification, measurement and treatment can both drive competitive advantage and sustain future profitability and growth.

Core finding – there is a 50/50 division among respondents with regards to their risk altitudinal leaning with regards to risk management. Over half feel it's a necessary activity but do not apply a proactive and preventative approach.

3.14. Question 14

What are the three best features of your company's risk management system or process?

This question allowed respondents to provide a list of their own subjective replies. There were thirteen respondents who contributed. One respondent indicated that they "have no system" and another stated that there system is "cumbersome". The other eleven respondents did go on to put forth what they qualify or deem as a best feature or best features of their company's risk management system or process.

Numerous 'best' features, with a cap of three per respondent, were listed as set out below and divided into three categories for ease of reference:

Cost based & direct process Related	**User friendliness**	**Outcomes & Related**
Reasonably cost efficient	Reporting/incident reporting (2)	Regular/annual review/assessment/modification of risk matrix (6)
It is a central and increasingly well-implemented process	Easily managed	Low turnover of the board and staff ensures retention of "corporate" knowledge
CEO/diverse board experience/in house professional leadership directs the process (5)	Simple/easy to understand risk matrix (2)	Long history of operation and experience
It is increasingly an integral part of the way we do business, it is not a peripheral system additional to our operating system (2)	It works (2)	Comprehensive matrix of potential risks, likelihood and consequence assessment, and mitigation measures (2)
	Buy in from employees	Drives to improve Operational area development and understanding
	• Proactive • Structured • Practical • Flexible	

Table: Current Strengths of risk management systems being used

Indicative assessment of the above key benefit aspects clearly indicates that there are numerous aspects that need to be incorporated into an integrated, proactive approach to truly add value. There were a few negative responses and non-responses which potentially indicate that there are gaps and issues with regards to an understanding the benefits of a system each organisation may or may not be applying.

Core finding – key benefits and features of a robust risk management system have a broad range but hinge on aspects such CEO and board experience as well as regular review and updates

3.15. Question 15

In your company, what are the three main areas of risk management that need to be developed or improved upon?

This question allowed respondents to provide a list of their own subjective replies. There were twelve respondents who contributed and put forth what they qualify or deem as an area or areas of risk management that need to be developed or improved upon.

Numerous 'areas', with a cap of three per respondent, were listed as set out below (N = 12) and divided into three categories for ease of reference.

Cost based & direct process Related	**User friendliness**	**Outcomes & Related**
Better internal communication and understanding required on risk management, strategic risk and mitigation strategies/changes (3)	The system needs to be further extended to all risks, non-technical as well as technical (2)	More proactive approach to risk management required, as cash position permit
More regular reviews of risk matrix and mitigation action plan (2)	It is a compliance task and not adding value	Political risk - how to effectively engage with Government without becoming a nuisance
Risk mitigation related to market conditions	Ease of use of risk management IT system (3)	The risk of not including a previously disadvantaged group in the shareholding of the organization and its implications
Financial Risk (2)	Desire to break risks down into individual events	Liability
To do it properly would be expensive	The risk management system with needs to be flexible enough to deal effectively with different types of risk e.g. safety 'events' through to slow burning risks that often result in directional deterioration rather than a specific event	Business Continuation
Poor reporting capabilities of IT risk management system		In country risk Travel risk (2)
Cash flow risk		People

Table: Current areas of weakness of risk management systems being used

Based on the input to this question it is clear that there is much room for improvement modification and adjustment. This improvement is diverse and creates the opportunity to assess potential for collaboration to address some of the weaknesses identified in this point.

Core finding – based on respondent feedback there are numerous areas for improvement and enhancement of risk management that need to be addressed.

3.16. Question 16

In terms of capital and fund raising please rate the following:

Capital and fund raising	Strongly disagree	Disagree	Agree	Strongly agree	Sample Size
Effective risk management is a critical requirement for raising funds	5.56% (1)	16.67% (3)	50% (9)	27.78% (5)	18
The way I present my risk register and associated action plan is important for investors	11.11% (2)	22.22% (4)	44.44% (8)	22.22% (4)	18
De-risking my project needs to be a priority to attract investment	5.56% (1)	5.56% (1)	38.89% (7)	50% (9)	18
Being able to speak about an approach to risk management makes us a more attractive investment opportunity as a result of demonstrating an improved capacity to manage risk	5.88% (1)	5.88% (1)	52.94% (9)	35.29% (6)	17

Table: Capital and fund raising

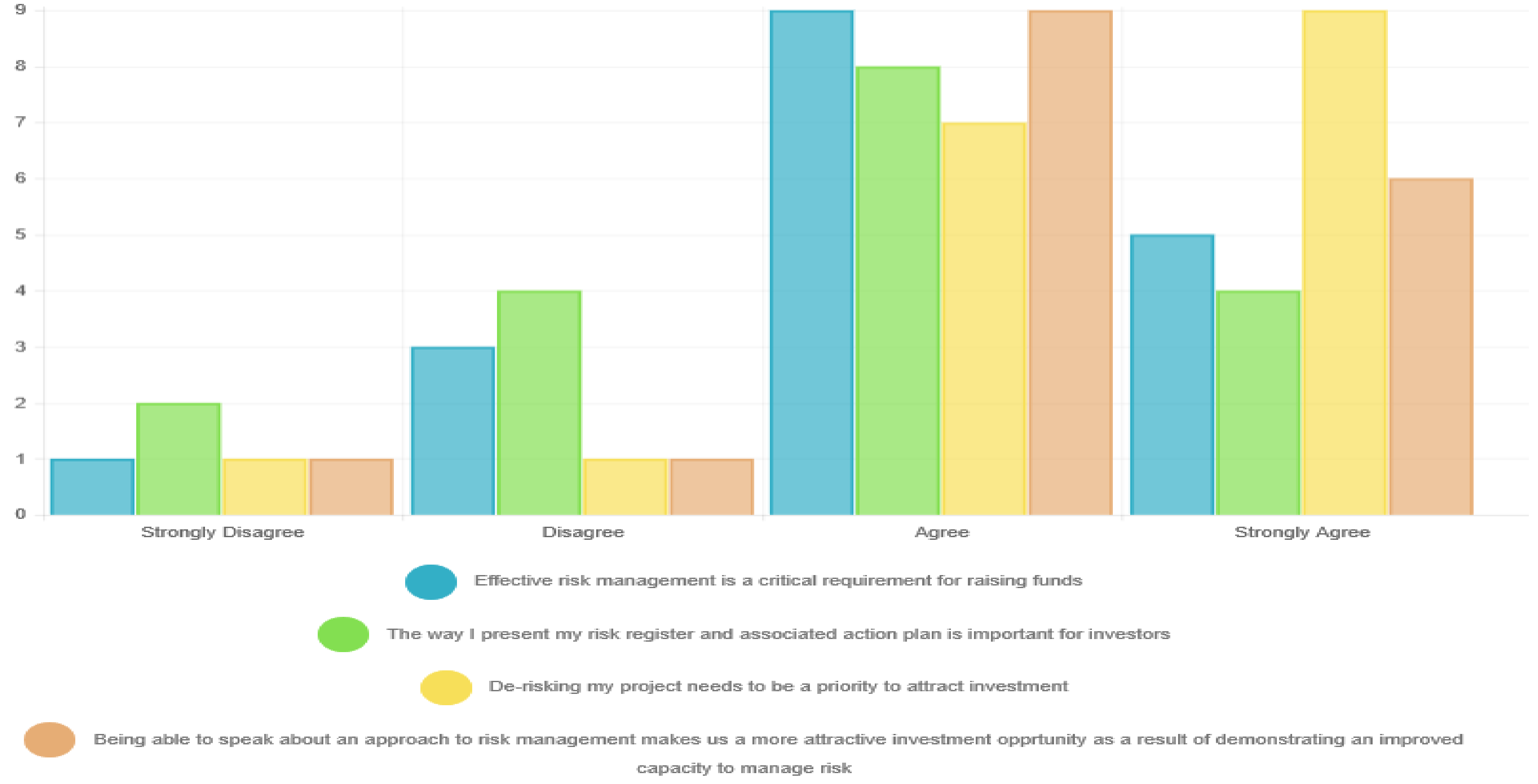

Figure: Capital and fund raising

The core outcome of this question was designed to assess the importance that respondents placed on risk as related to raising funds in the market. There is a clear confirmation that robust approach to risk management appears to be an important aspect of raising funds and accessing capital. Aspects such as up to date risk registers and whether or not risk management is a critical component of capital raising had between 20% and 30% of respondents stating that they did not think they were important aspects.

Core finding – based on respondent feedback it would appear that respondents agree with the need to have robust risk management systems in place to attract investors and capital.

3.17. Question 17

What are your biggest frustrations with the realities of risk management, compliance and related issues such as safety, security and emergency response?

This question allowed respondents to provide their own subjective replies. A number of contributions have been made.

Responses received in reference to the biggest frustrations with the realities of risk management, compliance and related issues such as safety, security and emergency response are listed below.

- Cultural and language barriers
- Time taken to report, investigate and act on incidents, then establish mitigation measures and communicate changes takes time that could otherwise be spent on technical matters
- Open reporting, knowledge of local customs and practises
- Most of the time the risk is overstated and thus the risk mitigation measures can become unrealistic and actions as a result are not always implemented
- No allocated resources to manage these aspects
- Too many issues
- Having everyone treat it seriously
- The biggest frustration is moving to a Safety and Health approach - hazard and event driven. This does not cater for Strategic Alignment. This approach is driven by an ease to understand rather than tackling a more difficult holistic approach
- Unpredictable West African Government
- None
- Failure amongst some and management to realise that a good risk analysis and planning is worth the time spent on it (2)

It is clear from the above points that the issues that cause frustration are both internal and external. There is also a consistent theme around culture and influencing behaviour which are crucial to successful risk solution implementations, some comments highlight the complexity and breadth of the risk management requirement which further adds to frustration.

Core finding – There are numerous frustrations that reflect both internal and external realities including culture, behaviour and political issues.

3.18. Question 18

Is there any professional training method used to facilitate knowledge improvement on risk? (Optional) If so please provide a brief description.

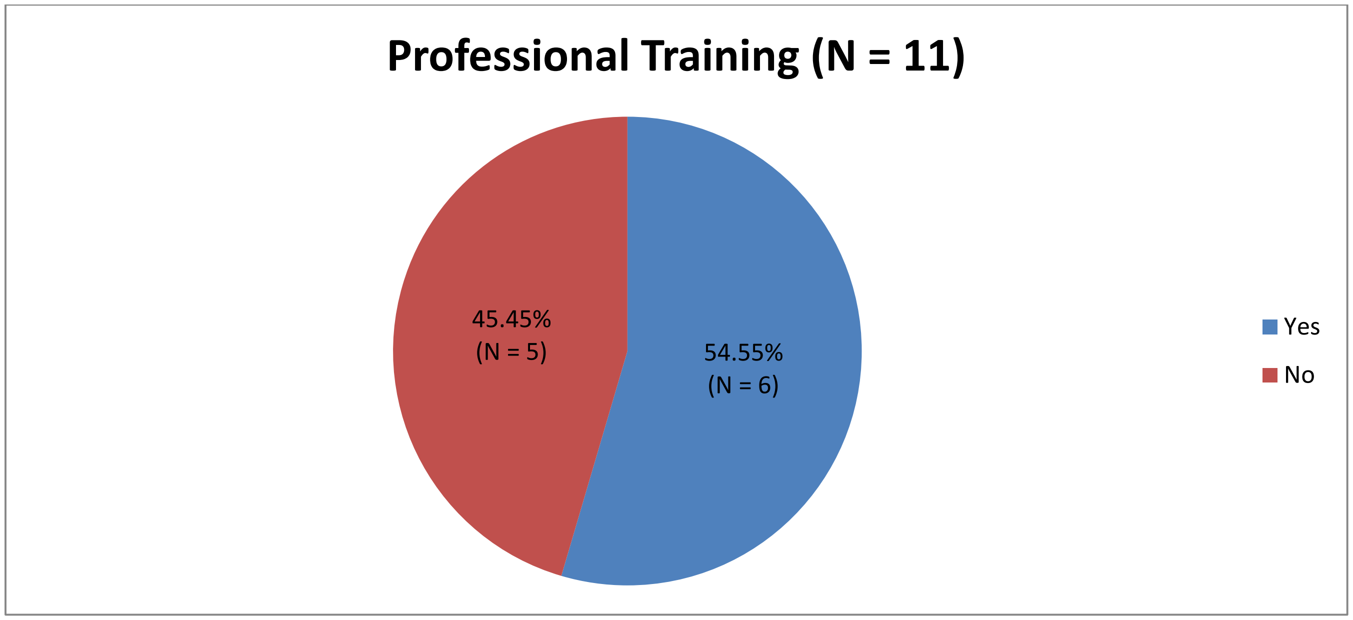

Figure: Professional Training

54.55% of the respondents indicated that a professional training method/s is used to facilitate knowledge development in reference to risk, which brings to the fore a sense of proactive thinking, learning and approach with industry experts. However it also shows that 45.44% do not engage external expertise and are not developing themselves and/or their staff in this area.

Core finding – as an indicative sample just over half of the respondents are utilising professional training and development expertise to upskill themselves and their staff in the field of risk management.

3.19. Question 19

Please indicate the proportion of time spent on risk management activities in your organisation?

Time spent	**0 - 20% of time**	**20% - 40% of time**	**40% - 60% of time**	**60% - 80% of time**	**Sample size**
Before an incident/ event	50% (9)	33.33% (6)	0	16.67% (3)	18
During the course of an incident/event	35.29% (6)	23.53% (4)	17.65% (3)	23.53% (4)	17
After an incident/ event	41.18% (7)	29.41% (5)	17.65% (3)	11.76% (2)	17

Table: Time spent

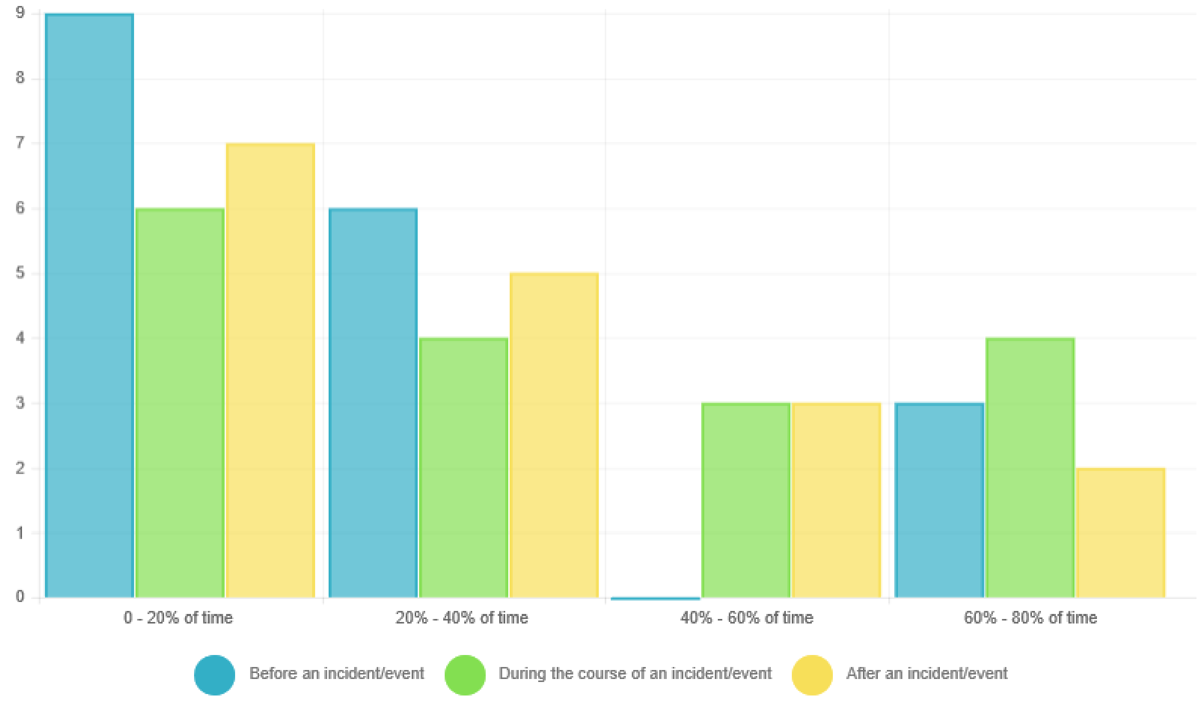

Figure: Time spent

It is important to allocate the use of limited resources such as time very effectively. Ideally the majority of time should be allocated to activities focused on identifying and mitigating potential incidents or threat situations. The feedback shows this but in a limited manner which illustrates the opportunity to better allocate time spend on risk activities i.e. if more time if out in beforehand there should be less of requirement for the during and after allocations.

Core finding – Time spend on risk activities is a critical consideration and based on respondent's feedback there is potential to better apply time spend in a proactive manner.

4. CONCLUSION

In the past risk managers were largely marginalised in their organisations, as risk and in particular hard risk, have previously been identified as low level grudge spend areas. Globalisation, compliance, legislation and media reach have now made the previous reactive approach obsolete. A reactive risk ignorant approach is bad for business on many levels and fortunately is no longer the norm and the opposite is materialising. It is becoming common sight to see more risk managers being tasked with demonstrating how they can safeguard organisations and impact bottom-line performance on a strategic level and/or corporate officeholders educating themselves to make better decisions in these fields. From the data collected it can be seen that risk management conversations, processes and practices are continuing to advance into the mainstream of business life. However, some have not progressed beyond viewing risk management as a compliance necessity and a cost of doing business. In order to create a more tangible link between risk management and the strategic growth of an organisation, more companies need to consider the concept as an important management function.

End Report.