Edith Cowan University

From the SelectedWorks of David J Brooks Dr.

April, 2008

The Development and Presentation of Psychometric Concept Maps within the Knowledge Domain of Security Risk Management

David J Brooks, Dr.

Available at: https://works.bepress.com/david_brooks/52/
The Development and Presentation of Psychometric Concept Maps within the Knowledge Domain of Security Risk Management

David Jonathan Brooks

This thesis is presented for the degree of Doctor of Philosophy of Curtin University of Technology

May 2008
DECLARATION

This thesis contains no material which has been accepted for the award of any other degree or diploma in any university. To the best of my knowledge and belief, this thesis contains no material previously published by any other person except where due acknowledgement has been made.

Signature: 

Date: May 2008
ABSTRACT

The purpose of this interpretive four-phase study was to develop and apply a technique of multidimensional scaling (MDS) to present psychometric concept maps within the knowledge domain of security risk management. The first phase defined the knowledge categories and subordinate concepts of security. Phase two developed and presented the psychometric MDS concept map, with expert validation in phase three. Phase four considered the appropriateness of MDS to develop and present consensual concept maps.

The study’s psychometric MDS security risk management concept map presented the expert knowledge structure of security risk management. The psychometric concept map demonstrated the inclusive and spatial locality of significant security risk management concepts, conceptual complexity of this domain and the central aspect of threat. In addition, the psychometric MDS concept mapping technique proved to be appropriate for developing, constructing and presenting consensual concept maps. This outcome was consistent with similar reported psychometric concept mapping studies. However unlike these reported studies, the Delphi process was integral in the development of the study’s propositional linkages, importance in effective knowledge transfer.

The study outcomes presented 14 security knowledge categories and the psychometric MDS concept map of security risk management. In addition, the appropriateness of the psychometric MDS concept mapping technique was demonstrated. The development and presentation of both the security knowledge categories and the psychometric MDS security risk management concept map may aid, in part, the consensual development of a security body of knowledge. Also, security experts’ consensual understanding of security risk management may allow improved teaching and learning within this knowledge domain. Finally, the psychometric MDS concept mapping technique may have many benefits within teaching and learning, augmenting our understanding and transfer of implicit knowledge structure.
ACKNOWLEDGEMENTS

To my principal supervisor, Professor David Treagust, who provided critical, constant and most timely support throughout the study. It took us 6-months to gain an understanding of what we were trying to achieve from this study; however, once we had consensus, the rest was relatively painless. Thank you for your advice, guidance and thorough support.

My associate supervisor, academic mentor and friend, Professor Clifton Smith, who has provided guidance and support from my undergraduate study to this thesis. Thank you.

The security industry practitioners who assisted and supported me in this study. Their support, willingness and interest, in what many may have considered quite abstract work, proved a great motivator in being able to complete this study.

The security researchers and academics, who for many years have worked in an obscure field of study and which is now just becoming recognised. Thank you for giving me the opportunity to build on your previous work, and in some small part, further the science of security.

Finally, my wife and love, Glenda, who has for many years lost me to my research. This thesis is forever hers, as it is mine.
CONTENTS

ABSTRACT .................................................................................................................. iii
ACKNOWLEDGEMENT ............................................................................................... iv
CONTENTS ................................................................................................................... v
LIST OF TABLES ........................................................................................................... x
LIST OF FIGURES ........................................................................................................ xi
PUBLICATIONS AND CONFERENCE PRESENTATIONS ............................................ xii

CHAPTER 1: INTRODUCTION ....................................................................................... 1
  1.1 Introduction ........................................................................................................... 1
  1.2 Background of the study ...................................................................................... 1
  1.3 Significance of the problem .................................................................................. 2
    1.3.1 Security ......................................................................................................... 2
    1.3.2 Concept mapping .......................................................................................... 3
  1.4 Purpose of study .................................................................................................... 5
  1.5 Research questions .............................................................................................. 7
  1.6 Methodology of the study .................................................................................... 8
  1.7 Outline of the thesis ............................................................................................ 10
  1.8 Conclusion ........................................................................................................... 12

CHAPTER 2: REVIEW OF LITERATURE ..................................................................... 13
  2.1 Introduction ........................................................................................................... 13
  2.2 Knowledge categorisation .................................................................................... 13
    2.2.1 Working memory .......................................................................................... 14
    2.2.2 Memory process ........................................................................................... 15
    2.2.3 Long-term memory ....................................................................................... 17
    2.2.4 Knowledge categorisation ............................................................................ 18
    2.2.5 Knowledge ................................................................................................... 22
    2.2.6 Expert knowledge structure ......................................................................... 23
    2.2.7 Becoming a domain expert ......................................................................... 25
    2.2.8 Knowledge categorisation conclusion ......................................................... 26
  2.3 Concept mapping .................................................................................................. 26
    2.3.1 Types of concept maps .................................................................................. 29
    2.3.2 Propositional linkages ................................................................................... 31
    2.3.3 Modelling concept maps .............................................................................. 32
      2.3.3.1 Multiple-choice questionnaire technique ............................................. 33
      2.3.3.2 Interview technique ............................................................................... 33
      2.3.3.3 Psychometric analysis technique ......................................................... 34
    2.3.4 Concept maps in teaching and learning ....................................................... 36
    2.3.5 Concept mapping limitations ....................................................................... 39
    2.3.6 Concept mapping conclusion ....................................................................... 43
  2.4 Security ................................................................................................................ 45
    2.4.1 Defining security ........................................................................................... 46
    2.4.2 Security knowledge structure ....................................................................... 48
    2.4.3 Security education ......................................................................................... 55
    2.4.4 Security associations .................................................................................... 58
2.4.5 Security conclusion .................................................. 60
2.6 Concluding the review of literature .................................. 62

CHAPTER 3: MATERIAL AND METHOD ............................... 63
3.1 Introduction .................................................................... 63
3.2 Study design ................................................................... 64
  3.2.1 Phase one: Knowledge categorisation ............................ 65
  3.2.2 Phase two: MDS knowledge structure ........................... 65
  3.2.3 Phase three: Expert knowledge structure validation .......... 66
  3.2.4 Phase four: Expert validation of the MDS concept map ...... 66
  3.2.5 Two-staged study: Pilot study ..................................... 67
3.3 Population ...................................................................... 67
3.4 Instruments .................................................................... 69
  3.4.1 Research instrument 1: MDS concept mapping survey ...... 69
  3.4.2 Research instrument 2: Expert knowledge structure validation 70
3.5 Research methodology ................................................... 71
  3.5.1 Multidimensional scaling ............................................ 71
  3.5.2 Interviews .............................................................. 74
3.6 Study limitations ........................................................... 77
3.7 Ethics ........................................................................... 78
3.8 Conclusion ..................................................................... 79

CHAPTER 4: PILOT STUDY .................................................. 81
4.1 Introduction .................................................................... 81
4.2 Pilot study: Phase one Knowledge categorisation ................... 81
4.3 Pilot study: Phase two MDS knowledge structure ................. 82
4.4 Pilot study: Phase three Expert knowledge structure validation .... 88
  4.4.1 Assertion 1 .............................................................. 88
  4.4.2 Assertion 2 .............................................................. 92
  4.4.3 Assertion 3 .............................................................. 94
  4.4.4 Assertion 4 .............................................................. 95
  4.4.5 Phase 3: Assertion conclusion ..................................... 96
4.5 Pilot study: Phase four Expert validation of the MDS concept map .... 98
  4.5.1 Assertion 1 .............................................................. 98
  4.5.2 Assertion 2 .............................................................. 100
4.6 Pilot study: Reliability and validity .................................... 103
4.7 Study modifications ....................................................... 104
4.8 Pilot study limitations .................................................... 106
4.9 Conclusion ..................................................................... 107

CHAPTER 5: PHASE ONE - SECURITY KNOWLEDGE
CATEGORISATION ......................................................... 109
5.1 Introduction .................................................................... 109
5.2 Investigation and critique of national and international tertiary courses 109
  5.2.1 Critiqued institutions and awards ................................. 111
    5.2.1.1 Edith Cowan University, Australia ......................... 111
    5.2.1.2 University of Portsmouth, United Kingdom .......... 112
7.7 Assertion 4: The map did not effectively represent concept linkage ..... 155
  7.7.1 Propositional concept links ........................................ 156
  7.7.2 Propositional informing labels ..................................... 157
  7.7.3 Assertion 4 conclusion .............................................. 158
7.8 Conclusion ............................................................................. 159

CHAPTER 8: PHASE FOUR – EXPERT VALIDATION OF THE
PSYCHOMETRIC MDS CONCEPT MAP .............................................. 162
  8.1 Introduction .......................................................................... 162
  8.2 Assertion 1: The concept map presented a valid knowledge structure .. 162
    8.2.1 Concept map structure ................................................ 163
    8.2.2 Category complexity ................................................... 164
    8.2.3 Propositional linkages ................................................. 166
    8.2.4 Assertion one conclusion ............................................. 166
  8.3 Assertion 2: MDS can be used to develop and structure concept maps .. 166
    8.3.1 MDS presented suitable knowledge structure .................. 167
    8.3.2 Closer concepts indicated stronger relationships ............. 168
    8.3.3 MDS presented conceptual relationships ....................... 169
    8.3.4 MDS mapping methodology ........................................ 172
    8.3.5 Assertion two conclusion ........................................... 174
  8.4 Reliability and validity .................................................... 174
    8.4.1 Reliability ............................................................... 175
    8.4.2 Validity ................................................................. 176
    8.4.3 Reliability and validity conclusion ................................. 177
  8.5 Security risk management concept map .................................. 178
  8.6 Conclusion ............................................................................. 178

CHAPTER 9: CONCLUSIONS, RECOMMENDATIONS & LIMITATIONS 181
  9.1 Introduction .......................................................................... 181
  9.2 Summary of the study and conclusions .................................. 181
    9.2.1 Phase one: Knowledge categorisation ............................ 182
    9.2.2 Phase two: MDS knowledge structure mapping .............. 182
    9.2.3 Phase three: Expert knowledge structure validation ........ 183
    9.2.4 Phase four: Expert validation of the MDS concept map .... 184
  9.3 Recommendations .......................................................... 185
    9.3.1 Benefits of the security risk management concept map ..... 186
    9.3.2 Future research .......................................................... 188
      9.3.2.1 Methodology of MDS concept mapping .................... 188
      9.3.2.2 Propositional linkages .......................................... 189
      9.3.2.3 MDS mapping strength of relationship and clustering 190
      9.3.2.4 Reliability .......................................................... 191
  9.4 Limitations .......................................................................... 191
    9.4.1 Defining security ....................................................... 191
    9.4.2 Course critique and data extraction .............................. 192
    9.4.3 Sample size and nature ............................................... 192
    9.4.4 Cognitive knowledge structuring .................................. 193
    9.4.5 Reliability and validity of MDS knowledge mapping ..... 193
**LIST OF TABLES**

<table>
<thead>
<tr>
<th>Table 1.1</th>
<th>Research questions and related phases of study</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 2.1</td>
<td>Degree of directedness in concept map evaluation</td>
<td>33</td>
</tr>
<tr>
<td>Table 2.2</td>
<td>ASIS Common knowledge categories of security model</td>
<td>51</td>
</tr>
<tr>
<td>Table 2.3</td>
<td>ASIS Revised common knowledge categories of security model</td>
<td>51</td>
</tr>
<tr>
<td>Table 2.4</td>
<td>Security knowledge categories</td>
<td>52</td>
</tr>
<tr>
<td>Table 2.5</td>
<td>Active Australian security associations</td>
<td>58</td>
</tr>
<tr>
<td>Table 4.1</td>
<td>Security and allied industry related West Australian courses</td>
<td>81</td>
</tr>
<tr>
<td>Table 4.2</td>
<td>Pilot study: Phase one security risk management category and subordinate concepts</td>
<td>82</td>
</tr>
<tr>
<td>Table 4.3</td>
<td>Pilot study: Phase two security risk management category and subordinate concepts</td>
<td>83</td>
</tr>
<tr>
<td>Table 4.4</td>
<td>Pilot study: Predefined survey questions</td>
<td>83</td>
</tr>
<tr>
<td>Table 4.5</td>
<td>Pilot study: Phase two revised survey format</td>
<td>84</td>
</tr>
<tr>
<td>Table 4.6</td>
<td>Pilot study: Pearson two tailed correlation</td>
<td>85</td>
</tr>
<tr>
<td>Table 4.7</td>
<td>Pilot study: Utilisation of concept terms by David and Andrew during the expert interviews</td>
<td>90</td>
</tr>
<tr>
<td>Table 5.1</td>
<td>Location and number of security related courses</td>
<td>110</td>
</tr>
<tr>
<td>Table 5.2</td>
<td>Critiqued security courses</td>
<td>111</td>
</tr>
<tr>
<td>Table 5.3</td>
<td>Concepts count extracted from course units of study titles</td>
<td>115</td>
</tr>
<tr>
<td>Table 5.4</td>
<td>Security knowledge categories</td>
<td>116</td>
</tr>
<tr>
<td>Table 5.5</td>
<td>Initial security risk management category and supporting concept frequency count</td>
<td>121</td>
</tr>
<tr>
<td>Table 5.6</td>
<td>Security risk management category and supporting concepts for expert validation</td>
<td>122</td>
</tr>
<tr>
<td>Table 5.7</td>
<td>Security risk management category and supporting concept</td>
<td>124</td>
</tr>
<tr>
<td>Table 6.1</td>
<td>Common expert propositional linkages</td>
<td>131</td>
</tr>
<tr>
<td>Table 6.2</td>
<td>Expert recommended alternative propositional labels that were adopted</td>
<td>133</td>
</tr>
<tr>
<td>Table 7.1</td>
<td>Phase three: Expert interview questions</td>
<td>139</td>
</tr>
<tr>
<td>Table 7.2</td>
<td>Phase three: Expert interview – assertion relationship to questions</td>
<td>140</td>
</tr>
<tr>
<td>Table 7.3</td>
<td>Phase three: The six expert’s profiles</td>
<td>140</td>
</tr>
<tr>
<td>Table 7.4</td>
<td>Phase three: Assertion one – expert comments</td>
<td>145</td>
</tr>
<tr>
<td>Table 7.5</td>
<td>Phase three: Assertion two – expert comments</td>
<td>151</td>
</tr>
<tr>
<td>Table 8.1</td>
<td>Phase four: Expert evidence in support of assertion 1</td>
<td>163</td>
</tr>
<tr>
<td>Table 8.2</td>
<td>Phase four: Expert evidence in support of assertion 2</td>
<td>167</td>
</tr>
</tbody>
</table>
LIST OF FIGURES

Figure 1.1 Four phases of the study .................................................. 9
Figure 2.1 Multi-store memory model ................................................ 15
Figure 2.2 Taxonomy of long-term memory ....................................... 17
Figure 2.3 Conceptual categories hierarchies .................................... 22
Figure 2.4 Hierarchical nature of knowledge ...................................... 24
Figure 2.5 Concept map of concept mapping ..................................... 29
Figure 2.6 Types of concept maps ..................................................... 30
Figure 2.7 Integrated security standards framework model ..................... 53
Figure 4.1 Pilot study: MDS knowledge structure of security risk management 86
Figure 4.2 Pilot study: Draft psychometric MDS security risk management concept map ...................................................... 87
Figure 4.3 Pilot study: Psychometric MDS security risk management concept map ................................................................. 102
Figure 5.1 Phase one: Security risk management concept extraction methodology ................................................................. 120
Figure 6.1 Phase two: Psychometric MDS concept mapping methodology .... 126
Figure 6.2 Psychometric MDS security risk management knowledge structure 129
Figure 6.3 Psychometric MDS concept knowledge structure ready for propositional linkage insertion ........................................... 130
Figure 6.4 Initial psychometric MDS security risk management concept map .. 132
Figure 6.5 Psychometric MDS security risk management concept map ........ 134
Figure 7.1 Individual experts additional recommended propositional linkages .. 157
Figure 9.1 Propositional ranking ......................................................... 190
PUBLICATIONS AND CONFERENCE PRESENTATIONS

There were a number of publications and conference presentations that resulted from the research undertaken in this thesis. A list of publications and conference proceedings are presented, including the publication’s abstracts.

Publications

This article’s content is presented, in part, within Chapters 2, 4 and 5.

Abstract
Private security is a multi-disciplined industry, requiring a diverse range of knowledge across many domains. Additionally and perhaps due to the diversity of private security, security has not been effectively defined. Security has many meanings dependant on applied context and concept definition. But security is developing into a discipline that does contain a rich knowledge structure, demonstrated to a degree through the increasing educational offerings of security at the tertiary level. Therefore, if security has not been appropriately defined can a security body of knowledge be presented?

The study critiqued international tertiary security courses (n=104) to consider what may define a security body of knowledge. Security experts selected international tertiary security courses (n=7) to provide source data for content analysis. From these selected security courses a table of security concepts (n=2001) were extracted, resulting in a final knowledge categorisation (n=13) of private security. Security knowledge categories included; criminology, business continuity management, facility management, fire science, industrial security, information and computer security, investigations, physical security, security principles, risk management, security law, security management and security technology. In addition, these security categories were integrated into previous
work to propose the Science of Security Framework. The development and presentation of the security knowledge categories and security framework will aid, in part, the consensual development of a security body of knowledge.


This article’s content is presented, in part, within Chapters 2 and 5.

**Abstract**

Security education at the tertiary level is still in its infancy, with limited consensual agreement on content requirement. The security industry is diverse and multi-disciplined, with practitioners originating from many disciplines. But security experts have a rich knowledge structure, although there has had limited research to map this knowledge structure. This limited mapping reduces the ability of tertiary educators to provide industry focused teaching and learning.

The study investigated and critiqued international tertiary undergraduate security courses (n=104). Supported by both industrial and academic security experts, further analysis reduced the number of courses for content analysis (n=7). Course content was analysed and security concepts extracted. Concept extraction utilised Linguistic Inquiry and Word Count (LIWC) text and content analysis. Linguistic analysis categorised the more utilised security concepts, supported by subordinate concepts.

The study presented a number of significant findings. According to the study, a large majority of the critiqued security courses did not effectively represent organisational or corporate security. A table of security categories (n=14) was presented and included security technology. The study appeared to indicate that security education should include all fourteen knowledge categories. A list of subordinate security concepts
(n=2001) was also produced, with security technology (n=226) presenting primary technologies.


This article’s content was developed from Chapters 2 and 7; however, restricted content from this article was included in this thesis.

**Abstract**

AS/NZS4360:2004 suggests that the risk assessment process should not be conducted or information gathered in isolation. This insular method of data collection may lead to inaccurate risk assessment, as stakeholders with vested interests may emphasise their own risks or game the risk assessment process. The study demonstrated how a consensual risk assessment approach may result in a more acceptable risk assessment outcome when compared to individual assessments.

The participants were senior managers at a West Australian motel located on the West Coast Highway, Scarborough. The motel consists of four three storey blocks of units, resulting in a total of 75 units. The three main areas of the business are Reception and Management, Housekeeping and Maintenance. The participants were interviewed individually and then as a group.

Two activities took place in the study, an individual identification and analysis of risks affecting the facility, followed by a consensual group analysis of the same risks. The individual risk assessment results were collated and compared to the results of the consensus group. This demonstrated that individuals over or under emphasise some risks, dependant on personal affect. The study illustrated that a consensual style of risk
information collection and assessment was more acceptable to the group then assessments conducted in isolation.


This article’s content is presented, in part, within Chapters 4 and 5.

**Abstract**

The security industry comprises diverse and multi-disciplined practitioners, originating from many disciplines. It has been suggested that the industry has an undefined knowledge structure, although security experts contain a rich knowledge structure. There has also been limited research mapping security expert knowledge structure, reducing the ability of tertiary educators to provide industry focused teaching and learning. The study utilized multidimensional scaling (MDS) and expert interviews to map the consensual knowledge structure of security experts in their understanding of security risk. Security risk concepts were extracted and critiqued from West Australian university courses. Linguistic analysis categorised the more utilized security risk concepts. MDS tested these concepts and presented a spatial knowledge structure (STRESS1=0.35, a=0.64), further tested and validated by security experts (n=30).

The study presented a number of significant findings. A table of security categories, with supporting subordinate concepts was presented. The security risk consensual knowledge map suggested that the concept threat occupied a central theme for security experts. Spatial location of security risk concepts provided an indication of conceptual relationships. Finally, the sequential structure and concept clusters provided an indication of security expert conceptual decision making.
Security is a diverse and multi-disciplined industry, which requires a breadth of knowledge originating from many disciplines. Security does not contain a clear definition, perhaps due to this diversity and inter-disciplinary function. Also, it has been suggested that the industry has an undefined knowledge structure, although security experts do contain a rich knowledge structure. There has been research attempting to define a security body of knowledge, but with limited agreed consensus.

The study utilised cognitive psychology exemplar view to inform the study in knowledge categorisation. A part of a larger study is presented within the paper, being the knowledge categorisation of security. International tertiary security courses (n=104) provided the source data, with final courses (n=7) selected for content analysis. Linguistic Inquiry and Word Count provided text and content analysis of the security courses, resulting in the concept extraction of each critiqued course. Linguistic analysis categorised the more utilised security concepts into security knowledge categories.

The study presented a number of significant findings. A table of security knowledge categories (n=14), with supporting subordinate concepts (n=2001) was presented. Security knowledge categories included; criminology, emergency/contingency planning, facility management, fire science, industrial security, information and computer security, investigations, physical security, security principles, risk management, security law, security management, security technology and threats. Finally, the development and presentation of the security knowledge categories aids the consensual development of the security body of knowledge.
Conference Presentations


CHAPTER 1
INTRODUCTION

1.1 Introduction
The study addressed a technique to present a consensual expert knowledge structure of security using psychometric concept mapping. Concept mapping and multidimensional scaling (MDS) were integrated to form a psychometric technique to develop and represent a consensual knowledge structure. The study applied this psychometric technique within the domain of security using the knowledge category of security risk management. There has been restricted research in both the utilisation of MDS to develop and represent concept maps, and in the presentation of security risk management expert knowledge structure.

1.2 Background of the study
World exposure to terrorist attacks in Glasgow (2007), London (2007; 2006; 2005), Jakarta (2004), Russia (2004), Iraq (2007-2004), Spain (2004), Bali (2002) and New York (2001) has raised social concern over the ability of governments to protection its citizens. An address by Prime Minister John Howard on Australian national security stated that the Bali attacks had touched all Australians and that the financial impact of the 11th September 2001 cost the United States 0.75 percent of US GDP or US$75 billion (Howard, 2004). Australian Attorney-General Philip Ruddock stated that A$8 billion had been expended on direct security-related measures since 2001 (2007). In Europe, a billion Euro coherent strategy was being developed to coordinate military and civilian research in security-related projects (Horvath, 2004). These issues have raised both national and international requirement for tertiary trained security practitioners (School of Engineering and Mathematics, 2004a).

In the United States there are 10,000 security companies employing 1.8 million guards, equating to almost three private security officers to every public officer and this ratio is expected to increase (Hemmens, Maahs, Scarborough & Collins, 2001). Cities in the United States were spending US$70 million per week on security services (Fischer &
Green, 2004). In Australia it was estimated that the security industry is valued at over A$4.3billion, which is expected to grow over the next decade (McKeague, 2006). However, the security industry is an emerging and relatively young discipline (Fischer & Green, 2004; Tate, 1997) and the traditional distinction between past security entities of public police, private security and defence are merging (Ferguson, 2004; Morley & Vogel, 1993). The expansive nature of security has resulted in limited and diffuse understanding, even though extensive resources are being expended.

1.3 Significance of the problem
The study considered two research problems: the knowledge structure of security and the utilisation of a psychometric MDS concept mapping technique to present consensual knowledge structure. The resolution to each problem aided the other, resulting in a number of significant outcomes.

1.3.1 Security
Security is “assured freedom from … want, precautions taken to ensure against theft or a person or thing that secures or guarantees” (The Angus & Roberston, 1992, p. 903). According to Fischer and Green “security implies a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of such disturbance or injury” (2004, p. 21). Security has to also be expanded to consider national security and the defence of a nation, as well as public policing. Still others may consider security as crime prevention, security technology, risk management or loss prevention (Brooks, 2006). Moreover security may not necessarily be restricted to the law-abiding, directed towards crime or for the good (Manunta, 1999). A traditional definition of security is the provision of private services in the protection of people, information and assets for individual safety or community wellness (Craighead, 2003) in preventing undesirable, unauthorised or detrimental loss of organisational assets (Post & Kingsbury, 1991).

Security may present different meaning to different people, given time, place and context. It has been proposed that security has to have a shared definition among many
disciplines, and that gaining definition is both essential and urgent (Manunta, 1999). However, current international security has shifted into an ambiguous arena (Horvath, 2004). Variance results in a society that has no clear understanding of what security is, nevertheless, with a divergence of stakeholder interest (Manunta, 1999). This is a view proposed by Fischer and Green, when they stated that “there is no universal agreement on a definition or even on the suitability of the term [security]” (2004, p. 37). It has been argued that security lacks definition (Tate, 1997) and therefore lacks structured knowledge, although this lack of definition should not conclude that security does not contain a definable knowledge structure. These diffuse views result in a society that has no clear understanding of security.

There has been a demand for appropriate security education since the 1950’s (Fischer & Green, 2004), although within Australia there is limited occupational classification, no single national association, limited career structure, fragmented education and no independent academic discipline (Tate, 1997). Nevertheless security education has an excellent future considering the indicated growth (Fischer & Green, 2004), although according to Manunta (1999) academia is content to continue to discuss security without definition. Without a concise understanding of security, how can educators develop appropriate programs and curriculum in security education? Within the context of the study, security was considered to be the provision of private services to protect people, information and asset – namely organisational security.

1.3.2 Concept mapping

Concept maps represent knowledge structure (Markham, Mintzes & Jones, 1994) and may be used to display concept understanding and reach consensus (Eysenck & Keane, 2002; Novak, 1990; Novak, 1998). Concept maps are spatial maps that exhibit hierarchically structured knowledge through the construction of n concepts that have propositional linkages and statements to provide meaning (Bennett & Rolheiser, 2001). Experts will have a robust understanding of conceptual knowledge within their domain (Novak & Gowin, 1984), which may be presented as a concept map.
The use of MDS to develop psychometric concept maps first appeared in the late 1980’s (Trochim, 1989a; 2005b), although this procedure only considered knowledge clustering and contradicted Novak’s (1990) view of concept mapping. During this period, Markham, et al. (1994) used MDS to test the validity of concept mapping, with consideration of Novak’s (1990) previous work. Markham, et al. (1994) demonstrated that concept mapping provided a theoretically valid and powerful tool, and that MDS provided an appropriate statistical technique to define concept maps. Markham’s view was validated by further MDS concept mapping studies (Ruiz-Primo, Schultz, Li & Shavelson, 2001; Streveler, Miller & Boyd, 2001), although investigative research into psychometric MDS analysis technique appears to have been limited particularly when considering Novak’s (1990) view of concept mapping.

Concept maps have been widely used in science education for many years (Hoz, Bowman & Chacham, 1997), providing an alternative approach to assist teaching and learning (Bennett & Rolheiser, 2001; Carr, 1996). Teaching and learning may benefit from concept mapping through the development and display of expert knowledge structures, assist in developing curriculum (Smith, 2003), aid novice learners in the understanding of conceptual relationships (Tunnicliffe & Reiss, 2004) and as an alternative to more traditional assessment techniques (Hoz, et al., 1997). MDS, integrated with concept mapping, can provide a research method to develop and present psychometric expert knowledge structures. Psychometric MDS concept mapping proved a suitable technique, as experts will cluster knowledge concepts within multiple dimensions (Markham, et al., 1994; Turner, 2002) providing their own knowledge structure.

There were a number of potentially significant outcomes in conducting this study, which include the:

- Advancement of the implicit understanding of organisational security.
- Presentation of a definition of organisational security within an educational context.
- Presentation of the consensual organisational security knowledge categories and subordinate concepts.
Presentation of a consensual psychometric MDS concept map of the knowledge category security risk management and subordinate concepts.

 Appropriateness of MDS to integrate with concept mapping in the development and representation of psychometric concept maps.

 Contribution of an understanding in how security experts consider security risk management.

 Allowance of future development of tertiary security education, curriculum design, and teaching and learning.

 Support of the emerging knowledge domain of security.

### 1.4 Purpose of study

There is a need to consider both the investigation of a security body of knowledge and the use of psychometric MDS concept mapping. Although distinct topics of inquiry, they were integrated to allow psychometric MDS concept mapping to be tested within an applied knowledge domain of security.

Security is to a degree an undefined term (Tate, 1997), as the security industry is broad and multi-disciplined in nature (Hesse & Smith, 2001), and occupations are heterogenous. Current international politics has further broadened the definition of security, from both a national and international perspective. It has been proposed that security requires shared meaning (Manunta, 1999), although this is capricious (ASIS International, 2003) and with no universal agreement (Fischer & Green, 2004). Nevertheless, it is proposed that security can only achieve definition through applied context and concept definition. Concept definition may to a degree be achievable through a consensual body of knowledge.

There has been restricted research in presenting a security body of knowledge, with publications primarily by ASIS (2003) and others (Brooks, 2006; Hesse & Smith, 2001; Risk Management Institute of Australasia, 2007b). These limited publications are perhaps due to the diversity of what is meant by security, which makes research activity diffuse. Although this body of knowledge has not been explicitly presented, there is
supporting literature to develop this body of knowledge. Supporting literature encompasses not only both research and industry association publications, however, also developed and appropriate organisational security tertiary degree awards. These degrees can provide security knowledge categories and supporting subordinate concepts developed by security experts, which will assist in presenting a security body of knowledge.

Experts, with domain knowledge and practice, develop a rich knowledge structure with higher implicit understanding (Kellogg, 2003) and complex schema. Concepts are structured in a hierarchical manner, allowing problems to be solved faster (Eysenck & Keane, 2002) and at a different conceptual level to novice practitioners (Chi, Feltovch & Glaser, 1981). Expertise is not automatic, achieved through structured learning and full adaptation (Ericsson & Charness, 1997). Also knowledge may be taught in a sequential manner, even through we may visual ideas or concepts (Novak & Gowin, 1984). The ability of educators to understand, define, map and represent expert knowledge is vital if teaching and learning is to be more effective. The use of concept mapping to represent rich knowledge structure (Markham, et al., 1994) can assist the teaching and learning process.

Concept maps, as discussed in preceding sections, may be used to present knowledge structure (Markham, et al., 1994), display concept understanding and reach consensus (Eysenck & Keane, 2002). However, concept maps are generally individual in development and volatile in nature (Kellogg, 2003), require interpretation and can be ambiguous (Turns, Atman & Adams, 2000). They may also be distorted or incorrect as the concept map is based on existing knowledge (Gentner & Gentner, 1983) and there are concerns regarding reliability and validity (Ruiz-Primo, et al., 2001).

Multidimensional scaling elicits underlying structure from the sum of a group, reducing complex data through presentation in dimensional space. Presentation demonstrates object proximity, with the clustering of similar concepts together and dissimilar concepts farther apart (Cox & Cox, 2000). Experts will link implicit concepts, resulting in concept
clustering of similar concepts or the representation of knowledge structure (Martinez-Torres, Garcia, Marin & Vazquez, 2005; Streveler, et al., 2001). There has been a degree of research into the use of psychometric MDS knowledge mapping, however restricted research in the psychometric concept mapping technique. MDS, when integrated with concept mapping, is considered a novel approach in developing and representing psychometric concept maps, nevertheless, this technique required further investigative research.

1.5 Research questions

Five research questions resulted in a four phase study (Table 1.1), which guided the inquiry into the psychometric development and presentation of the psychometric MDS security risk management concept map. The phases of study and related research questions are shown in Table 1.1.

Table 1.1

<table>
<thead>
<tr>
<th>Research questions and related phases of study</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phase One: Knowledge Categorisation (Discussed in Chapter 5)</strong></td>
</tr>
<tr>
<td>Research Question 1: What are the knowledge categories and subordinate concepts of security?</td>
</tr>
<tr>
<td><strong>Phase Two: MDS Knowledge Structure Mapping (Discussed in Chapter 6)</strong></td>
</tr>
<tr>
<td>Research Question 2: What is the expert knowledge structure and subordinate concepts of security risk management as measured by multidimensional scaling?</td>
</tr>
<tr>
<td><strong>Phase Three: Expert Knowledge Structure Validation (Discussed in Chapter 7)</strong></td>
</tr>
<tr>
<td>Research Question 3: What is the expert knowledge structure and subordinate concepts of security risk management as measured by interviews?</td>
</tr>
<tr>
<td><strong>Phase 4 Expert Validation of the Psychometric MDS Concept Map (Discussed in Chapter 8)</strong></td>
</tr>
<tr>
<td>Research Question 4: Can a psychometric multidimensional scaling concept map of the security risk management knowledge category and subordinate concepts be developed and represented?</td>
</tr>
<tr>
<td>Research Question 5: Is multidimensional scaling an appropriate psychometric technique to develop and represent concept maps?</td>
</tr>
</tbody>
</table>
1.6 Methodology of the study

The study was divided into four sequential, nevertheless, distinct phases (Figure 1.1). Each phase had predetermined objectives, supporting one or more research questions. Phase one Knowledge Categorisation sourced security knowledge concepts, principally international tertiary security baccalaureate degree courses offered by seven universities. These security courses allowed concepts to be extracted, categorised and tabulated, resulting in the knowledge category of security risk management. Phase two MDS Knowledge Structure Mapping psychometrically measured and presented, as a spatial psychometric concept map, 29 experts’ views of the security risk management knowledge category.

Phase three Expert Knowledge Structure Validation comprised interviews with six additional security experts to validate both the psychometric MDS security risk management concept map and the security risk management category. Finally Phase four Expert Validation of the Psychometric MDS Concept Map was designed to achieve two outcomes. The first outcome compared and contrasted the validity of the knowledge category of security risk management and the psychometric concept map. The second outcome validated, within the context of the study, the psychometric concept mapping technique in representing consensual knowledge structure.
Figure 1.1 Four phases of the study

Chapter 5

Phase One: Knowledge Categorisation

1. Review and analyse international tertiary security course structures for security concepts.
2. Extract concepts from seven defined tertiary security courses.
3. Develop and tabulate security knowledge categories through literature critique.
4. Tabulate the security risk management knowledge category with subordinate concepts through convergence.

Chapter 6

Phase Two: MDS Knowledge Structure

1. Develop, from the security risk management knowledge category and subordinate concepts, the MDS concept mapping survey instrument; namely Research Instrument No 1.
2. MDS survey thirty security experts.
3. Analyse and interpret the MDS spatial knowledge representation.
4. Present the psychometric security risk management concept map.

Chapter 7

Phase Three: Expert Knowledge Structure Validation

1. Develop Phase three assertions.
2. Interview six security experts with outcomes from Phase one and Phase two, with Research Instrument No 2.
3. Analyse and interpret expert response.

Chapter 8

Phase Four: Expert Validation of the Psychometric MDS Concept Map

1. Develop Phase four assertions.
2. Compare and contrast Phase two and Phase three outcomes.
3. Analyse and interpret results.
1.7 Outline of the thesis

The thesis is structured in a sequential manner, reflecting the study’s methodology and research questions. The following chapter, Chapter two, reviews the supporting theoretical foundation of the study, providing an analytical summary of cognitive knowledge categorisation, concept mapping and the security industry. Cognitive knowledge categorisation presents the concept of knowledge, memory, knowledge categorisation and expertise. Concept mapping considers map modelling, maps in teaching and learning, concept mapping limitations and supports the presentation of the psychometric MDS security risk management concept map. Security presents research into the conceptual definition of security, diversity and complexity of the industry, the security body of knowledge, tertiary security education and security associations.

The supporting materials and methods, considering study design, population sampling, research instruments and methodology are presented in Chapter three. The study design comprises the four phases of the study, with supporting objectives. Population sampling considers the approach in the selection of the study’s sample size, followed by the research instrument’s design and construction. The research methodology considers both MDS and interviewing techniques as methods to extract and catalogue conceptual knowledge. Chapter four presents the pilot study, which applied the four phases of the study, and resulted in pilot study outcomes. In addition, the pilot study assessed the suitability of the study and led to improvements in the primary study design.

Phase one, describing the development of the security knowledge categorisation and responding to Research Question one, is presented in Chapter five. International tertiary undergraduate security courses were investigated and critiqued. Supported by security experts, selected undergraduate courses were analysed for content and concepts were extracted and tabulated, resulting in the security risk management category. Security experts conclude Chapter five with the validation of the security risk management category concepts.
Phase two, describing the development of the psychometric MDS concept map of security risk management and responding to Research Question two, is presented in Chapter six. The security risk management category subordinate concepts were embedded into the MDS research survey instrument, which was completed by 29 security experts. MDS data analysis resulted in the presentation of the psychometric MDS knowledge structure of security risk management. Propositional linkages and supporting labels were incorporated into the knowledge structure, presenting the psychometric security risk management concept map. Finally, reliability and validity of the psychometric concept map are considered.

Phase three, describing the expert inquiry of the psychometric MDS security risk management concept map and responding to Research Question three, is presented in Chapter seven. Assertions were formed and the opinions of security experts were sourced through semi-structured interviews. Expert opinions are presented as supporting evidence to validate the four predefined assertions.

Phase four, describing the comparative inquiry between the development of the psychometric security risk management concept map (Chapter 6) and expert validation (Chapter 7), is presented in Chapter eight. Comparison allowed Research Questions four and five to be addressed, and as with the proceeding chapter, assertions were formed to respond to these research questions. Assertions consider the validity of the psychometric security risk management concept map, and the use of MDS to develop and represent consensual concept maps.

Finally, the conclusions, recommendations and limitations of the study are presented in Chapter nine. This chapter concludes the study, summarising the research questions and final study outcomes. Recommendations are considered in how the psychometric MDS security risk management concept map may increase an understanding of security risk management. Potential avenues for further study and study limitations conclude the chapter.
1.8 Conclusion
The study was designed to improve understanding in two areas. The first considers a technique to develop and represent consensual expert knowledge structure, using psychometric MDS concept mapping. The second applied the psychometric MDS concept mapping technique within the domain of security, to develop and present a psychometric security risk management concept map. Both areas have restricted research applied, however, the study outcomes may both aid teaching and learning for teachers and students. While the thesis does not provide definitive answers, in particular with the need to develop a consensual security body of knowledge, it does go some way in building on previous work and assisting those who will come in the future.
CHAPTER 2
REVIEW OF LITERATURE

2.1 Introduction
The theoretical foundation of the study is presented in this chapter by providing an analytical summary of knowledge categorisation, concept mapping and the security discipline. Knowledge categorisation (2.2) involves discussion of the concept of knowledge, cognitive memory, knowledge categorisation and expertise. Concept mapping (2.3) includes the presentation of concept maps, modelling maps, maps in teaching and learning, and limitations of concept mapping. Concept mapping supported the development and presentation of the psychometric MDS security risk management knowledge structure. Security (2.4) includes the presentation of research into the conceptual definition of security, the diversity and complexity of security, research and development of a security body of knowledge, tertiary security education and security associations. The content of the chapter is summarised with a conclusion (2.5).

2.2 Knowledge categorisation
Angus and Robertson define knowledge as “facts or experiences known by a person or group of people ... specific information about a subject” (1992, p. 557). However, according to Clancey knowledge “is more than written scientific facts and theories” (1997, p. 285). Knowledge is not discovered, on the contrary, uses and expands existing concepts (Novak & Gowin, 1984) and is “a possible state of affairs, either real or imaginary” (Eysenck & Keane, 2002, p. 533). As new knowledge is gained, change in understanding regarding existing knowledge is achieved. Knowledge is viable (Rennie & Gribble, 1999), constructed and built on previous knowledge.

Knowledge may commence with object and pattern recognition, nevertheless these do not provide an appropriate explanation within the study to define knowledge. Knowledge is integral to memory structure, which is concerned with how the memory may organise, store and retrieve knowledge. According to Atkinson and Shiffrin (1999) these processes are referred to as the multi-store memory model, which provides
memory architecture containing three types of memory storage - the sensory store, short-term memory and long-term memory.

The sensory store caches the biological sensory inputs which, depending on need, may decay within seconds or be transferred into short-term memory. Short-term memory has little capacity and fragility of storage, and Miller claimed that in terms of capacity may comprise seven plus or minus two units, with a unit comprising of numbers, letters, words (cited in Reisberg, 2001) or labels. These units may be referred to as chunks or packages of information. According to Eysenck and Keane (2002), there are significant differences between short-term memory and long-term memory, such as temporal duration, storage capacity, forgetting mechanism and the effects of brain damage. Recent research has indicated that the multi-store memory model is not only too simplistic (Kellogg, 2003) but also is in error due to the relationship between short-term memory and long-term memory, with importance placed on rehearsal and the routing of information (Eysenck & Keane, 2002; Logie, 1999).

### 2.2.1 Working memory

The failure of the multi-store memory model to fully define memory structure led “current cognitive literature” (Jonides, 1998, p. 215) to propose a replacement of the short-term memory store with working memory. Working memory (Figure 2.1) is said to have three components, such as the central executive, phonological loop and visuo-spatial sketchpad (Eysenck & Keane, 2002). The central executive is the key component, with the other two components providing input (Jonides, 1998). The phonological loop provides short-term storage for speech based information and sub-vocal articulation. A visuo-spatial sketchpad provides short-term storage for visual and spatial processing of information (Baddeley, 1999; Reisberg, 2001).
The central executive, as with long-term memory, is divided within sections of the brain. According to Baddeley (1999), the central executive’s major functions are switching of retrieval plans, timesharing dual tasks, selecting stimuli attention and activation of long-term memory. Working memory has been demonstrated to remove errors in the multi-store short-term memory. However, research has not been able to quantify the central executive capacity and full functions, therefore researchers have claimed that this still does not present a valid representation of working memory (Eysenck & Keane, 2002; Kellogg, 2003).

**2.2.2 Memory process**
Memory process may be defined as the ability of a person to retain and recall information, sensations, thoughts or knowledge over a period of time (The Angus & Robertson, 1992). The strength of memory retention and recall of a learner has been shown to depend on the depth of stimuli processing and analysis, defined as either maintenance rehearsal or elaborative rehearsal. Maintenance rehearsal may involve repeated analysis or recycling learnt information within working memory. Whereas elaborative rehearsal involves linking information in working memory with information stored in long-term memory (Kellogg, 2003). The memory process has a major impact on the ability of long-term memory to retain and retrieve, nevertheless, it has been
claimed that the level of process used by learners is difficult to assess (Eysenck & Keane, 2002).

Research into the memory process has indicated that memory retention and recall depends on interaction between memory processing during encoding and retrieval. Nevertheless, memory processing is a complex and interactive process that involves top-down and bottom-up processing (Lockhart & Craik, 1990) and that shallow processing does not always present limited memory retention and therefore retrieval. The ability of the memory to retain or forget knowledge has been shown to display a linear logarithmic loss function, although the exception appears to be motor skills and autobiographical memory (Jonides, 1998).

Recognition and recall comprise a two-theory approach; recall is involved in a search process followed by recognition. The two-theory approach has been shown to be in error as this would make recognition more effective than recall, which is often not the case. If effective recall can search and retrieve, recognition should not fail (Eysenck & Keane, 2002). However, the encoding specifically principle argued that a “greater amount of informational overlap is required for successful recall than for successful recognition. The reason is that recall involves naming a previous event, whereas recognition involves only a judgement of familiarity” (Eysenck & Keane, 2002, p. 176). Nevertheless, as memory appears to depend on both recall and recognition, there is little measurable overlap and both are affected by different contexts (Kellogg, 2003).

Both a two-theory approach and encoding specifically principle have been described as too simplistic, as they do not consider multi-route approaches. Also, recall may occur as either a direct or indirect process, as can recognition. Recall and recognition are said to both require two-way retrieval. Two-way retrieval leads into the memory process for knowing and can include episodic and semantic long-term memory (Eysenck & Keane, 2002).
2.2.3 Long term memory

Long term memory is the most important component for knowledge development and maintenance. There are many contemporary long-term memory theories, which according to Eysenck and Keane (2002) are becoming increasing difficult to discriminate between. As with working memory, long-term memory does not appear to be unity with scholarly disagreement between multiple systems or component models (Kellogg, 2003). Long-term memory theories that inform the study include episodic and implicit memory (Figure 2.2), with episodic memory providing the primary supporting model.

![Figure 2.2 Taxonomy of long-term memory](Adjusted from Kellogg, 2003, p. 151)

Episodic memory is the stored and encoded memory that may be gained through our every day life experiences. This memory uses the prefrontal cortex and is said to be a higher level cognitive process (Eysenck & Keane, 2002). Semantic memory is similar to episodic memory – a mental thesaurus – that organises the knowledge a person possesses about words and other verbal symbols, their meanings and referents, about relations among them, and about rules, formulas, and algorithms for the manipulation of these symbols, concepts, and relations (Tulving, 1972).
Explicit memory is the retrieval of information from experience, whereas implicit memory may be regarded as retrieval of information that has no recognition of learning or experiencing (Reisberg, 2001). There are crucial differences between explicit and implicit memory in the process of conscious recollection. The mind uses many areas of the brain in the retrieval of implicit memory, as the implicit memory tasks range across all brain functions (Eysenck & Keane, 2002).

Implicit learning is learning information without verbalising what has been learnt (Seger, 1994). As implicit memory is descriptive, implicit learning allows increased understanding of memory processing. Studies have attempted to use complex tasks to test implicit learning and the participant’s relationship with performance principles (Eysenck & Keane, 2002). However, it could be argued that this process may involve heuristic effects in learning similar to risk and judgement. This approach may also lead to a core difference between expert and novice, as an expert utilises implicit patterns to construct arguments and analogies (Zeitz, 1997).

Research with amnesia patients proposed the notion that there are two or more long-term memory systems. This proposal was based on the distinction between declaration knowledge and procedural knowledge. Declaration knowledge is knowing something, and includes semantic and episodic memory. An example of declaration knowledge could be the knowledge that the concept of a cat is subsumed under the feline animal group. Procedural knowledge is for example knowing how to ride a bicycle (Eysenck & Keane, 2002). Semantic or episodic memory provide an informing theory to the study as “it is through semantic memory that we categorise the world … to see a specific object as a general kind” (Kellogg, 2003, p. 204).

2.2.4 Knowledge categorisation
A person is exposed to information in his or her everyday life and concurrently knowledge has to be economised and abstracted into categories, generally referred to as concepts. Concepts may be further divided into implicit (inclusive) or explicit (concrete) concepts. These concepts are developed and maintained within long-term memory,
however there is a cognitive balance between the number and effectiveness of possible concepts. Concepts need to be informative, based to a degree on the natural world, economic and cohesive (Eysenck & Keane, 2002) and organised into categories (Kellogg, 2003). Similar objects are grouped together within a conceptual category and these groupings are generally a product of the learner’s environment.

There are considered to be four theories for concept categorisation – defining-attribute, prototype, exemplar-based and explanation views (Eysenck & Keane, 2002; Reisberg, 2001). The defining attribute view considers that attributes define item categorisation, which membership is inclusive and that subordinate concepts should contain the attributes of super-ordinate concepts. However, evidence does not fully support this theory (Eysenck & Keane, 2002) and therefore will not be further considered.

The prototype view considers that concepts are formed around the most commonly exposed or best example method and that category membership is based on averaged similarity (Reisberg, 2001). For example, a kangaroo could be considered to be a prototype for marsupial. People consider attributes or characteristics that form a kangaroo, which becomes the abstract concept for marsupials. This view allows for gradients of membership, considers abstract concepts within both artificial and natural worlds, and allows for demarcation between categories. Nevertheless, research has found that not all concepts have prototype characteristics, particularly those that are more abstract or inclusive. People also consider the relationships between attributes or characteristics when categorising are likely to modify their views on attributes. Although similarity does present a suitable argument, it does not consider unnatural groupings or why people may group certain objects (Eysenck & Keane, 2002) – particularly relevant to this study with its investigation of implicit security risk management concepts.

The exemplar-based view considers that people will use previous examples or particular instances to categorise, based on averaged similarity, thereby extending the prototype theory. This view allows people to categorise some items faster then others. For example, a kangaroo would be categorised as a marsupial relatively rapidly, whereas the
lesser known quokka would not (A quokka is a small marsupial, approximately the size of a domesticated cat and found in Western Australia (Rottnest Island Authority, 2005)). Items that are more typical increase their cue and therefore memory retrieval (Herrman, Yoder, Gruneberg & Payne, 2006). When there is no singular exemplar, the memory extracts the next closest approximation. This theory also accounts for the greater consistency of concept prediction and conceptual instability found with concepts (Eysenck & Keane, 2002). Nevertheless there are limitations with the exemplar-based view, as research has found that typicality and category judgement should be causal (Hampton, 1995).

Categorisation allows a person to predict likely attributes or characteristics of an instance or object. According to Murphy and Ross (cited in Eysenck & Keane, 2002) categorisation is not a very useful cognitive function, whereas the ability to quickly predict likely characteristics of an object may be a survival benefit. Categorisation allows inferences, with complex predictions made on category membership. However concepts can be unstable, producing undefined boundaries and changing membership. Category membership can change due to differing goals, perspective, experience or context, although the more common categories do remain stable over extended periods of time (Kellogg, 2003). In addition, neither attribute, prototype nor exemplar categorisations effectively explain ad hoc conceptual formations (Barsalou, 1983).

The explanation view was considered the primary knowledge categorisation theory informing the study, as this view considers that there are more complex and causal relationships in concept categorisation. The explanation view still considers similarity an important aspect, based on attributes and characteristics, however these alone do not provide a conclusive elucidation. Additional consideration within the explanation view is the importance of a person’s experience, existing knowledge and causal relationships between attributes, which may be represented by schemata. As salient knowledge of the concept increases so does the categorisation in multiple dimensions, which only occurs when the appropriate background knowledge is present. Concepts are stored in working
memory and are dynamic in structure (Eysenck & Keane, 2002), catering for ad hoc concepts.

Categorisation is a repeating theme within concept representation theories. Research, particularly on object concepts, has been well investigated in psychology (Eysenck & Keane, 2002; Kellogg, 2003). Common findings in these research studies include category judgement, typicality gradients, hierarchies, prediction and the instability of concepts. Category judgement defines whether an instance or object is a member of the category. Early research focused on developing rule-based attributes, whereas more recent research has shown that this is only one aspect of many considerations. More common instances produced what has been termed typicality gradient, where more commonly exposed objects presented reduced judgement time (Logie, 1999).

Concept categories aid cognitive economy through a conceptual three level hierarchy (Figure 2.3). These three levels – a superordinate, basic and subordinate are considered core domains of knowledge (Atran, Medin, Ross, Lynch, Coley, Ek & Vapnarsky, 1999). The superordinate level is the most implicit, abstract or inclusive, and is used for general categories. The basic level follows the superordinate level, which is where the majority of categorisation is applied and has the majority of definable attributes. Difference in instance or object definition at the basic level is generally dependent on the person’s experience. The basic level is the most used and recognised, is the first level acquired by young children and has the greatest level of similarity of instance or objects (Reisberg, 2001). Finally, the subordinate level, which contains explicit object definition, generally has similar or common attributes with the proceeding basic level (Eysenck & Keane, 2002).
2.2.5 Knowledge

Knowledge is constructed, is built on previous knowledge, and utilises and expands existing concepts (Novak & Gowin, 1984). Previous knowledge is an important aspect in memory performance. As new knowledge is gained, change in understanding with existing knowledge is achieved. According to DeGroot (1966), expert chess players can recall the position of 24 chess pieces if they form a feasible game play, whereas amateur players can remember approximately 10 pieces. However, place the pieces in a random format and experts can remember no more than amateurs. Expert knowledge is not an innate memory skill, as it can be learnt and acquired (Ericsson & Charness, 1997).

Knowledge is not mere facts, as claimed at the commencement of the discussion, moreover knowledge is based on previous knowledge, understanding, experience and the individual's interaction within their environment. Knowledge may not only be concrete fact or reality, however, is in addition perceptual understanding for that
individual. This approach is the constructivism view, that knowledge is viable and not absolute fact (Rennie & Gribble, 1999).

2.2.6 Expert knowledge structure

Expert performance may be defined as consistent performance on a domain specific representative task (Ericsson & Charness, 1997), although expertise cannot be so easily defined (LaFrance, 1997). Expertise requires a number of abilities that includes problem solving skills, conceptual understanding, domain knowledge and experience. A novice, when compared with an expert, will classify problems differently (Chi, et al., 1981). Novices generally group problems together, based on the same or similar surface features (schema). However experts classify problems based on deep structure, such as problems that could be solved with the same or similar principles (Kellogg, 2003). Experts tend to work forwards to a solution, whereas novices work backwards. Novices attempt to apply concepts as a best-fit solution to the problem, until they find a suitable concept fit. Nevertheless, experts may still spend as much time analysing and attempting to solve the problem, even through they generally solve a problem four times quicker than a novice (Chi, et al., 1981).

Experts structure concepts into hierarchical categories (Figure 2.4), allowing problems to be solved faster even through they spend the same time in analysis (Eysenck & Keane, 2002). In figure 2.4, the square represents superordinate or abstract features, whereas the circle and triangle represents basic and subordinate features, with numbers representing the number of problems in each category. This approach is considered backward chaining, where an expert proceeds in a forward chain (Kellogg, 2003).
Research by Chi et al. (1981) of expert and novice physicists has shown that these two groups have different representation of problems and therefore solve these problems at different conceptual levels. Novices appeared to group similar *surface features* together in a sequential manner, focusing on similar physical objects and keywords to solve a problem, whereas experts grouped problems together, defined by their *deeper structure* and principles (Kellogg, 2003). Novak and Gowin (1984) had demonstrated higher implicit understanding with concept mapping in the domains of management and marketing, with greater expertise leading to a deeper comprehension of hierarchical concept maps.

There are primary differences between domain experts and novices. Experts remember better, even through research has shown that they do not have greater memory capacity (Eysenck & Keane, 2002). Experts develop and use different problem solving strategies, and have a richer schema. Although what may be considered evident, experts have superior knowledge context which leads to the development of defined schemas, encoding context specific concepts and solutions. Finally, what could be considered a critical aspect within expertise, is greater and more extensive domain practice (Green & Gilhooly, 1992). These aspects allow experts to solve problems quicker by applying previously learned solutions or effectively applying similar solutions to new problems.
2.2.7 Becoming a domain expert

Development and acquisition of expertise is the result of a number of memory processes. Both physical and cognitive practice will result in what may be defined as the power law of practice, which demonstrates that continued practice will improve performance on a linear scale (Logan, 1988). For most experts, a decade of incremental learning and practice within a domain may allow that person to achieve domain expertise in knowledge and skill (Ericsson & Charness, 1997). Accordingly, development of expertise may be supported through knowledge chunking, proceduralisation and learning from mistakes (Eysenck & Keane, 2002).

Achievement of expertise is not automatic, otherwise everyone within a discipline for an extended period of time would become expert. According to Ericsson and Charness (1997), individuals achieve expert performance through not only incremental learning and practice, however, through structured learning and effortful adaptation. Effortful adaptation is the deliberate practice that is motivated by the goal of improving performance. Continued effortful practice allows memory to be developed that removes intermediate steps of processing, referred to as chunking and becoming the norm in many cognitive architectures (Anderson, 1996; Newell, 1990).

Proceduralisation is problem solving attempts and instruction, often referred to as adaptive control of thought (ACT) theory. Declaration memory stores and retrieves information chunks, and procedural memory contains and develops production rules for situations. Experts form chunks of information, develop declaration memory and procedural knowledge. Learning from mistakes allows the development of knowledge. Novices may begin with basic concepts and limited experience, nevertheless with practice and learning from performance errors, build expert context knowledge (Eysenck & Keane, 2002). It can be argued that this domain experience leads to a better implicit understanding of how concepts integrate and apply. An “important part of becoming an expert in a domain is becoming facile at processing information at the appropriate level of abstraction for that domain” (Zeitz, 1997, p. 44).
2.2.8 Knowledge categorisation conclusion

Knowledge requires not only rote memorisation of facts or figures, however, also an accumulation of past experience. Knowledge is contained within many parts of the brain, being acquired, stored and retrieved through the sensory store, working memory and long-term memory. Memory is the ability of a person to retain and recall information, sensations, thoughts and knowledge. When considering knowledge, long-term memory is important. Nevertheless, there are many competing long term memory theories within cognitive psychology, although *episodic memory* informed this study.

As information is gained, knowledge has to be abstracted and categorised for cognitive economy. Categorisation involves cognitively grouping similar objects, although categorisation has to be informative, economic, cohesive and based on the real world. As with long-term memory, there are various categorisation theories. However, recent research (Eysenck & Keane, 2002; Kellogg, 2003; Logie, 1999) claimed that the *explanation* view was the most inclusive, as this considers object attributes, characteristics and relationships, and the person’s existing knowledge and experience. Therefore, the explanation view was the informing theory supporting knowledge categorisation within this study.

Knowledge is constructed from existing and new information, which may be either explicit fact or perception. As people gain domain knowledge, they may become an expert. Nevertheless expertise is not the exclusive gathering of information, however a rich understanding of knowledge and how that knowledge integrates into concepts. Experts, unlike novice learners, understand domain knowledge in a hierarchical manner and have more complex schema. This knowledge categorisation can be represented with concept maps, showing rich knowledge structure (Markham, et al., 1994).

2.3 Concept mapping

Concept maps may be defined as a representation of a state of affair or situation. People may attempt to understand the world though developing a concept map of the situation, an idea, understanding or principle. Concept maps are thinking tools, that are used to
explore different aspects of a topic (Wallace, Schirato & Bright, 1999). Concept maps are generally imaged, dynamic and outcome-based simulations that are used in everyday life to think and understand the world (Eysenck & Keane, 2002; Johnson-Laird, 1983; Norman, 1983). Concept maps enable people to exchange an idea, have shared understanding, provide a common language, reach conclusions in decision-making and guide their action (Norman, 1983; Novak & Gowin, 1984). Concept maps may also be referred to as mental maps, mind maps, naive theories or folk theories, although these are considered to have different characteristics (Bennett & Rolheiser, 2001).

Concept maps attempt to present many aspects of human cognition, from direct representation of a physical entity to abstract thought. Physical representation may map the flow of electricity, supported by visual objects like the flow of water or people. This view supports concept understanding as once a person understands the physical process, most will accept a formal model of the process (Bar & Travis, 1991). Representation of abstract thought is far less defined and involves implicit knowledge, although these models will “represent aspects of external reality” (Borges & Gilbert, 1999, p. 96). According to Eysenck and Keane (2002), people will often make discoveries using concept models to simulate aspects of the world, an ability that appears to depend on domain specific knowledge based on experience.

Experts achieve their status through an understanding of domain knowledge in a hierarchical manner, with a robust understanding of conceptual relationships. Explicit knowledge is subsumed under higher order implicit knowledge (See previous Figures 2.3 and 2.4). However, knowledge is often taught in a sequential manner, even through our minds represent knowledge within a hierarchical form (Novak & Gowin, 1984). Concept maps allow this hierarchical presentation of knowledge to the novice learner, aiding teaching and learning.

Concept maps do not necessarily mimic the physical entity or abstract thought. Map development has been used to great effect to model physics and chemistry concepts to aid learning and therefore understanding (Gilbert & Boulter, 1998; Treagust,
Even through these concepts are more inclusive, they are still an abstract model. Johnson-Laird presented an example when emulating a breaking wave with software, concluding that it would be “absurd to criticize [sic] the program on the grounds that it was not wet” (1983, p. 9).

Early research into physics and chemistry concept maps (Gentner & Gentner, 1983; Johnson-Laird, 1983; McCloskey, 1983) demonstrated that naive maps were well articulated and fairly consistent across individuals; nevertheless, when compared to fundamental principles were incorrect (Eysenck & Keane, 2002). Research studies have concluded that concept mapping provides a “theoretically powerful and psychometrically sound tool” (Markham, et al., 1994, p. 91) for assessing domain knowledge. Concept mapping allows a method to externalise knowledge structure in an overt manner (Novak & Gowin, 1984).

Concept maps may take many forms, however, within the context of this study they are defined as graphical representations of structured knowledge. According to Novak and Gowin, concept maps are a “schematic device for representing a set of concept meanings embedded in a framework of propositions” (1984, p. 15). The schema may be as a body of knowledge, being the summation of domain experts understanding of their knowledge structure at that point in time (Trochim, 2005b), or as an individual and how a concept map may represent their understanding.

Visually concept maps are graphical representations made up of branches, nodes, interconnecting lines and propositions, with hierarchical structure and horizontal integration (Figure 2.5). The hierarchical nature of concept categorisation may be demonstrated by an artefact, such as a clay hammer (subordinate level), hammer (basic level) and tool (superordinate level) (Kellogg, 2003). Nodes or branches represent concept clusters, being concepts that are similar in idea, principle or application. Within nodes, explicit concepts are subsumed by higher order implicit concepts. The lines between the nodes indicate relationship between concepts, with an explicit statement
linked to a line. The relationship between the two nodes, line and statement is the proposition (Bennett & Rolheiser, 2001).

Figure 2.5 Concept map of concept mapping
(Novak, n.d.)

2.3.1 Types of concept maps
According to Johnson-Laird (1983), concept maps may be divided into two distinct types, such as physical or conceptual maps. Physical maps provide representation of physical systems and research has tended to focus on physical objects, particularly in chemistry, physics and biology domains (Johnson-Laird, 1983; Novak, 1998), whereas conceptual maps represent abstract or inclusive knowledge categorisation (Eysenck & Keane, 2002; Reisberg, 2001). A user will develop a concept map of an object (Figure 2.6), referred as the target system. The conceptual model attempts to represent the user’s target system and this is generally developed by experts, whether scientists, curriculum designers or teachers. The scientist’s conceptualisation is a model of a model, which
attempts to represent the user’s concept model (Norman, 1983). Nevertheless, according to Ross and Munby (1991), a u

Figure 2.6 Types of concept maps
(Adjusted from Norman, 1983)

Research has further defined types of concept maps – scientific, teaching, concept and expressed models. A scientific or consensual model could be considered a theory which has been developed, tested and accepted as scientific theory. A teaching model is a simplistic model of the scientific model, constructed by teachers to aid teaching and learning. The concept model is a personal representation of the state of affairs or target. Finally, the expressed model is the resulting outcome expressed by the person, through action, speech or writing (Treagust, et al., 2004).

Norman (1983) stated that concept maps and the conceptualisation of concept maps have three properties, being the belief system, observability and predictive power. The belief system is perceptual understating, with observability of the causal link between person and system. Predictive power allows the person to understand and anticipate. Criticism has expanded these three properties to include the physical link, multiple models and volatility (Eysenck & Keane, 2002) of concept models. Concept maps must have a degree of linkage between the physical system they purport to model and the person’s conceptual mapping, otherwise it will not be an effective model. The physical link is not
necessarily a duplicate of the real world, however an emulation. A person may also have multiple models of the same system to deal with different environments or actions of that system. Finally concept maps are volatile, evolving when knowledge changes (Eysenck & Keane, 2002).

When asked to model their concept map of an activity, people may distort their map believing that this view is a valid representation. Nevertheless, their own understanding of their concept map is not always correct (Gentner & Gentner, 1983) and assimilation of the concept map into cognitive structure depends on their existing knowledge (Bar & Travis, 1991). In addition, when domain experts are compared to novice learners they have a greater number of concepts and relating propositions. Experts tend to define their knowledge within concept clusters, which are more extensive, have greater cross concept linkage, increased branches, greater hierarchical structure and are more complex. For example, Markham, et al. (1994) demonstrated that students majoring in a discipline had a greater array of domain-specific, implicit and superordinate concepts that organised their knowledge structure. It was claimed that the number of valid concepts and propositions can be taken as a quantitative measure of expertise (Markham, et al., 1994).

2.3.2 Propositional linkages

Concept maps are a representation of how a person may understand knowledge and the meaningful relationship between knowledge concepts. The relationships between these concepts are in the form of propositional linkages, such as a linking line and supporting label or statement between two concepts. The propositional linkage is developed from a statement describing that linkage (Novak & Gowin, 1984; Tan, 2000).

Propositional linkages describe the binding relationship or statement between two or more concepts (Novak & Gowin, 1984), nevertheless they do not necessarily have to be true (Wilson, Halford, Gray & Phillips, 2001). According to Eysenck and Keane “propositional representations are considered to be explicit, discrete, abstract entities that represent the ideational content of the mind” (2002, p. 247). Propositional linkages
may be expressed explicitly in a full sentence, as opposed to single words, offering the expert and therefore learner, greater cognitive and structural understanding of the concept map (Hoz, et al., 1997). However, according to Johnson-Laird (1983), extended or descriptive statements do not necessarily increase the usefulness of the model.

### 2.3.3 Modelling concept maps

There are many methods, with an enormity of variations (Hoz, et al., 1997; Ruiz-Primo, et al., 2001), to extract, develop and present concept maps. Nevertheless, it is claimed that there are three primary methods, being *multiple-choice questionnaire, interview or psychometric analysis* techniques. These methods may use a number of techniques to extract the initial participant data, including word association, tree construction, free sort, similarity rating, ordered tree, questionnaire, experimentation, card sorting, teaching assignment, and paper and pencil. Within these three primary areas, many variations in research and teaching have been applied (Robin & Hambleton, 2003; Streveler, et al., 2001; Turns, et al., 2000).

An aspect of many of these methods is the *directedness* with which the process is applied to data extraction and participant concept mapping development. An open interview will allow the participant to develop and display his or her concept map structure including inclusive concepts, hierarchical nature and propositions. Whereas a multiple-choice questionnaire or psychometric analysis allows restricted input from the participant, with a high degree of researcher or assessor interpretation (Ruiz-Primo, et al., 2001). It is stated that to a degree the most appropriate method will depend on the intent of the concept map, as a non-structured or less direct approach may lead to divergence of concept maps. Variance may be undesirable in a teaching and learning environment, as it becomes difficult to develop appropriate types of concept maps, evaluate and assess concept models between cohorts, and achieve consensual maps.
Table 2.1

Degree of directedness in concept map evaluation

<table>
<thead>
<tr>
<th>Map Components</th>
<th>High degree of directedness</th>
<th>Low degree of directedness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concepts</td>
<td>Provided by assessor</td>
<td>Provided by participant</td>
</tr>
<tr>
<td>Linking Lines</td>
<td>Provided by assessor</td>
<td>Provided by participant</td>
</tr>
<tr>
<td>Statements</td>
<td>Provided by assessor</td>
<td>Provided by participant</td>
</tr>
<tr>
<td>Map Structure</td>
<td>Provided by assessor</td>
<td>Provided by participant</td>
</tr>
<tr>
<td>Propositions</td>
<td>Provided by assessor</td>
<td>Provided by participant</td>
</tr>
</tbody>
</table>

(Adjusted from Ruiz-Primo, et al., 2001, p. 262)

2.3.3.1 Multiple-choice questionnaire technique

Multiple-choice questionnaires comprise of defined and structured questions that have a number of prepared responses, with participants selecting what they believe is the most appropriate response. These instruments have been used to measure a large number of participants concept understanding (Tan, 2000) and when compared to interviews, these test are generally quicker to administer, score and analyse (Tan & Treagust, 1999). However, this type of test may not elicit implicit knowledge, understanding or alternative concept maps as participants are guided by the multiple-choice questions and response, resulting in an inappropriate concept map. Errors may be caused by multiple-choice questionnaires, as participants may interpret the questions in a different manner than the designer intended. Participants may have reading comprehension error that cannot always be detected through this style of test. Finally, participants may guess their response, further skewing results. This view was supported by Markham, et al., (1994) when they claimed that not all conceptual dimensions may be shown through multiple-choice questionnaires tests.

2.3.3.2 Interview technique

Interviews allow researchers to develop concept maps and gather knowledge that may not be achieved through other methods, for example non-verbal communication to elicit true meaning. Interviews allow the measure of attitudes, how variable relationships may be defined and to validate other research methods (Cohen, Manion & Morrison, 2002). An expert can quantify understanding through diagrams, as the participant draws his or
her understanding of knowledge and justifies relating propositions. The quality, interpretation and predictability of the participant’s mapping will indicate their understanding of the concept (Tan, 2000).

Interviews may be structured, semi-structured or unstructured (Cohen, et al., 2002; Tan, 2000). Structured interviews involve predefined questions and these are rigidly maintained. Semi-structured involves predefined questions, nevertheless, these may be open-ended or allow a degree of diversion from the questions. Unstructured interview involves open-ended questions that are guided in part by the response given by the participant. Interview questions may be direct or indirect, deal with a general or specific event or invite fractal response or opinions. The type of interview used should depend on the required outcome. There are disadvantages with interviews, primarily the possible bias of the interviewer, not eliciting true opinion, subjectivity of analysis, a costly interview process, time consuming to apply and the motivation of the interviewed (Cohen, et al., 2002).

2.3.3.3 Psychometric analysis technique

There are many psychometric techniques that may be used to extract concept maps from participants, including multidimensional scaling (MDS) (Agrafiotis & Lobanov, 2001; Ding, 2003; Trochim, 2005b), hierarchical clustering, latent partition analysis, smallest space analysis, Reuter’s method, Warren’s method, (Hoz, et al., 1997), Linear Structural Relationships (LISREL) and trajectory mapping (Lokuge, Gilbert & Richards, 1996). In considering these studies, it was proposed that there had been restricted research into psychometric MDS concept mapping techniques.

MDS was used within the study as a novel process that presents a spatial presentation of underlying dimensionality (Agrafiotis & Lobanov, 2001), developed from the sum of individual experts. MDS facilitates the demonstration of multiple dimensionality though the clustering of expert knowledge (Markham, et al., 1994), without pre-determined interpretation of spatial locality (Turner, 2002). Ohanian (cited in Stein, 1997) supported
this view, when stating that expertise can be measured as a construct that contains multiple dimensions.

The use of MDS in concept mapping was first presented by Trochim (1989b), and his later work expanded and detailed the methodology of constructing and presenting concept maps (Trochim & Cook, 1994). Nevertheless, Trochim’s (1989b) earlier work considered only knowledge structure, a rather restricted approach that contradicted Novak’s (1990) view of concept mapping and which continued to more recent work (Trochim, 2005b). During this period Markham, et al. (1994) used MDS as a method to test the validity of concept mapping, considering the previous work by Novak (1990). Markham, et al. (1994) demonstrated that concept mapping provided a theoretically valid and powerful tool, and that MDS proved an appropriate statistical technique to define concept maps. A view that more recent researchers have validated, through additional MDS concept mapping studies (Ruiz-Primo, et al., 2001; Streveler, et al., 2001).

Recent researchers have integrated both concept mapping and MDS, which included studies that consider a scientific method to design a teaching methodology used in basic signal processing (Martinez-Torres, et al., 2005), the spatial variation of species diversity (Cheng, 2004), techniques used by physiotherapists in Southeast Australia (Turner, 2002) and computer-based collaborative learning environments (Kealy, 2001). However, all these studies generally only considered the integration of concept mapping and MDS at the structural knowledge level, without considering the complete psychometric concept mapping process.

MDS does not provide a holistic concept map of complex domain knowledge structure, as it can only elicit and demonstrate knowledge clusters. Propositional statements, which provide concept map understanding (Bennett & Rolheiser, 2001) and therefore concept relationships, are not presented by MDS. Some form of additional analysis has to be applied to the psychometric MDS concept map and this requires a degree of expert association. Although the use of MDS to develop concept maps and present knowledge
structure has been validated by previous authors (Markham, et al., 1994; Streveler, et al., 2001), it is proposed that there is still more research required to validate a reliable psychometric MDS concept mapping methodology.

2.3.4 Concept maps in teaching and learning

Concept mapping has been widely used in science education research and development for over 20 years (Hoz, et al., 1997; Markham, et al., 1994) – without concept maps being limited to any particular cohort of learner (Rice, Ryan & Samson, 1998). According to Novak and Gowin, concept mapping has a “positive influence on teaching, learning, curriculum, and governance” (1984, p. 6), supported by McAleese who claimed that concept mapping is an “adjunct to teaching and [is] coming of age (1999, p. 351). Understanding how people develop and use concept maps can aid effective teaching and learning. This understanding supports the teacher in knowledge transfer, what knowledge pathways to consider, how to effectively develop these and whether they provide the appropriate level of implicit understanding. In addition, concept maps support curriculum development, knowledge acquisition and content (Smith, 2003), design of instructional materials, identification of misconceptions, teacher and student understanding of constructed knowledge (Novak, 1996) and how effective delivery can be achieved in the classroom (Novak & Gowin, 1984). However, teaching and learning cannot be wholly addressed unless the domain knowledge structure is known and understood (Novak & Gowin, 1984; Smith, 2003), an area where concept mapping can assist.

The ability of students to construct complex concept maps may demonstrate their understanding of domain knowledge, as learning requires new knowledge to relate to old and that knowledge is built on existing conceptual understanding (Novak & Gowin, 1984). Students who constructed valid concept maps were able to “generate substantially greater number of scientifically acceptable propositions” (Markham, et al., 1994, p. 92), a view supported through the testing of students’ animal and plant clustering, and interspecies relationships (Tunnicliffe & Reiss, 2004). Knowledge definition and structure facilitates cognitive understanding (Reisberg, 2001), and the difference between domain
experts and novices is how their knowledge may be structured (Bennett & Rolheiser, 2001; Ruiz-Primo, et al., 2001). Teaching and learning should explicitly support students’ efforts in understanding knowledge and its structure, and how knowledge structure is presented allows the design of educational programs (Novak & Gowin, 1984).

To progress from novice learner to expert requires both the acquisition of knowledge and the ability to apply implicit knowledge or demonstrate connected understanding of concepts (Kinchin, 2001). Experts apply a greater level of abstract processing, complexity and interpretation in their use of knowledge concepts, whereas novices only consider surface level knowledge (Zeitz, 1997). Experts link abstract concepts that may be used to resolve similar problems (see Figure 2.4), unlike a novice who attempts to find a solution that may fit (Green & Gilhooly, 1992). Therefore, experts cluster similar concepts together and unlike concepts apart and such concept maps may demonstrate implicit cognitive development or “knowledge arenas” (McAleese, 1999). As research with concept maps of electricity has shown, “pattern of progression may be related to individual’s acquisition of conceptual knowledge” (Borges & Gilbert, 1999, p. 95).

It could be argued that novice learners should be exposed to domain concept maps as early as possible, even if they cannot fully understand the many propositions. This concept map exposure may allow novice learners to begin to develop an understanding of these concepts and their relationships. However, this idea is opposed “since exposure to highly complex and abstract models is more appropriate for learners who wish to continue their studies” (Coll & Treagust, 2003, p. 685). Nevertheless, a degree of holistic understanding of an expert’s concept map may assist novice learners to begin to develop their own valid concept map, a view supported by Treagust, et al. who proposed that “teaching models can play a pivotal role in initiating students’ development of scientific models, mental models, and expressed models” (2004, p. 1). In addition, concept maps may help students manage their knowledge when dealing with complex cognitive tasks (Tergan, 2004).
Conventional assessments fail to recognise that in-depth disciplinary knowledge may be based on an understanding of causal relationships among domain concepts, a premise advanced by Novak and Gowin (1984). Novak and Gowin (1984) stated that even the most objective tests only achieve a low to moderate correlation rate ($r=0.2$ to 0.7) and that when compared to later performance, the correlation drops to near zero. Concept maps are workable alternative evaluation tools, an idea supported by other studies (Kankkunden, 2001; Shymansky, et al., 1997) because they expose and express dimensions of knowledge that traditional assessments cannot (Hoz, et al., 1997). However, there are limitations in the ability of concept maps to provide a workable evaluation method. As Kinchin put forward, “the problem with classroom concept mapping has not been explicitly addressed by the literature” (2001, p. 1257). Problems with concept mapping in teaching and learning may include the epistemological belief by classroom teachers, the philosophy of the curriculum (Kinchin, 2001) and the ability to use concept maps in practical evaluation (Rice, et al., 1998).

Nevertheless, there is agreement that concept maps present knowledge structure (Ruiz-Primo, 2000) and capture configurable property of knowledge more effectively than other assessment methods (Markham, et al., 1994; McAleese, 1999). However, a study found that the inclusion of concept maps within the learning environment did not significantly improve the externalisation of the students’ conceptual understanding, although students did find the concept map helpful (Rice, et al., 1999; Rye & Rubba, 1998). As Novak and Gowin stated, “meaningful learning proceeds most easily when new concepts or concept meanings are subsumed under broader, more inclusive concepts” (1984, p. 15). The ability of students to be able to relate concepts within a domain is “an important characteristic of scientific literacy” (Ruiz-Primo, et al., 2001, p. 260), with concept maps providing students with the means “to discover tentative meanings for concepts taught” (Kankkunden, 2001, p. 287).

Concept maps assist “students to organise and represent their thoughts” (Bennett & Rolheiser, 2001, p. 292). Knowledge is stored within memory in a hierarchically organised structure and relationships between concepts may be dependent on inclusive
abstract understanding, leading towards more concrete lower level concepts (see Figure 2.3). A student who presents a concept map with an incorrect hierarchy, process, complexity or propositional linkages may not necessarily be wrong, on the contrary, they may have a creative understanding of the concepts (Kinchin, 2001). Progressive differentiation of concepts is the increase in knowledgeable understanding of existing known concepts, which deepens the person’s understanding of that and related concepts. Integrative reconciliation increases as the person’s understanding of a concept increases, leading to a more robust propositional understanding (Novak & Gowin, 1984).

Although concept maps may aid teaching and learning, they are “not a perfect assessment solution … and remain ambiguous” (Turns, et al., 2000, p. 172). However, in the majority of the literature (Kinchin, 2001; McAleese, 1999; Novak, 1996; Ruiz-Primo, 2000) researchers remain supportive of the benefits of concept mapping in teaching and learning, along with the utility of concept maps (Rice, et al., 1998). Nevertheless, there needs to be greater research to investigate which aspects of students’ knowledge are considered by the many different techniques to develop and assess concept maps (Ruiz-Primo, et al., 2001). In addition, the limitations of concept mapping in teaching and learning has to be considered.

2.3.5 Concept mapping limitations
There are limitations with concept mapping, with both traditional individualistic approaches and the use of psychometric MDS concept mapping. Within this section, the capricious nature of concept mapping, cognitive information chunking, semantic understanding and directed concept mapping techniques are considered. The use and appropriateness of concept mapping in teaching and learning is presented – with the epistemological belief by teachers, the philosophy of curriculum design (Kinchin, 2001) and the practical application of concept maps (Rice, et al., 1998). In addition, concept mapping reliability and validity conclude this section.

Concept maps are developed by people to fit what they consider to be the real world. However within a variable environment, this fit could result in a complex and volatile
map that may exceed a person working-memory (Kellogg, 2003). The cognitive comprehension component of concept maps has not been fully defined and within the context of how background knowledge and uncertainty affect maps – both may have significant affect on concept map construction (Eysenck & Keane, 2002).

Millar claimed that short-term memory has restricted and fragile storage capacity, resulting in information chunking (cited in Reisberg, 2001). An example may be the use of the security principle CPTED, which for a domain expert would be considered a single chunk of information. However, for a novice this may require up to five chunks of information, being crime-prevention-through-environmental-design. Chunking limits the ability to deal with more than seven concepts simultaneously (Novak & Gowin, 1984), leaving a degree of cognitive encumbrance when considering larger concept maps.

People may have varying semantic understanding of knowledge categories or concepts when described by words, resulting in concept map distortion. Expertise may also lead to increase use of domain jargon or terminology to consider what others may describe in more simplistic language (Markham, et al., 1994). As a result of these issues, concept maps require interpretation and can remain ambiguous (Turns, et al., 2000). According to Novak and Gowin (1984), a method to overcome semantic understanding is to develop knowledge categories by classifying how the participants used their knowledge. Consequently, semantic understanding within long-term memory can support concept mapping, as “in spite of much language-related research, language data remained underestimated and under-exploited as a unique and amazing source of information for reconstructing deeper cognitive process” (Fauconnier, 1997, p. 5).

Templates have been used to construct students’ concept maps, a method that facilitates evaluation against a valid consensual or expert constructed map using directed mapping overlays. However, one drawback of this directed approach is the tendency for assessors to interpret only what they wish to see, producing a biased evaluation (Novak & Gowin, 1984). A view supported when considering highly-directed concept mapping techniques.
(see Section 2.3.3) and the likelihood that this may “misrepresent knowledge structure by imposing a structure on [the students’] responses” (Ruiz-Primo, et al., 2001, p. 262).

Studies (Ruiz-Primo, et al., 2001; Schau & Mattern, 1997) tested two interview concept mapping techniques of fill-in-the-gaps (directed) and construct-a-map (undirected), finding that construct-a-map provided a better evaluation of knowledge. Nevertheless, the use of concept maps in classroom evaluation still remains a complex process, “very likely too much to be used in the regular classroom setting” (Rice, et al., 1998, p. 1123). However, and in contrast, Kankkunen (2001) recommended that the assessment of concept maps should take place in the classroom.

Experts may have their own unique concept map of how they view conceptual knowledge structure and relationships. While these may be valid concept maps, these alternative maps do not necessarily represent a domain approach. Research has not fully demonstrated how people counter valid concept maps with alternative examples (Polk, 1993). Domain experts may maintain their own semantic understanding of concepts, resulting in their own unique and resilient knowledge structure (Markham, et al., 1994). However, this idea may be opposed as it has been claimed that as a person gains greater expertise, so his or her concept maps become more consensual (Kealy, 2001).

Many studies have tested the ability of concept maps to improve teaching and learning (Bennett & Rolheiser, 2001; Kealy, 2001; Kinchin, 2001; Martinez-Torres, et al., 2005; McAleese, 1999; Turns, et al., 2000). One such study (Rye & Rubba, 1998) found that the inclusion of a concept map within the learning environment did not significantly improve the externalisation of the students’ conceptual understanding, although the students did state that they found the concept map helpful. In addition, demonstrating that a person can understand a concept map does not causally guarantee that the person will be able to apply these conceptual relationships (Turns, et al., 2000). Nevertheless there is general support, as demonstrated in the literature, in the ability of concept maps to aid teaching and learning – concept maps are just not used within the classroom.
Concept mapping may be restricted in classroom application due to epistemological belief by teachers and the philosophy of curriculum design (Kinchin, 2001). As Novak (1996) stated, concept mapping can be a useful tool in organising curriculum, lectures and text; however, only a minority of classroom teachers regularly use concept maps to organise their lessons. This restricted use of concept mapping, as a basis for classroom activities, was observed by Kinchin (2001). In addition, Rice, et al. (1998) raised the limited practical application of concept maps.

Teachers have their own pedagogical model of concepts which guide their decisions on teaching and learning. Superseding their pedagogical model are the questions that they should pose, how the concepts may be presented to the students and how student problems may be resolved; all are complex issues (Zimmermann, Boulter & Gilbert, 2004). The development of concept maps, although aiding novice learners, does not necessarily produce an instructional curriculum (Perkins cited in Wilson & Cole, 1996). However, improved teaching and learning is likely to result from increased understanding of domain concepts (Martinez-Torres, et al., 2005; McClure, Sonak & Suen, 1999; Turns, et al., 2000).

Concern with the reliability and validity of concept mapping has been raised by a number of authors (Hoz, et al., 1997; Markham, et al., 1994; Ruiz-Primo, et al., 2001), resulting in the need to address these issues before concept mapping is applied within the wider teaching community (Ruiz-Primo & Shavelson, 1998). Nevertheless, research does support the appropriateness of concept mapping as a general representation of cognitive knowledge structure (Eysenck & Keane, 2002; Reisberg, 2001) and this is supported by psychometric MDS to develop and present such knowledge structure (Rye & Rubba, 1998; Streveler, et al., 2001; Turner, 2002). According to Trochim, “the concept mapping process can be considered reliable … to generally-recognised standards for acceptable reliability levels” (1993, p. 1). However, no study was found that tested the reliability and validity of the inclusive psychometric MDS concept mapping methodology.
As Eysenck and Keane (2002) claimed, concept modelling presents an effective general theory that has been well dispersed, explains aspects of imagination in counterfactual and spatial reasoning, and creativity and probabilistic reasoning. This view was supported by Novak and Gowin (1984), because “concept mapping has a potential for enlisting this human capacity for recognising patterns … to facilitate learning and recall” (p. 28) and resulting in concept mapping making a valid tool in science education (Markham, et al., 1994).

2.3.6 Concept mapping conclusion

Concept maps are considered a suitable method to represent knowledge structure (Markham, et al., 1994) because they can be used to present a person’s understanding of an idea, exchange these ideas and reach consensus (Eysenck & Keane, 2002; Novak, 1998). Concept maps may be displayed as spatial maps that exhibit hierarchically structured knowledge through the construction from $n$ concepts, with interconnecting lines between these concepts and propositional statements that provide meaning (Bennett & Rolheiser, 2001).

Experts contain a robust understanding of conceptual knowledge within their domain (Novak & Gowin, 1984) which may be presented as a concept map. In an individual’s construct there are considered to be a number of concept map types, divided into physical and conceptual (Johnson-Laird, 1983). However, more recent research has offered additional concept maps, such as scientific, teaching, concept and expressed models (Treagust, et al., 2004).

There are a number of different methods to model concept maps, such as multiple-choice, interview or psychometric analysis techniques (Ruiz-Primo, et al., 2001), however within these three methods there are many more variations (Robin & Hambleton, 2003; Streveler, et al., 2001). The degree of directness various in each concept mapping method (Ruiz-Primo, et al., 2001), with the interview technique being the least-directed and allowing the participant to develop his or her own self-directed map. In contrast, the psychometric MDS technique is highly-directed and there is limited
contact between the participant and the concept map, except for data extraction. Investigative research into psychometric MDS concept mapping technique appeared to have been limited, particularly considering Novak’s (1990) view of concept mapping.

The use of MDS to develop psychometric concept maps first appeared in the late 1980’s, with early work by Trochim (1989a). Trochim expanded and detailed the methodology of using MDS to construct and present concept maps (2005b), however, only knowledge structure was considered. This approach contradicted Novak’s (1990) view of concept mapping, because Novak considered concept mapping as a representation of a person’s understanding, requiring both knowledge structure and informing propositional linkages. Nevertheless during this period, Markham, et al. (1994) used MDS to test the validity of concept mapping, taking into consideration Novak’s (1990) previous work. Markham, et al. (1994) demonstrated that concept mapping provided a theoretically valid and powerful tool, and that MDS provided an appropriate statistical technique to define concept maps, a view validated by recent psychometric MDS concept mapping studies (Ruiz-Primo, et al., 2001; Streveler, et al., 2001).

Concept maps have been widely used in science education for many years (Hoz, et al., 1997; McAleese, 1999; Rice, et al., 1998) and provides an alternative approach to assist teaching and learning in a number of ways (Bennett & Rolheiser, 2001). For example, teaching and learning may benefit from concept mapping through the development and display of expert knowledge structure, assist in developing curriculum (Smith, 2003), aid novice learners in the understanding of conceptual relationships (Tunnicliffe & Reiss, 2004) and as an alternative to more traditional assessment techniques (Hoz, et al., 1997; Ruiz-Primo, 2003).

Concept maps have limitations because they are capricious in nature, limited due to cognitive memory chunking, distorted via semantic concept understanding, have many construction techniques, have restricted practicability within classroom teaching and learning, and concern in their measures of reliability and validity. Nevertheless MDS, when integrated with concept mapping, can provide an appropriate research method to
develop and present expert knowledge structure as concept maps, because experts cluster knowledge concepts within multiple dimensions (Markham, et al., 1994; Turner, 2002). The integration of MDS and knowledge structure to develop and represent psychometric MDS concept mapping was a significant objective of this study.

2.4 Security
Security can be defined as assured freedom from poverty or want, precautions taken to ensure against theft, espionage, or a person or thing that secures or guarantees (The Angus & Roberston, 1992). Moreover, security may be the “protection of assets from loss” (McCrie, 2004, p. 11) or the “full range of functions required to protect the modern enterprise against pure losses” (Walsh & Healy, 2004, p. 1-I-2). According to Fischer and Green, “security implies a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of such disturbance or injury” (2004, p. 21). Security may also be considered the relationship between the individual and state which is an objective for the individual that can only be achieved as a collective (Rothschild, 1995).

However, security may also be expanded to consider national security and the defence of a nation, through armed force or the use of force to control a state’s citizens. Security may imply public policing with state employed public servants. Still others (Brooks, 2006; Smith, 2003) may consider security as crime prevention, security technology, risk management or loss prevention. Moreover, security may not necessarily only be restricted to the law-abiding, directed towards crime or for the common good (Manunta, 1999). The variance of security results in a society that has no clear understanding of what security is, nevertheless, which has a divergence of interests from many stakeholders (Manunta, 1999). This view is held by Fischer and Green, when they stated that “there is no universal agreement on a definition or even on the suitability of the term [security]” (2004, p. 37).

Historically, security was considered the private protection of an individual or their property and was offered only to those who could afford such paid protection. Private
protection expanded to include like-minded individuals who formed cohorts to fund private security protection. Through social expansion public policing developed, funded though public monies gathered from taxation (Fennelly, 2004). The traditional definition of public security is the protection of lives, property and general welfare of people in the community. On the other hand, private security is the provision of services in the protection of lives, information and assets within the private sector (Craighead, 2003).

Private or commercial security may be considered the provision of paid services in preventing undesirable, unauthorised or detrimental loss of organisational assets (Post & Kingsbury, 1991). Nevertheless, security may present very different meaning to different people, given differences in time, place and context. It has been claimed that security has to have a shared definition among many disciplines, that is essential and urgent (Manunta, 1999). However, the current international fight against terrorism and related threats has shifted security into an ambiguous arena (Horvath, 2004), where security may be presented within many diverse knowledge domains.

### 2.4.1 Defining security

It has been claimed that security lacks definition (Tate, 1997) and therefore lacks structured knowledge. In addition, the security discipline is diverse, cross-disciplined and without a defined or specified knowledge or skill structure (Hesse & Smith, 2001). However, this view should not lead to a conclusion that security does not contain a definable knowledge structure. As a comparison, other disciplines are poorly structured, nevertheless, experts have still developed and defined abstract interpretation (Zeitz, 1997). The diversity and cross-disciplined nature of security will evolve as the discipline becomes more professional, concepts are developed and defined, and tertiary education increases to support the discipline. As Fischer and Green (2004) advised, security has an excellent future considering the growth indicated in the discipline.

Security has strong parallels with Defence, because they both provide protection; however, there are “disturbing differences” between these industries (Tate, 1997, p. iii). Defence, as with other related industries, is often considered to be security. An example is the parallelism demonstrated through police and military organisations with increasing
convergence in their response to Australian homeland security challenges (Ferguson, 2004). In contrast and opposing this convergence is the breadth of agencies that may respond; within Australia there are “over 30 separate government departments and agencies contributing to safeguarding Australia” (Yates, 2004, p. 3). This diverse and multi-disciplined approach to security cannot support a single definition of security (Morley & Vogel, 1993). As ASIS International stated, “every time we think we’ve got the definition of the security field nailed, somebody … starts taking some of the nails away” (2003, p. 10). Nevertheless, it has been proposed that security has to have a shared definition among the many disciplines that incorporate security, and that this is essential and urgent (Manunta, 1999).

Manunta (1999) put forward a definition of security that used the formula:

\[
\text{Security} = f(A, P, T) Si
\]

When asset \((A)\), protection \((P)\), threat \((T)\) and situation \((Si)\)

The formula proposed that security requires a number of mutually inclusive components. For security to be considered there must be an asset \((A)\) to protect, that there is some person, organisation or community to provide a level of protection \((P)\) and a threat \((T)\) to the asset in a situation \((Si)\). Nevertheless, it is proposed that this formula does not provide a conclusive definition for security or assist in the presentation of a security body of knowledge. It is argued that security experts do use a rich knowledge structure, which can be extracted and defined as a consensual model. A view supported by McCrie, who stated that “the combination of industry-specific research and practices over the past generation has created a corpus of learning” (2004, p. 17).

Within the context of this study, security has to be considered within a commercial, organisational or private context for the protection of people, information and assets. This view is supported by ASIS International (2000), when indicating that organisational security management is a distinct field, separate from police or justice domains. Otherwise, with the breadth of applied security domains, there could be a divergence of
these distinct knowledge categories. Therefore, within the context of the study, security can be extrapolated as the scientific inquiry of organisational security management (ASIS International, 2003).

Within the Australia and New Zealand Standard Industrial Classification (ANZSIC) structure, the security industry is not classified as one industry; rather its members are spread across many associated industries that include many occupations. There also are omitted occupations including security technicians, security sales personnel, security clerks and security trainees (Tate, 1997). Designated in this way, occupational heterogeneity may lead to additional problems for the industry, primarily the ability of domain experts to effectively deal with conceptual change. According to Zeitz “experts respond poorly to conceptual changes to the domain, such as changing the rule of play or in processing stimuli which violate the principles of the domain” (1997, p. 47), resulting in inflexibility and a poor ability to define representation. To reduce conceptual change, security should not necessarily be defined by concept, but rather by the context of the application (Manunta, 1999). Therefore, it could be claimed that a robust and sound body of knowledge may lead to the ability to define security through both concept and context.

2.4.2 Security knowledge structure

The traditional entry into the security industry are by those seeking a second career after retirement from active service in the military or police (ASIS International, 2003). However, a second career approach may not be effective in providing the industry with an appropriate security knowledge base. Today a security professional, within organisational security, should have expertise in management, risk management, loss prevention, be technically capable (Simonsen, 1996) and understand security principles. However, there is still an imperfect knowledge structure (Tate, 1997) and academic research into security. An ad hoc approach leads to the “existing body of knowledge [which] lacks the overall vision that may only come from a genuine academic approach” (Manunta, 1996, p. 236), as the “role of academia is to provide the skills and knowledge needed for a professional practitioner, as well as to research, question and to teach
principles and concepts of the discipline” (Hesse & Smith, 2001, p. 89). In contrast McCrie (2004) opposed this view, when claiming that security specific research and practices over the past generation has created a body of knowledge, which has been categorised into functional categories. While this view is valid, appropriate categorisation requires concept definition within the security context.

A major problem arises in that if there is no consensual definition of security, how can there be valid development of curricula? Most tertiary level security courses have been developed from police, justice or crime prevention paradigms (Smith, 2001b; Tate, 1997), which according to ASIS International (2003) should be separate and discrete from security. Using neighbouring domain experts may lead to courses that are contain allied domain knowledge and are inappropriate for the security industry (Dolahenty, 2000). As a Western Australian Government Report found, the security industry has no integrated career structure (Tate, 1997), an issue that increases the lack of domain cohesion within the industry for practitioners and educators.

Security “clearly needs specialized [sic] professional training and universal recognition as an academic discipline” (Simonsen, 1996, p. 229). There is a lack of academic undergraduate level security programs, with most focused on criminal justice, crime prevention or risk management (Manunta, 1996). Fortunately today this proposed lack of academic security programs has changed. Davidson (2005) claims that there are now more than 300 2-year and 4-year institutions that offer some level of security course. The United States Department of Homeland Security has included US$70 million in 2004 to develop multi-disciplined areas of university research to support the department’s mission statement (School of Engineering, 2004).

Security “is not merely a matter of intuition or common sense: it involves a complex body of knowledge, analytical abilities, and know-how” (Simonsen, 1996, p. 229). According to Smith, security knowledge is being established through the development of appropriate domain concepts (2001a). This view is supported by Simonsen who stated that the “body of knowledge of security has grown rapidly in the past decade” (1996, p.
In 1993, “security science borrowed heavily from established disciplines to acquire the conceptual structures of knowledge necessary for the internal logic of this emerging applied science” (Smith, 2001a, p. 32).

As proposed by McCrie (2004), today there is an established body of knowledge in security, which may be demonstrated through the “continuing demand for publishers and academic institutions for texts that are security pure and refereed journals that will publish intellectual research and writing about all aspects of security” (Simonsen, 1996, p. 230). “Security management has developed to the point where it deserves recognition as a free-standing management science” (Simonsen, 1996, p. 229) and is a discrete field of academic study (ASIS International, 2003).

However, security cannot be considered a discipline in its own right because a field of inquiry requires its own theories and methodologies to be considered a discipline (Novak & Gowin, 1984). As Tate stated, “industry members will be well versed in industry operations, but they will not necessarily have an overview or have developed strategic concepts” (1997, p. 11). Nevertheless, the security industry, security associations and academia are beginning to develop security knowledge structure, though a forum of cooperation.

One area of progression in the development of security knowledge structure is the ASIS practitioner/academic symposia (American Society for Industrial Security, 1999; ASIS International, 2003). An outcome of these symposia was the development of a consensual security model containing the core element of security, which was to provide a baseline for tertiary level course development (ASIS International, 2003). According to Gilmore (cited in ASIS International, 2003) there has been three significant achievements from the symposia – the Body of Knowledge Task Force, Security Education and Career Study (ASIS International, 2005) and an edited textbook (McCrie, 2002).
The 2000 ASIS practitioner/academic symposium attempted to develop knowledge category descriptors for each of their proposed common elements of security (Table 2.2), defined in the 1999 symposium. An objective of the symposium was a consensus based model containing the primary knowledge categories, presented as concepts (American Society for Industrial Security, 2000).

Table 2.2

ASIS Common knowledge categories of security model

<table>
<thead>
<tr>
<th>Security</th>
<th>Physical security</th>
<th>Personnel security</th>
<th>Information systems security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Risk management</td>
<td>Legal aspects</td>
<td>Loss prevention</td>
</tr>
<tr>
<td></td>
<td>Legal aspects</td>
<td></td>
<td>Investigations</td>
</tr>
</tbody>
</table>

(American Society for Industrial Security, 2000, p. 87)

Core knowledge categories, developed from the ASIS symposium (2000), resulted in the participants proposing a revised model (Table 2.3). The revised common knowledge categories increased from a previous nine concepts to 18 concepts. Further symposia focused on defining these common knowledge categories, defining generic core competencies (American Society for Industrial Security, 2002) and commencing on the development of a security body of knowledge (ASIS International, 2003).

Table 2.3

ASIS Revised common knowledge categories of security model

<table>
<thead>
<tr>
<th>Security</th>
<th>Physical security</th>
<th>Personnel security</th>
<th>Information systems security</th>
<th>Investigations</th>
<th>Loss prevention</th>
<th>Risk management</th>
<th>Legal aspects</th>
<th>Emergency/contingency planning</th>
<th>Fire protection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Crisis management</td>
<td>Disaster management</td>
<td>Counterterrorism</td>
<td>Competitive intelligence</td>
<td>Executive protection</td>
<td>Violence in the workplace</td>
<td>Crime prevention (general)</td>
<td>CPTED</td>
<td>Security architecture and engineering</td>
</tr>
</tbody>
</table>

(American Society for Industrial Security, 2000, p. 100)
In contrast, Hesse and Smith (2001) proposed four knowledge categories appropriate for tertiary security education – security, business and management, computing and IT, and generic (Table 2.4). It was postulated that through academia, these knowledge categories would provide security managers with core knowledge for appointment in the security industry. While these knowledge categories were appropriate for generic supervisory or managerial occupations, they did not necessarily incorporate all security knowledge categories proposed by ASIS International (2003).

Table 2.4

<table>
<thead>
<tr>
<th>Security knowledge categories</th>
<th>Business &amp; Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Law</td>
<td>Law</td>
</tr>
<tr>
<td>Threats</td>
<td>Management theory</td>
</tr>
<tr>
<td>Security technology</td>
<td>Technology</td>
</tr>
<tr>
<td>Security theory</td>
<td>Business</td>
</tr>
<tr>
<td>Risk management</td>
<td>Accounting</td>
</tr>
<tr>
<td>Technology</td>
<td>Cultural knowledge</td>
</tr>
<tr>
<td>Investigative procedures</td>
<td>Industrial relations</td>
</tr>
<tr>
<td>Security equipment</td>
<td>HRM</td>
</tr>
<tr>
<td>Physical security</td>
<td>Contract management</td>
</tr>
<tr>
<td>Security standards</td>
<td>Duty of care</td>
</tr>
<tr>
<td>Life safety systems</td>
<td>Equal opportunity</td>
</tr>
<tr>
<td>Cultural knowledge</td>
<td>Ethics</td>
</tr>
<tr>
<td>Asset protection</td>
<td>Fraud</td>
</tr>
<tr>
<td>Intelligence</td>
<td></td>
</tr>
<tr>
<td>Duty of care</td>
<td></td>
</tr>
<tr>
<td>Fraud</td>
<td></td>
</tr>
<tr>
<td>Security perception</td>
<td></td>
</tr>
<tr>
<td>Surveillance</td>
<td></td>
</tr>
<tr>
<td>Generic</td>
<td>Computing &amp; IT</td>
</tr>
<tr>
<td>Analytical</td>
<td>IT systems</td>
</tr>
<tr>
<td>Research</td>
<td></td>
</tr>
</tbody>
</table>

(Hesse & Smith, 2001, pp. 98-99)

A collaborative project between the Attorney-General’s Department, Australian Standards and the Australian security industry attempted to identify and clarify requirements for future security standards. The project, funded by the Australian Federal Government, solicited and received comment from across the critical infrastructure protection network, both private and public. As part of the outcome, the project
developed an initial integrated security framework model (Figure 2.7), broken into five knowledge categories considered at four operational levels. The five knowledge categories consider IT and computing security, physical security, identity management and access control, procedural security and personnel security (Bazzina, 2006, pp. 85-86).

![Figure 2.7 Integrated security standards framework model](Adjusted from Bazzina, 2006, p. 85)

Reflection upon the ASIS common knowledge categories (Table 2.3), the security framework (Figure 2.7) could be considered broad in approach and therefore difficult to operationalise. Further criticism of the integrated security framework model included failing to align with the complex approach from the Australian Commonwealth Protective Security Manual (Bazzina, 2006) and not considering risk management. A further Standards Australia Security Standards Framework was proposed, rectifying these criticisms by encapsulating overall governance and management of the organisation, with risk management embedded within physical security, information security and personnel security (Bazzina, 2006).

After consultation with industry and government, the Risk Management Institution of Australasia developed a Security Risk Management Body of Knowledge publication. Although focused on security risk management, the document represented practice
areas, such as *protective security, people security, physical security, information security*, and *information and communications technology* (ICT) security. In a unique approach, information security and ICT were presented as discrete and separate knowledge areas. Information security was considered to be the protection of information, whereas ICT was considered to be the protection of information technology systems. Consideration was made that a principles-based approach should be taken by categorising security into practitioner areas (Risk Management Institute of Australasia, 2007b), an approach put forward by Manunta (1999).

The view that security risk management is an ordinate knowledge category may be opposed, as according to Manunta “there are a number of ontological discrepancies between the concept of security and that of risk, which deserve further study and investigation” (2002, p. 43). In addition, the majority of security knowledge categories discussed above presented risk management as a subordinate concept of security (ASIS International, 2003; Hesse & Smith, 2001), whereas the Risk Management Institution of Australasia (2007b) considered security risk management as the prime security category. This debate can only further assist the development and presentation of an overarching consensual security body of knowledge.

Finally, there is a number of scientific-based security texts that provide security knowledge. Some of the more used text, demonstrated by their continual editions and expansive use, include *Introduction to Security* (Fischer & Green, 2004), *Protection of Assets Manual* (Walsh & Healy, 2004), *The Design and Evaluation of Physical Protection Systems* (Garcia, 2001) and from an Australian perspective, *AS/NZ4360 Risk Management* (Standards Australia, 2004a). In addition, there are a number of international scholarly journals, which assist in propagating security research. These journals include the *Journal of Security Administration, Security Journal, Security Education Journal* and *The CPTED Journal*, to list a few.

A security body of knowledge is being developed, demonstrated by a number of significant industrial, academic and government organisations working toward this goal.
A number of core knowledge categories continue to be presented, such as personnel security, physical security, IT and computing, security technology and risk management (as shown in Figure 2.7). These core knowledge categories are leading to a degree of consensus in a number of security knowledge categories. However, as demonstrated by ASIS (2003) in their common knowledge categories (Table 2.3), much of this development work does not consider the breadth and depth necessarily to define the security body of knowledge.

2.4.3 Security education
There has been a demand for security education since the 1950’s (Fischer & Green, 2004). In a West Australian Department of Training report into the training needs of the security industry, Tate (1997) raised a number of key findings regarding the educational needs of the industry, such as restricted government occupational classification, no national peak association, limited career structure, fragmented education and no independent academic discipline. However, security education has an excellent future considering the indicated industry growth (Fischer & Green, 2004), although according to Manunta (1999) academia is content to continue to discuss security without definition.

In the United States there has been courses in security for many years, however, in general only at the vocational level (Fischer & Green, 2004). Similarly Tate (1997) observed that vocational education appears to be well established with many courses in guarding, investigation, risk, lock-smithing, and the electrical and electronic trades. The Australian study by Tate (1997) identified 109 security courses and 94 short courses, excluding in-house or propriety courses. These courses were targeted in support of base entry personnel and to meet and satisfy legislative requirements. Nevertheless, Fischer and Green did state that “only 50 percent of states [US] had imposed any training standards ... and that training for private security personnel is less than adequate” (2004, p. 90). These courses are still considered basic, fragmented and limited, with each sector of the industry having their own training body.
When developing a tertiary level security course, Smith stated that there was “no formal discipline in security science [that] was accessible, so that the conceptual structures on which to build a curriculum was not available” (2001a, p. 32). Therefore, there is a clear need for training and educational research to map core competencies standards (Tate, 1997). While there may be an expectation that personnel in academia will provide appropriate security courses, the lack of self-understanding in security (Horvath, 2004; Manunta, 1999) makes this difficult to be effectively achieved. As Dolahenty stated, tertiary “lecturers are flying blind and designing courses as they go” (2000, p. 31). This view was supported by a study into the development of an industry-based security curriculum, in where only tertiary institutions had developed educational security programs in their areas of expertise and markets (Hesse, 1999). The only effective method would be for industry to articulate with academia (Fischer & Green, 2004), as has already been demonstrated by a number of academia and security industry associations linkages (ASIS International, 2003; Kidd, 2006).

Tertiary security education is one area where development is most required as there are numerous vocational or associate degrees in security, however, little at undergraduate and postgraduate level (Simonsen, 1996). In contrast, Manunta stated that “more than 60 universities worldwide offer degrees, MSc and PhD in security matters” (1999, p. 63), although a large majority of these tertiary institutions offer only single units of study, part programs or are in related discipline areas that include information security, criminology, justice, policing, law, management or engineering. Indeed, as Fischer and Green (2004) noted, most security programs offered a criminal justice degree. In addition, ASIS (2005) stated that security has a business function and is not a subset of criminal justice. Consequently, students should pursue courses in security management, business, terrorism studies, emergency management, or personnel and information management.

Both ASIS and the Security Institute (UK) actively encourage tertiary educators by presenting their security courses in their publications. ASIS publishes a comprehensive listing of academic institutions that offer tertiary level security courses, with the most
recent updated in March 2007 (ASIS International, 2007a). The publication lists 113 tertiary courses in the United States and an additional six international courses offered in Australia, Brazil, Canada and the United Kingdom. ASIS supports the course listing publication and also provides an additional publication that presents career opportunities in the security industry, discussing academic programs in security (ASIS International, 2005).

The Security Institute publishes a yearly directory of qualifications (Kidd, 2006) that includes both tertiary institutions and private vocational trainers. Unlike the ASIS publication, the 2005 Security Institute publication contains far fewer tertiary courses, with eight from the UK and two international, and 17 private vocational training organisations (Kidd & Mountain, 2005). However, neither ASIS nor the Security Institute (UK) judge, accredit or endorse any of these programs, contrary to other disciplines in engineering and medicine. ASIS only lists security programs, not those involved with criminology or justice programs unless they have a security speciality (ASIS International, 2007a).

As an applied discipline, security has begun to develop a body of knowledge in both undergraduate and postgraduate tertiary programs (American Society for Industrial Security, 1999; Smith, 2001b), though the core of these programs is the undergraduate security degree course. Due to the diversity of security (ASIS International, 2005) the content and structure of the courses vary, however, the course must be appropriate for organisational security otherwise the degree course will not be embraced by the security industry and therefore not survive.

Tertiary level research and education will develop security specific concepts, theories and principles as evidence by the US Department of Homeland Security “engaging the academic community to create learning and research environments in areas critical to homeland security” (School of Engineering, 2004). Currently, four tertiary institutions have been selected and given grants of US$13million each, with each forming a research centre whose missions are to improve national security through the development and
application of tools for managing risks and consequences of terrorism (Greenemeier, 19 January 2005). As Smith stated “security education research in security … will evolve the paradigms, principles, models and theories of the emerging discipline, with the formulation of a stable knowledge structure” (2001a, p. 36). In addition, it is important to map these security concepts, with supporting propositional relationship, enabling the security industry to develop a better insight into the knowledge structure of organisational security and assist security educators.

2.4.4 Security associations

Industry associations that self-regulate their members may, to a degree, show industry professionalism (Penzarella & Cook, 1998); however, as with the security industry itself, the security industry associations are fragmented and diverse, and generally only represent one sector of the industry. The diversity of security associations may be demonstrated by the current active associations within Australia (Table 2.5). Such fragmentation increases the inability of associations to provide cohesion, leading to a lack of policy direction (Tate, 1997). The drive of most security associations appears to be in the development and delivery of vocational training, rather than tertiary education (Manunta, 1996).

<table>
<thead>
<tr>
<th>Active Australian security associations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Management Institution of Australian</td>
</tr>
<tr>
<td>Victorian Security Institute</td>
</tr>
<tr>
<td>Institute of Security Executives</td>
</tr>
<tr>
<td>Australian Institute of Professional Intelligence Officers</td>
</tr>
<tr>
<td>eSecurity Innovation and Awareness (SECIA)</td>
</tr>
<tr>
<td>Facility Management Association</td>
</tr>
<tr>
<td>International Assoc. of Bomb Technicians and Investigators</td>
</tr>
</tbody>
</table>

(Security Professionals' Congress, 2007; Security Professionals' Taskforce, 2008)

According to Tate (1997), as an emerging industry security has to establish a federal industry representative body to provide national policy and leadership. However when
reviewing Australia’s security bodies, each state has at least one or more industrial bodies representing only local sectors of the security industry, with linkage to their own representative and training body (Tate, 1997). Consequently, this leads to opposing strategies and an inability to provide leadership, thereby maintaining the disjointed nature of the security industry. This view was held by the National Academic Consortium for Homeland Security (n.d), in the desire to promote the development of better-informed public policy and strategy regarding national security issues.

There are a number of significant security associations operating in Australia, perhaps the most prominent being ASIS International. ASIS was founded in 1955 and has a current approximate membership of 35,000 and 205 chapters worldwide. There are currently three chapters in Australia, located in New South Wales, Victoria and Western Australia. ASIS advocates the role and value of security management and its members to government, private organisations, media and the public (ASIS International, 2007b). ASIS promotes and self administers three certified programs in security, with the aim to “meet stringent, internationally accepted requirements for education, experience and examination” (ASIS International, 2005, p. 6). The Australian Security Industry Association Ltd (ASIAL), founded in 1969, was formed by members of the industry in an attempt to “force shady operators out of the business” (Cowan, 1999, p. 1). In 1999, ASIAL had 2,500 corporate members (Cowan, 1999) and represented approximately 85% of the Australia security industry (ASIAL, 2007), although this considers only electronic installers and monitoring sector.

Other associated security bodies include the Australian Institute of Professional Intelligence Officers (AIPIO), founded in 1990 primarily for intelligence professionals. Their charter is to foster professionalism and comprised approximately 150 members. AIPIO holds an annual intelligence conference and publishes a related journal three times a year (Australian Institute of Professional Intelligence Officers, 2006). The Risk Management Institute of Australasia (RMIA), although not a specific security industry association, does actively promote co-operation between disciplines such as safety, health, education, fire, finance, security and other industries (Risk Management Institute

The Australian Information Security Association (AISA) was founded in 1999 to promote awareness and understanding of information security. AISA currently has approximately 600 members across most Australian states and territories (Australian Information Security Association, 2005). The Institute of Security Executives (ISE) was founded in 1966 and has approximately 900 members, although the institute is only active in two Australian states or territories, such as New South Wales and the Australian Capital Territory (Institute of Security Executives, 2006). Another Australian state-based association is the Security Agents Institute of Western Australia (SAIWA), established in 1978 with a mission to provide leadership in the provision of loss and crime prevention (Security Agents Institute of Western Australia, n.d).

The list of security associations operating in Australia (Table 2.5) indicates that there are some 11 associations, either directly or indirectly involved with the security industry. The listing demonstrates the diversity and breadth of the security industry, nevertheless, the list is not comprehensive. All security associations appeared to have one common goal to promote improved standards and professionalism in the security industry (Security Agents Institute of Western Australia, n.d). As security associations continue to develop and solidify, they will likely provide industrial cohesion, be instrumental in defining organisational security, and provide consensus in the presentation of a security body of knowledge.

2.4.5 Security conclusion

Security has a variance of definition dependant on applied context, both within society and the security industry. The Australian security industry is valued at over A$4.3billion (McKeague, 2006), with recent world events raising social concern over the ability of society to protect itself. This concern has led to political intervention, further merging the distinction between many aspects of security, whether private security, national
defence, homeland security or policing. Security does require an item, object or thing to have a degree of value and that someone or something will use a resource to protect that item. Within the context of the study, security was considered to be organisational security.

The security industry is diverse, cross-disciplined and multi-skilled, although the industry does contain organisational security experts. This expert knowledge structure may be extracted and defined to not only further the development of a singular definition, moreover to present expert knowledge structure and a body of knowledge. The industry has commenced the development of a body of knowledge, through industry associations, tertiary institutions, and national and international documents. The body of knowledge is still most diverse, emulating the industry. Nevertheless, a number of core knowledge categories appear to be consensual, which includes physical security, personnel security, risk management, emergency management, security technology, and information technology and computing.

Tertiary education is assisting the development of a security body of knowledge, although it can be proposed that academia cannot define security any more effectively than the industry itself. General security education has been offered since the 1950’s, but only at the vocational level. Today some researchers consider that there is a wealth of tertiary education although others disagree. What is considered important is progressive research in specific security theories, concepts and principles.

Security associations reflect the situation of tertiary education – the many industry associations are as diverse as the industry. In addition, associations reflect their members, leading to an inability of these associations to provide leadership, policy, education and professional development. As the Australian context demonstrates, there are 11 active security industry related associations. Nevertheless, it is proposed that as security associations continue to develop and solidify, that they will provide industrial cohesion, be instrumental in defining organisational security and provide consensus in the support of a security body of knowledge.
2.5 Concluding the review of literature

This chapter has presented aspects of knowledge categorisation, concept mapping and the security industry. In the first two-parts of the literature review the theoretical frameworks of knowledge categorisation and concept mapping supporting the study were discussed. Within the context of cognitive psychology, knowledge structure and memory categorisation was considered. In addition, how knowledge may be categorised and expert knowledge structured, with the explanation view considered the primary knowledge categorisation theory informing the study.

Within the context of cognitive psychology, knowledge structure and categorisation considered memory, how knowledge may be categorised and expert knowledge structure, with the explanation view considered the primary knowledge categorisation theory informing the study.

Concept mapping, as described by Novak (1990), provided a method to represent expert knowledge structure within a spatial format. In addition, and to address the research questions, the integration of multidimensional scaling to develop and present concept maps was extended beyond Novak’s method of concept mapping. This integrated approach allowed consensual expert concept maps of knowledge to be developed and presented in this thesis.

Finally, the security industry was discussed – presenting a definition of security within the context of the study, considering the breadth of the security industry, research into the knowledge structure of security, tertiary security education and relevant Australian security associations. The security industry was considered to be multi-disciplined and despite the diverse nature of the industry, organisational security is beginning to develop a body of knowledge.
CHAPTER 3
MATERIAL AND METHOD

3.1 Introduction

The materials and methods supporting the study, including study design, population, research instruments, research methodology, study limitations and ethical considerations are described in this chapter. The study design provides an overview of the interpretive research, presenting the four phases and supporting objectives. Discussion of population considers the methodology used in the sample selection, followed by the two research instrument’s design and construction. The research methodology presents multidimensional scaling (MDS) and interview techniques as the means to identify and construct knowledge. Concept mapping and MDS provided a method of inquiry to develop and model the security risk management knowledge structure. Finally, limitations and ethical aspects of the study are considered.

3.2 Study design

In this study, an interpretive (Moules, 2002) research methodology was employed such that the research questions could be addressed in a sequential manner within the phases of the study. The interpretive view considers that science should be both robust and rigorous; however, humans differ from inanimate objects and from each other. Therefore, it is necessary to begin with individuals and understand their interpretations of their world, that “theory is emergent and must arise from particular situations” (Cohen, et al., 2002, p. 23).

The interpretive research approach supported the study design, as each phase of the study informed the subsequent phase. The study was designed as four distinct phases, with predetermined research questions and phase objectives. Security knowledge categorisation (Phase 1) commenced the study, followed by MDS knowledge structuring (Phase 2). Expert knowledge structure validation (Phase 3) was then completed, with a final comparative and interpretation stage (Phase 4). These two final phases applied expert interviews and the development of assertions, a method most suited to
interpretive research (Cohen, et al., 2003). This sequential methodology of the study supported the informing approach, providing a final reflection phase.

Interpretive research allows the initial inductive development of assumptions – or assertions – in order to respond to research questions (Cohen, et al., 2002; Merriam, 1988). Assertions may be considered “a positive statement, usually without evidence” (Angus & Roberston, 1992, p. 55). However, according to Erickson (1986) assertions may be formed from either the review of data corpus or the development of an evidence chain – developed by the researcher having considered the data corpus, patterns of generalisation, linkage between data and with informed induction. As the study developed, resource data were collected and analysed, leading to the formation of assertions – “that frame and interpret the data” (Treagust, Jacobowitz, Gallagher & Parker, 2001, p. 142). Data resources for this study included the extracted security categories and subordinate concepts (Phase 1), development and presentation of the psychometric MDS security risk management concept map (Phase 2), the expert interviews (Phase 3) and the final comparative phase (Phase 4). The proceeding Phase one and Phase two of the study allowed assertions to be formed for Phase three and four.

Data that tested the validity of assertions must attempt to support or deny assertion evidence (Thiele & Treagust, 1994). This evidence may be subtle and inconclusive, with some evidence more robust than others; nevertheless, discrepancies in data must be returned for closer examination – essential for inquiry. The aim of assertions is not to demonstrate conclusive causal linkage, moreover, appropriate evidence to support the assertion (Erickson, 1986). The use of assertions has limitations – the need to have substantial numbers of events, that rare events are not tested well and the ability of the researcher to demonstrate systematic evidence to support the assertion for an external reader (Erickson, 1986).

3.2.1 Phase one: Knowledge categorisation

Security knowledge categorisation required the investigation and critique of national and international tertiary undergraduate security courses. Course selection was initially
based on the use of security-related concepts within the titles of the courses offered, with further reduction to consider content. Once appropriate undergraduate security courses were selected, supported by security experts, the course structures were analysed and concepts extracted and tabulated. Concept extraction used Linguistic Inquiry and Word Count (LIWC) text and content analysis (Pennebaker, Francis & Booth, 2001). LIWC operates by comparing words from an internal dictionary of more than 2,300 words categorised into 70 hierarchical dimensions against the text document (Collins, Carey & Smyth, 2005; Mehl & Pennebaker, 2003). LIWC was “chosen because of its proven success with such analysis in general” (Self-continuity warranting practices, 2003, p. 96), however within the study its full linguistic analysis capability were not used. According to Collins, et al. (2005), the reliability and validity of LIWC has been established.

Basic linguistic dimensions were tested including word frequencies, words per sentence, word position and related concepts (Cassell & Tversky, 2005; Collins, et al., 2005; Fresno & Ribeiro, 2004; Hiemstra, 1996; Pennebaker, et al., 2001), although these dimensions should not be used separately (Fresno & Ribeiro, 2004). Based on text and content analysis, concept categories were able to be extracted and defined (Pullman, McGuire & Cleveland, 2005). Expert opinion from four security experts were sourced to support the concept categorisation (Cohen, et al., 2002). In addition, using convergence (see Table 5.1) between the extracted security concept list, AS4360:2004 Risk Management Standard (Standards Australia, 2004a), Pilot Study results (see Chapter 4) and the four security experts, concepts were incorporated into the security risk management category. Phase one analysis enabled the operationalism of the security knowledge categories, the presentation of the security concept list and inclusion of these concepts into the knowledge category of security risk management.

3.2.2 Phase two: MDS knowledge structure
The second phase, MDS knowledge structure, used the MDS survey instrument with the embedded knowledge category of security risk management and supporting subordinate concepts. Expert security risk practitioners and academics – a total of 29 respondents –
completed the MDS survey instrument to elicit underlying MDS dimensions. The study used the MDS ALSCAL algorithm, which can analysis both metric and non-metric input data and produce spatial representation (Cox & Cox, 2000; Tull & Hawkins, 1993). From the MDS ALSCAL two-dimensional spatial presentation, a security risk management knowledge structure and concept clusters were presented. With the support of a further five security experts and academics, concepts had propositional linkages and supporting statements inserted to produce the psychometric MDS security risk management concept map.

3.2.3 Phase three: Expert knowledge structure validation
The third phase, expert knowledge structure validation, presented the psychometric MDS security risk management concept map to six security experts (see Chapter 7.3 for a description of each expert). Through semi-structured interviews, which were audible recorded and transcribed, each respondent’s opinions on the concept map were analysed and interpretations made. Subtle non-verbal language was also noted and inserted into transcripts. Resource data were identified and organised into assertions, which were developed to support the research questions.

The assertions were supported by commentary evidence presented in particular descriptive, general descriptive and interpretive commentary (Erickson, 1986). Particular descriptions provided events and instances, general descriptions provided patterns in the data and interpretive commentary showed connections between details and the more abstract ideas. Evidence within this phase used narrative vignettes and direct quotes taken from the expert interviews.

3.2.4 Phase four: Expert validation of the psychometric MDS concept map
Finally, the previous Phase two and Phase three outcomes were compared and contrasted. Comparison facilitated data triangulation (Cohen, et al., 2002) between the psychometric MDS security risk management concept map and expert opinion of the structure. Again, assertions were identified and organised to support or refute the research questions. The primary objective of Phase four was to quantify the
appropriateness of the psychometric MDS analysis technique to develop and present knowledge structures to support the development of psychometric concept maps within the context of the study.

3.2.5 Two-staged study: Pilot study

In addition, the study applied a two-stage approach, with the first stage being the completion of a pilot study (Chapter 4) and the second, being the primary study. The pilot study assessed the suitability of the research methodology and instruments when each phase of the pilot study was complete. Study improvements included the instrument format, inclusion of expert opinions in the Phase two psychometric MDS concept map structure, predefined category concept number and the development of assertions to support or refute the research questions. At this stage, the instruments produced an acceptable reliable and valid measure at each pilot study phase, supporting the decision to take the study to the primary stage. Once the pilot study was completed and improvements made, the primary study was completed.

3.3 Population

The target population was security industry practitioners or academics who could be considered by their peers as experts. Within the study, security expert was defined as a member who has been working in the industry for longer than nine continuous years, with three years at a significant and responsible employment position. This definition corresponded to the ASIS International definition for eligibility as a Certified Protection Professional (ASIS International, 2004).

To achieve a statistically valid sample of the population, it had been claimed that there is a requirement for ≥30 participants per research instrument cell (Fink, 1995; Leedy, 1989) or up to 100 participants per cell (DeVaus, 1992). Consideration has to be taken for possible variations in characteristics, with linear division throughout cells, although there has to be a compromise between sampling size, cost, accuracy and objectives of the study (DeVaus, 1992). However, MDS removed the need to apply a rationale approach to probability sampling (Trochim, 2005a) because MDS provides a summation
of cells and the instrument becomes a single cell or group (Borg & Gall, 1979). Therefore the primary factor in sampling size selection was the need for an appropriate MDS sample size. As Borg and Gall indicated, this approach resulted in the sampling size being selected from a work up approach (cited in Cohen, et al., 2002). Combined with non-probability dimensional sampling, this approach removed the need to define the sample size based solely on population.

Nevertheless, each phase of the study required a different population sample size, with the principle based on the MDS (Phase 2) sampling need. However, sampling size within each phase did consider the heterogeneity of the population and its experts. Heterogeneity was important to ensure that certain security expertise or industries were surveyed in equivalent proportion to the other (Cohen, et al., 2002) because some experts may only have expertise in their relevant areas. As mentioned, this approach was necessary because the security industry is diffuse and diluted across many industries (Tate, 1997).

Phase one necessitated the review and analysis of all undergraduate security courses offered at the tertiary level in Australia, Canada, New Zealand, United Kingdom, United States and South Africa, with 104 courses being reviewed (see Chapter 5 and Appendix D). Analysis resulted in seven critiqued courses being selected, based on non-probability dimensional sampling and supported by expert opinion of content (Feltovich, Ford & Hoffman, 1997; Trochim, 2005a). The sample size was considered appropriate due to the method of selection and data extraction intent, even through the sample size was not a mathematical random sample of the population (Krejcie & Morgan, 1970).

Phase two MDS analysis involved 29 industry experts selected by non-probability dimensional sampling with consideration of heterogeneity. MDS requires a finite set of parameters, with estimates based on the number of object coordinates plus the number of possible weights. If this measure is large relative to the number of matrix data values, the result may be unreliable. Integrated with the number of parameters was the consideration of MDS stress (see Chapter 3.5.1). The minimum sampling size for MDS
analysis was considered to be 30 participants (Cohen, et al., 2002), supported by similar studies that had used MDS analysis (Cheng, 2004; Martinez-Torres, et al., 2005; Nagy, n.d.). The sample size was not increased, as increasing non-probability sampling may lead to an increase in possible sample bias (Kalton, 1983). Participants were selected from national and international cohorts.

Phase three expert interviews used non-probability purposive sampling, comprising six participants deemed by peers as security experts and with consideration given to the selection of domain experts. Some defined domain experts are not measurably expert performers; metric research has shown that domain specific experts are two standard deviations above the general domain population (Ericsson & Charness, 1997). According to Stein (1997), researchers have used ad hoc methods to select whom they believed were domain experts. As Ericsson and Charness summarised, “researchers cannot seek out experts and simple assume that their performance on relevant tasks is superior” (1997, p. 231). Another method may allow those within the domain to select whom they consider experts and are “recognised within their professional [sic] as having the necessary skills and abilities to perform at the highest level” (Shanteau, 1992, p. 252). The study applied the latter, using peer selected experts.

Finally, Phase four comprised a comparative study between the outcomes of Phase two and Phase three. Therefore, Phase four did not require discussion on population or sampling.

### 3.4 Instruments

Two research instruments used in the study were designed to be applied in Phase two and Phase three.

#### 3.4.1 Research instrument 1: Psychometric MDS concept mapping

Research instrument 1 was developed from the security risk management knowledge categories and subordinate concepts. The psychometric MDS concept mapping survey instrument (Appendix H) used paired concepts from the knowledge category of security
risk management. Experts indicated on a sliding scale which concepts they considered were related (similar) or unrelated (dissimilar). These measures were then averaged as a method to “identify and understand” group perceptions (Tull & Hawkins, 1993, p. 434).

Instrument validity was assessed through face validity and non-related concept measures, with face validity assessed by expert judgement. Reliability was tested using Cronbach’s Alpha measure. Markham, Mintzes and Jones claimed that the use of MDS increases the reliability of concept maps (1994), however, MDS Kruskal stress (STRESS1) and r-squared (RSQ) measures of fit were tested (Cox & Cox, 2000; Kruskal & Wish, 1978; Schiffman, Reynolds & Young, 1981). The pilot study (Sections 4.3 and 4.6) further tested and improved the primary study’s instrument validity and reliability.

3.4.2 Research instrument 2: Expert knowledge structure validation
The semi-structured expert interviews (Appendix I) was a paper-based analysis of the knowledge structure and spatial locality of subordinate concepts presented in Phase two, namely the psychometric MDS security risk management concept map. The interviews quantified the confidence of the security risk management concept map with expert judgement. One-on-one interviews, completed with the researcher and peer selected experts, were recorded and transcribed for focused analysis. The interview questions were initially based on the research questions, with the interview transcripts being further analysed for data patterns and assertions (Erickson, 1986).

Instrument validity was assessed through face validity and convergence, with face validity assessed by expert judgement. Reliability was maintained with pre-constructed response coding to maintain consistency and tested using expert judgement. The results of the pilot study (Sections 4.4 and 4.6) allowed further primary study improvements, resulting in increased instrumentation validity and reliability. In Phase four of the study triangulation was applied, which according to Campbell and Fiske was “a powerful way of demonstrating concurrent validity, particularly in qualitative research” (cited in Cohen, et al., 2002, p. 112). Triangulation provided validation between study Phase two
and Phase three, adding support to the outcome from the psychometric MDS concept map. In addition, with the interpretive research approach (Smith, 1991), the “strategy of returning to the subjects for validation [to] reproduce the original meaning of the subjects” (Allen, 1995, p. 179) supported validity.

3.5 Research methodology
Research methodologies considered the use of MDS and interview techniques as methods to extract and present expert knowledge structure. MDS provided the initial method of analysis, presenting the psychometric MDS concept map of security risk management and providing the study’s inquiry. Interview techniques tested the psychometric MDS concept map through expert case studies.

3.5.1 Multidimensional scaling
There are many psychometric techniques that may be used to extract concept maps, including MDS (Agrafiotis & Lobanov, 2001; Ding, 2003; Trochim & Cook, 1994), hierarchical clustering, latent partition analysis, smallest space analysis, Reuter’s method, Warren’s method, (Hoz, et al., 1997), linear structural relationships (LISREL) and trajectory mapping (Lokuge, et al., 1996). This study used MDS, as analysis resulted in a spatial representation of knowledge concept clusters (Trochim & Cook, 1994) and allowed an analysis of judgements between variables to define dimensionality between such variables (Cohen, et al., 2002).

MDS is a statistical technique within the area of multivariate data analysis, which has “attracted worldwide interest” (Cohen, et al., 2002, p. 369) and has been used in many studies (Cox & Cox, 2000). These studies include knowledge structure in the form of concept mapping (Cheng, 2004; Martinez-Torres, et al., 2005; Trochim, 2005b; Turner, 2002). MDS reduces complex dimensional data and presents these data as a spatial representation. The reduction in data complexity through presentation in dimensional space allows hidden data structure formation. This dimensional representation demonstrates object proximity, with proximity being how similar or dissimilar objects are or are perceived to be (Cox & Cox, 2000; Kruskal & Wish, 1978). Spatial
presentation supported concept mapping, in that concept clusters can be demonstrated. MDS also provides a moderate to good construct validity for concept mapping (Hoz, et al., 1997).

MDS commences with a set of objects, which are paired and their dissimilarities measured. The distances between pairs of objects are placed in a half matrix format. Configurations of points are sought in dimensional space, with each point representing an object. MDS calculates a dimensional space configuration where the points distance match, as close as possible, the paired dissimilarities. The variation in matching defines the different techniques or algorithms of MDS (Cox & Cox, 2000). There are many MDS algorithms dependant on research requirements and associated data, including ALSCAL, INDSCAL and KYST. The study used ALSCAL (Alternative Least squares SCALing). According to Cox and Cox (2000) the benefit of ALSCAL is that analysed data may be nominal, ordinal, internal or ratio, allow missing or incomplete object measures, be asymmetric or symmetric, be unconditional or conditional and continuous or discrete, making this algorithm versatile. The MDS ALSCAL algorithm (3.1) is presented below:

\[
\delta_{re} = \left\{ \sum_{i} (x_{ri} - x_{si})^2 \right\}^{1/2}
\]

MDS requires a total number of parameters, with estimates based on the number of object coordinates plus the number of possible weights. If this measure is large relative to the number of data matrix values, the result may be unreliable. MDS requires a finite data set to precisely estimate the values of the parameters. Integrated with the number of parameters is the consideration of the stress measure. Stress is the goodness of fit and as a measure, indicates how far the data departed from the best possible fit (Schiffman, et al., 1981). A stress measure of zero may imply perfect modelling data by achieving a perfect dimensional space configuration.
There are several methods to measure MDS stress, with a common measure being Kruskal’s stress, often referred to as STRESS1. According to Cox and Cox (2000), STRESS1 is the preferred measure for MDS goodness of fit. Each iteration results in a stress value and it is important to ensure that improvements ($\leq 0.001$) can be made with proceeding iterations. ALSCAL also provides an R-squared measure of fit, interpreted in a similar manner to STRESS1 and reflective of the proportional variance to the measure of fit (Tull & Hawkins, 1993). The study used both STRESS1 and R-squared (RSQ) measures of fit. The MDS STRESS1 algorithm (3.2) is presented below:

$$S = \sqrt{\frac{S^*}{T^*}}$$

When $S^* = \sum_{r,s} (d_{rs} - d_{rs})^2$ and $T^* = \sum_{r,s} d_{rs}^2$.

In general, increasing dimensionality will cause a decrease in stress (Schiffman, et al., 1981). STRESS1 is related to the number of objects or subjects [I] and represented dimensionality [D]. A rule of thumb put forward by Kruskal and Wish (1978) was that $I>4D$ to reduce sensitivity of STRESS1. Based on a two-dimensional psychometric MDS concept map, an approach that defined the minimum number of knowledge category subordinate concepts.

MDS dimensionality can elicit hidden characteristics, although this was not a measure used in the study. Dimensionality is interpreted through lines in space, ideally at right angles to each other to facilitate description (Kruskal & Wish, 1978). Interpretation can be difficult and may require implicit understanding because determination of dimensions can be subjective (Tull & Hawkins, 1993). Nevertheless, MDS was used within the study to elicit underlying concept clusters developed from the summation of individual experts. This approach allowed demonstration of expert knowledge concept clusters within multiple dimensions (Markham, et al., 1994), without any pre-determined interpretation of spatial locality (Turner, 2002). Ohanian (cited in Stein, 1997) supported this view, stating that expertise can be measured as a construct that contains multiple dimensions.
Experts use a greater level of abstract processing, complexity and interpretation in their use of knowledge concepts, whereas novices only consider surface level knowledge (Zeitz, 1997). As mentioned previously, this approach allows experts to link abstract concepts to resolve similar problems, unlike a novice who attempts to find a sequential solution. Therefore experts are most likely to cluster implicitly similar concepts together and unlike concepts apart. It can be argued that MDS provides a suitable psychometric methodology to construct and present consensual concept maps (Markham, et al., 1994). However, MDS does not provide the holistic concept mapping relationship of knowledge structure, as it can only elicit and demonstrate knowledge clusters. Therefore, additional analysis has to be applied and expert interviews provided this additional information.

3.5.2 Interviews
Concept maps may be developed through interviews, which allow researchers to gather knowledge that may not be achieved through other methods, permitting non-verbal communication to be analysed and elicitation of true meaning. As Cohen, et al. (2002) advised, interviews allow the measure of attitudes, how variable relationships may be defined and to validate other research methods. During an interview an expert can quantify understanding through diagrams, extracting the interviewees understanding of knowledge and justifying relating propositions.

Interviews may be structured, semi-structured or unstructured (Guilfoyle & Hill, 2002; Tan, 2000), although interview types can be expanded to include many more groups dependant on source (Cohen, et al., 2002). Structured interviews involve predefined questions, which are rigidly maintained. Semi-structured interviews involve predefined questions, however these may be open-ended or allow some diversion from the predefined sequence. The semi-structured format has the capacity to add new questions during the interview, while retaining a degree of structure. This semi-structured format also allows for a better comparative study design (Guilfoyle & Hill, 2002). Unstructured interviews involve open-ended questions that are guided in part by the response given by the participant.
Interview design and application should be structured to follow seven stages of investigation, such as thematising, design, interview, transcribing, analysing, verifying and reporting (Cohen, et al., 2002). Thematising should ensure that the interview will elucidate, elaborate and respond to the research questions (Guilfoyle & Hill, 2002), moreover, should also justify the methodology and theoretical basis for the interview. Interview design is the preparation of the interview type, format and content, with the interview being the physical and social interaction with the participant. Conversion of this physical and social interaction into written data requires transcribing, which may be a form of analysis and interpretation (Kvale, 1996). Analysis is the division of the social interaction into its constituent parts to examine relationships (The Angus & Roberston, 1992), which may take many forms dependant on the study and requires a degree of coding. Coding allows the researcher to identify patterns, elicit understanding, and define relationships and causality. These parts may result in meaning through frequency, patterns, themes, clusters, clarification, factors and relationships (Cohen, et al., 2002). Verification should validate the reliability and validity of the interview; reporting is the presentation and communication of the interview.

During an interview there are a number of issues to consider. These include, where possible, avoiding interruptions or distractions, asking unrelated or embarrassing questions, jumping between topics, giving advice or offering opinion, summarising to early, being superficial or handling sensitive matters poorly (Field & Morse cited in Cohen, et al., 2002). According to Guilfoyle and Hill (2002) there are some basic principles that improve semi-structured interviews – politeness, honesty, trust, empathy, interest, openness, empowerment, information sharing, making people feel at ease, encouragement, patience (Carr, 1996) and providing a suitable environment to challenge assumptions.

As discussed, an interview may elicit a participant’s understanding that other types of tests may not, due to the ability of the interviewer to confirm an answer dependant on response. Elicitation requires a thorough knowledge of the study, the research questions and study domain. However, there are disadvantages with interviews, including
interviewer bias, not extracting true opinion, subjectivity of analysis, costly and time consuming interview process, and the motivation of the interviewed (Cohen, et al., 2002). Semi-structured interviews with pre-constructed coding can increase reliability, as this leads to common understanding between interviewers. In contrast, Scheurich (1995) claimed that this may not necessarily be the case, as changes in semantics, environment and emphasises can result in each participant perceiving a slightly different question. As the interview is a social interaction, power may also cause reliability errors, as there may be a mismatch in the relationship of the interviewer and interviewee (Cohen, et al., 2002).

Interviews have been shown to demonstrate low validity, as participants make consistent errors in either overstating or understating measures (Cohen, et al., 2002). Validity errors can be expanded to include race, religion, gender, age, sexual orientation, social class and status, and appear to be widespread (Scheurich, 1995). A process to overcome these errors, to some degree, is the use of another measure to validate the interview, referred to as convergence validity. The study used psychometric MDS to provide a degree of convergence validity. In a similar study structured interview validity was tested, with supporting concept mapping and psychometric analysis. The study found that there were convergence between these types of tests, having demonstrated moderate results (Hoz, et al., 1997).

Within the context of the study, semi-structured interviews quantified the confidence of the knowledge categories and locality of subordinate concepts through expert judgement. Interviews determined the quality, interpretation and predictability of the participant’s concept mapping and indicated their understanding of concepts (Tan, 2000). As a psychometric MDS concept map was one of the required study outcomes, data were subsumed to allow clarification of key concepts (Cohen, et al., 2002) and propositions. Therefore semi-structured and coded expert interviews provided a number of distinct study benefits, particularly quantifying the outcome of the psychometric MDS concept map of security risk management.
3.6 Study limitations

The study had to consider a number of limitations. These limitations included semantic and conceptual understanding of concept definition, the reliability and validity of concept mapping, the non-probabilistic approach to sampling and the sample size, the structured approach in research instrumentation and the interviewing technique.

Semantic understanding of each concept definition may differ, particularly with complex and implicit knowledge categories. Variance may be due to perception, experience or diffuse level of conceptual understanding. Scheurich (1995) stated that each participant may perceive or interpret a slightly different question to the designer’s intent due to semantics, environment and emphases, resulting in comprehension error that cannot always be detected. In addition, participants may guess their response, further skewing understanding and resulting in alternative or incorrect presented concept maps. These errors may lead to reduced reliability and validity of psychometric MDS concept maps, indicated through a high MDS STRESS1 measure. However, continual testing of reliability and validity in the development and presentation of the psychometric MDS concept map with expert input reduced possible variance in definition.

A number of authors have raised concern about the reliability and validity of concept mapping (Hoz, et al., 1997; Markham, et al., 1994; Ruiz-Primo, et al., 2001), with a claim that concept mapping effectiveness should be considered before community exposure (Ruiz-Primo & Shavelson, 1998). Nevertheless, according to Trochim the “concept mapping process can be considered reliable … to generally-recognised standards for acceptable reliability levels” (1993, p. 1). The study’s design purposively incorporated data triangulation to measure and control the psychometric MDS concept map reliability and validity.

The study’s sample size was not based on a mathematical random population sample (see Chapter 3.3), due to the use of non-probability dimensional sampling. This sampling approach could have resulted in a psychometric MDS concept map that did not reflect the general security expert population, which continues to increase due to the
diversity of the security industry (Fischer & Green, 2004; McKeague, 2006). Nevertheless, a degree of population heterogeneity was incorporated in the study design and participation sample.

To develop and present the psychometric MDS concept map, data were collected by an instrument comprising defined comparisons of security risk management concepts. Participants selected what they believed were the most appropriate differences between these concepts. This type of ranking scale instrument has been used to measure a large number of participants’ conceptual understanding and compared to interviews, these tests are generally quicker to administer, score and analyse (Tan, 2000). As participants are guided by predefined questions this type of test may not elicit alternative concept maps, producing skewed maps and resulting in concept maps that do not define the participants’ full knowledge understanding or present all conceptual dimensions (Markham, et al., 1994).

The interviewer or research instrument may reduce reliability and validity through poor interviewing technique or instrument design. There are many considerations in the attempt to reduce these issues, however, one effective method was the completion of a pilot study (Chapter 4). A comprehensive pilot study, with analysis of reliability and validity throughout each study phase, ensured that the study was suitable for continuation to the primary study. In addition, each phase of the primary study incorporated a degree of measure to monitor and control reliability and validity.

3.7 Ethics
A number of ethical issues were considered to protect the study’s participants. It was a requirement that participation in the study be voluntary, that the researcher did not disclose identity, that an overview of the study was presented, that all participants were ≥18 years old and that written consent was given by the participant before proceeding. Participants involved in Phase three were informed that the expert interviews were to be audible recorded and express permission be granted.
During the survey’s there were no financial incentives offered. The researcher offered no bias, deception or opinion during any stage of survey. Participants were informed that they may withdraw from the study at any time. Also, completed surveys remained strictly in confidence, participants were not identified or the survey information released to any other person or organisation. Any changes to the research design that may have had ethical implications, unforeseen risk or could harm the participants were reported and the study halted. The research study complied with Curtin University of Technology ethics policy and procedures.

3.8 Conclusion
This chapter presented the study design, population, research instrumentation, research methodology, study limitations and ethical considerations. Study design discussed the four distinct phases of the study and how each of these phase’s supported discrete research questions. Population and non-probabilistic sampling were discussed, with justification for sample size based primarily on the statistical requirement of MDS ALSCAL. Nevertheless, each phase of the study did require different sampling size, based on various factors.

The two research instruments, implemented in study Phase two and Phase three, were described. Research instrument 1, psychometric MDS concept mapping survey, used the security risk management concepts and measured conceptual similarities. Research instrument 2, expert knowledge structure validation, was a semi-structured interview to measure expert opinion. The research methodology used both quantitative and qualitative techniques to extract and present the psychometric MDS concept map of security risk management. The combination of these methodologies was unusual, nevertheless each supported the other.

Psychometric MDS produced a spatial representation of knowledge concept clusters, allowing an analysis of judgements between variables to define dimensionality between such variables. Semi-structured expert interviews provided data triangulation between study phases and quantified the psychometric MDS concept map structure. However,
MDS could not provide the holistic concept mapping relationships, as MDS can only elicit and demonstrate knowledge clusters and dimensionality. Therefore, expert interpretation supported the psychometric MDS concept map relationship development and representation.

Study limitations were considered, including semantic and conceptual understanding of concept definition, concept mapping reliability and validity, the non-probabilistic approach to sampling and sample size, the structured approach in research instrumentation and the interviewing technique. To conclude the chapter, ethical considerations of the study were presented.
CHAPTER 4
PILOT STUDY

4.1 Introduction
The pilot study and resulting outcomes are described in this chapter. The pilot study was performed to assess the suitability of the research methodology and instruments. Each phase of the study was completed, including knowledge categorisation (Phase 1), MDS knowledge structure (Phase 2), expert knowledge structure validation (Phase 3) and finally, the comparative study (Phase 4) between the MDS knowledge structure and expert opinion of this structure. The pilot study used the knowledge category and subordinate concepts of security risk management, with three expert security participants. The pilot study’s reliability, validity and limitations are presented. Finally, the pilot study resulted in a number of modifications to both the primary study’s research methodology and research instruments.

4.2 Pilot study: Phase one Knowledge categorisation
Phase one required the critique and categorisation of tertiary security courses, to respond to Research Question one: What are the knowledge categories and subordinate concepts of security? Three West Australian University courses were chosen, due to their proximity to the researcher and their offer of security-related awards. Tertiary institutions included Curtin University of Technology, Edith Cowan University and Murdoch University (Table 4.1).

Table 4.1
Security and allied industry related West Australian courses

<table>
<thead>
<tr>
<th>University</th>
<th>Award</th>
<th>Qualification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Curtin University of Technology</td>
<td>BSc (Security Technology)</td>
<td>Bachelor Degree (Honours)</td>
</tr>
<tr>
<td>Edith Cowan University</td>
<td>BSc (Security)</td>
<td>Bachelor Degree (Pass)</td>
</tr>
<tr>
<td>Murdoch University</td>
<td>BA (Security, Terrorism and Counter-terrorism)</td>
<td>Bachelor Degree (Pass)</td>
</tr>
</tbody>
</table>
Course syllabi were sourced from each institution, and security categories identified and extracted using Linguistic Inquiry and Word Count (LIWC) (Pennebaker, et al., 2001). From the analysis of the security risk management category, draft subordinate concepts were tabulated (Table 4.2) by the researcher to emulate study Phase one. The 21 most frequently used concepts from the security risk management category, with selection based on LIWC, were integrated into the Phase two MDS knowledge mapping instrument.

Table 4.2

<table>
<thead>
<tr>
<th>Draft Security Risk Management</th>
<th>Duty of care</th>
<th>Modelling</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis</td>
<td>Experience</td>
<td>Network</td>
<td>Risk management</td>
</tr>
<tr>
<td>Assessment</td>
<td>Hazards</td>
<td>Probability</td>
<td>Statistics</td>
</tr>
<tr>
<td>Communications</td>
<td>Intelligence</td>
<td>Protective risk</td>
<td>Threats</td>
</tr>
<tr>
<td>Consequence</td>
<td>Judgement</td>
<td>Psychometric risk</td>
<td>Vulnerability</td>
</tr>
<tr>
<td>Cultural risk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decision-making</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.3 Pilot study: Phase two MDS knowledge structure

Phase two objectives were to develop the psychometric MDS concept mapping survey for the knowledge category of security risk management and subordinate concepts, responding to Research Question two: What is the expert knowledge structure and subordinate concepts of security risk management as measured by multidimensional scaling? Once the instrument was developed, three security experts were surveyed and the psychometric MDS security risk management concept map developed.

The Phase two survey (see Appendix H) contained 15 security risk management concepts (Table 4.3), arranged in alphabetical order and reduced from the initial 21 concepts (Table 4.2). Concept reduction ensured that the survey could be completed within a reasonable time period; however, a minimum number of concepts were required to achieve an appropriate MDS STRESS1 measure. As mentioned, STRESS1 is related to the number of objects [I] or concepts and the presented mapping dimensionality [D]. The intent of the study was to develop a two-dimensional concept map and as Kruskal and Wish (1978) stated, to reduce the sensitivity of STRESS1 requires I>4D, resulting in
a minimum of eight concepts. Nevertheless, in consideration of memory chunking and the survey time constraint, no more than 15 concepts could be used. This interpretation resulted in 13±2 subordinate concepts per knowledge category being determined as the preferred survey number. This quantity allowed the more used concepts – as proposed by LIWC (Table 4.3) – to be tested without making the survey excessively long.

Table 4.3

*Pilot study: Phase two security risk management category and subordinate concepts*

<table>
<thead>
<tr>
<th>Security Risk Management</th>
<th>Analysis</th>
<th>Decision-making</th>
<th>Modelling</th>
<th>Risk management</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Communications</td>
<td>Hazards</td>
<td>Probability</td>
<td>Statistics</td>
</tr>
<tr>
<td></td>
<td>Consequence</td>
<td>Intelligence</td>
<td>Psychometric risk</td>
<td>Threats</td>
</tr>
<tr>
<td></td>
<td>Cultural risk</td>
<td>Judgement</td>
<td>Risk</td>
<td></td>
</tr>
</tbody>
</table>

With the psychometric MDS survey, each expert participant was also given a copy of the introduction letter. In addition, after each participant had read the instructions and completed the survey, they were asked predefined questions and to grade each question (Table 4.4) from a scale of one to five, with one being *very easy* and five being *very difficult*. The expert participants were also timed on survey completion.

Table 4.4

*Pilot study: Predefined survey questions*

<table>
<thead>
<tr>
<th>Predefined pilot study questions</th>
<th>Mean Response</th>
<th>Mean</th>
<th>SD</th>
</tr>
</thead>
<tbody>
<tr>
<td>In your opinion, was the survey well laid out?</td>
<td>Easy - moderate</td>
<td>2.33</td>
<td>0.58</td>
</tr>
<tr>
<td>Were instructions simple, to the point and provided sufficient direction?</td>
<td>Easy</td>
<td>2</td>
<td>1.00</td>
</tr>
<tr>
<td>Did you find the questions easy to read?</td>
<td>Easy</td>
<td>2</td>
<td>0.00</td>
</tr>
<tr>
<td>Could you understand the questions?</td>
<td>Easy</td>
<td>2</td>
<td>0.00</td>
</tr>
<tr>
<td>Did you feel the survey was relevant to the problem discussed in the Introduction Letter?</td>
<td>Very easy</td>
<td>1</td>
<td>0.00</td>
</tr>
<tr>
<td>Would you be willing to do the survey again?</td>
<td>Yes</td>
<td>1</td>
<td>0.00</td>
</tr>
<tr>
<td>Time to read &amp; complete the introduction letter &amp; survey?</td>
<td>14.33 minutes</td>
<td>1.53</td>
<td></td>
</tr>
</tbody>
</table>

A number of critical comments were expressed by the participants that included semantics, format and length of the survey, and that to complete the survey required thought. Semantic comments were concise and regarded the use of the concept’s
network and psychometric risk. During Phase one the term psychometric risk was changed to perception, as according to the experts these terms were interchangeable, however, perception was a more frequently used term. Network was not considered a commonly used concept within the security risk management category and was therefore removed from the pilot study.

The style of the survey raised a number of comments including the concept blocks, quantity of information presented and survey format. Due to the repeating format of concepts (see Appendix H), some participants stated that as they completed the survey they misread the concept they were assessing. It was recommended that concepts be organised into their own discrete blocks, with breaks between each concept block. The original survey (Table 4.5) had unrelated and highly related on each concept line. For the participants this made the survey appear to contain an excessive amount of information. Therefore the terms unrelated and highly related were relocated within the numeric sliding scale. It was also recommended that the font size be increased, however, to keep the survey to a maximum of three pages this was not incorporated. The required thought necessary to complete the survey demonstrated the complexity of the related concepts and was not considered further.

Table 4.5

*Pilot study: Phase two revised survey format*

<table>
<thead>
<tr>
<th>When compared to</th>
<th>Unrelated</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>Highly related</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk - Statistics</td>
<td>Unrelated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk - Threats</td>
<td>Unrelated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The introduction letter required amendments to improve participant’s instruction, reduce the complexity of the research overview and include the researcher’s title. It was recommended that the sample concepts be printed in a *bold* format, allowing the participant to clearly identify these. The overview of the study included specific concepts relating to the theoretical background of the study, however, it was claimed that these were too complex and that the participants may not have expertise in this
theoretical area. Therefore, the overview of the study was rewritten to be less theoretical in context. Finally, to increase empathy between the researcher and proposed participant, it was recommended that the researcher should clearly indicate his employer.

The completed survey data were compiled and tested for reliability and validity. Reliability was tested using Cronbach’s Alpha model, which produced a moderate ($\alpha=0.64$) result. Validity used face and concurrent validity. Face validity produced a result ($M=1.00$, $SD=0.00$) indicating that that the participants appeared to acknowledge that there was a clear relationship between the context of the study (detailed in the introduction letter) and survey (Table 4.3 and Appendix H). However, it must be noted that all participants had prior knowledge of the study before completing the survey. Concurrent validity was tested using Pearson two tailed correlation at $\geq95\%$ confidence level between the participant’s responses (Table 4.6), producing a moderate mean result ($r=0.40$, $SD=0.13$).

Table 4.6

*Pilot study: Pearson two tailed correlation*

<table>
<thead>
<tr>
<th>Participant</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0.491**</td>
<td>0.465**</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0.250**</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

** Correlation is significant at the 0.01 level (2-tailed)
N=3

The primary process for Phase two was to use MDS to analyse the collected data and present a psychometric concept map of security risk management. The MDS ALSCAL analysis ($STRESS1=0.35$, $RSQ=0.27$) produced the spatial map of security risk management knowledge structure (Figure 4.1). However, the MDS STRESS1 was relatively high, as $<0.05$ provides an excellent representation with no significant misinterpretation and $\leq0.15$ represents a moderate two-dimensional representation (Cheng, 2004).
Figure 4.1 Pilot study: MDS knowledge structure of security risk management
(comms = communications; cultrisk = cultural risk; intell = intelligence; psycho = psychometric risk; stats = statistics)

Figure 4.1 required rotation (approximately 50°), removal of axis data, and inclusion of propositional statements and labels. Propositional statements and labels were inserted by the researcher, based on spatial concept proximity to indicate the degree of relationship, supported by a security expert. The insertion of the propositional statements and labels resulted in the development and presentation of the pilot study draft psychometric MDS security risk management concept map (Figure 4.2).
Figure 4.2 Pilot study: Draft psychometric MDS security risk management concept map

Note: analy = analysis; configs = configuration; conseq = consequence; coms = communications; cult risk = cultural risk; decis = decision; judge = judgement; intel = intelligence; percep = perception; prob = probability
**4.4 Pilot study: Phase three Expert knowledge structure validation**

Phase three required expert knowledge structure validation of the psychometric MDS security risk management concept map (Figure 4.2) with interviews of two security experts – David and Andrew. An expert interview survey (Appendix A) was developed to analyse and interpret the opinions of both experts regarding the knowledge category security risk management, subordinate concepts (Table 4.3) and psychometric security risk management concept map structure (Figure 4.2).

Experts were selected based on their security experience, academic standing and availability to the researcher. The interviews, completed using a semi-structured interview instrument, were audible recorded and transcribed. This approach allowed analysis of the collected data using QSR N6 and triangulation with study Phases one and two. The interview transcripts were analysed for data patterns and in conjunction with the research questions, assertions formed (Erickson, 1986). This resulted in four assertions that responded to Research Question three: What is the expert knowledge structure and subordinate concepts of security risk management as measured by interviews?

**4.4.1 Assertion 1: Experts considered that the MDS concept map for the category of security risk management presented a suitable foundation knowledge structure**

There was evidence that MDS developed and structured a valid concept map of the security risk management category. As David commented when asked whether the structure described the ideas underlying risk “I do .. it’s including a lot of things that normally are not included that a lot of people do not think about .. I find that pretty good and the relationships are very helpful.” Later this comment was further supported when asked if the map represented a valid and appropriate relationship in the ideas of risk, to which he replied “this really represents what I would … personally think and the whole concept of security risk”.
When Andrew was asked his opinion on the map’s structure and its validity, he provided a positive response. Regarding the structure of the map, he stated that “I think it includes most of the main concepts, but in terms of the actual structure and the way the relationships between the various concepts have been formed, there would be a few things that I would question.” Although not unconditional, he later stated that “I would say that the relationships are fairly sound”.

The concept map’s visual representation provided an interesting response from both experts. David observed that “it visually shows where the core of this whole entire concept is .. risk, threat, consequence and the arrangement of everything else around it really does simulate the importance of all the different areas and where they lie.” Andrew supported the spatial “top” locality of the concept risk from a “hierarchical point of view”. He later reaffirmed this point by stating that “if I was going to define a starting point, I would probable say risk.” It could be argued that this would appear to demonstrate the implicit nature of the concept risk and ascending explicit subordinate concepts within the map’s structure.

When the experts were asked what they considered were the most important ideas in security risk management, Andrew chose risk, threat and “then there's a lot I would consider”. David provided a different response, choosing decision followed by “the likelihood of the threat”, combining two concepts. However, when a transcript word count was completed, David and Andrew both used risk (53;12%: 131;27%) and threat (52;12%: 80;16%) twice as many times as any other concept (Table 4.7). This frequency count placed risk as the most commonly used concept, followed by the concept threat.
Table 4.7
Pilot study: Utilisation of concept terms by David and Andrew during the expert interviews

<table>
<thead>
<tr>
<th>Concept</th>
<th>David No</th>
<th>David %</th>
<th>Andrew No</th>
<th>Andrew %</th>
<th>Ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>53</td>
<td>12</td>
<td>131</td>
<td>27</td>
<td>1</td>
</tr>
<tr>
<td>Threat</td>
<td>52</td>
<td>12</td>
<td>80</td>
<td>16</td>
<td>2</td>
</tr>
<tr>
<td>Consequence</td>
<td>29</td>
<td>6.5</td>
<td>43</td>
<td>8.7</td>
<td>3</td>
</tr>
<tr>
<td>Decision</td>
<td>47</td>
<td>11</td>
<td>12</td>
<td>2.4</td>
<td>4</td>
</tr>
<tr>
<td>Statistics</td>
<td>20</td>
<td>4.5</td>
<td>19</td>
<td>3.9</td>
<td>5</td>
</tr>
<tr>
<td>Probability</td>
<td>11</td>
<td>2.5</td>
<td>23</td>
<td>4.7</td>
<td>6</td>
</tr>
<tr>
<td>Culture/al</td>
<td>8</td>
<td>1.8</td>
<td>25</td>
<td>5.1</td>
<td>7</td>
</tr>
<tr>
<td>Analysis</td>
<td>12</td>
<td>2.7</td>
<td>10</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>Judgement</td>
<td>15</td>
<td>3.4</td>
<td>5</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>Perception</td>
<td>9</td>
<td>2</td>
<td>9</td>
<td>1.8</td>
<td>10</td>
</tr>
<tr>
<td>Model</td>
<td>7</td>
<td>1.6</td>
<td>0</td>
<td>0</td>
<td>11</td>
</tr>
<tr>
<td>Communication</td>
<td>5</td>
<td>1.2</td>
<td>0</td>
<td>0</td>
<td>12</td>
</tr>
</tbody>
</table>

The opinions of the experts were sought regarding a number of conceptual relationships. An unusual aspect in the formation of the security risk management concept map was the central locality of the concept threat and the experts were asked to comment on this matter. This question produced varying response from both experts, with David generally considering that this term did present a valid location. As David stated “I would say that it [threat] is quite a central theme” and went onto say that “without threat, there is no need for a whole lot of risk concepts.”

In contrast, Andrew did not provide such a direct response to this issue, although he did find “it is interesting that threat came out. Perhaps because threat is also a concept that people can latch onto quite easily. Threat is obviously a central idea and very important.” Later Andrew also stated that “there is no problem with threat relating to all these things.” Nevertheless, according to both experts the concept threat should be positioned in a relatively central location within the security risk management concept map, supporting the map’s knowledge structure.
The other conceptual relationship questioned was the linkage of risk, threat, consequence and decision. The experts were asked if they considered these links were valid and if so, to justify their response. David responded with an affirmative:

I believe they are justified, why is because . . . that is the process you have. A risk which is a threat, threats have consequence and consequence aids decision. Like it’s outlined here exactly and that’s the very basic concept of security risk and why we go about identifying risk and why we end up managing risk.

Andrew was not as decisive, commenting “certainly there is a clear relationship there. Although whether it’s linear or not, I would kind of think about that a bit more.” He then raised AS/NZS4360 Risk Management, stating that you would “only be getting half the picture” unless you considered probability within the sequence. Probability did not appear in the security risk management concept map sequence, although probability was spatially located in close proximity to consequence.

There was agreement from both experts that hazard was not a concept that is generally used by security experts within the category of security risk management. As David stated “I could do without it” and Andrew indicated that hazard is not a term used “purely in security”, however more as an “inanimate kind of threat”. Both experts concurred that the concept map contained the most significant risk category concepts. However, Andrew did comment on the spatial locality of both statistics and modelling, considering that it “is quite interesting” that they are so far apart. There was no comment from David regarding this issue.

In considering the concept map’s structure, spatial representation, central theme of threat, sequential nature of concepts and the exclusive use of significant security risk management concepts, it can be concluded that the psychometric security risk management concept map appeared to represent a valid knowledge structure, supported by both security experts. As David stated, “this structure is good, you do not want to destroy that”; nevertheless, there were a number of issues relating to the complexity of the security risk management category and the concept map’s propositional linkages.
4.4.2 Assertion 2: The sequential nature of the concept clusters represented expert decision-making

The expert’s were asked whether they felt as if a number of conceptual relationships within the security risk management concept map (Figure 4.2) represented their thought process. These relationships included the sequential linkages and knowledge clusters of:

- risk, threat, consequence and decision
- judgement forms threat
- judgement aids modelling
- risk is statistics and forms risk management
- General integration of the risk subordinate concepts

Risk, threat, consequence and decision, with supporting propositional linkages, demonstrated what could be argued was a core thought process of security experts. Along with the central theme of threat, this sequence appeared to be a significant knowledge construct. As discussed in assertion one, David clearly agreed. Andrew also stated that he felt there was a clear relationship, however likelihood should also be included within the sequence. When asked about the relationship of consequence aiding decision both experts concurred, with David responding that “they’re in the right order” and Andrew stating “absolutely, yes.” There was general agreement between both experts that this representation was appropriate.

The security risk management concept map presented the link judgement forms threat – a relatively long spatial link. Expert evidence indicated that although the map showed a propositional link, this was not supported by the experts. It appeared that the MDS knowledge structure appropriately represented a dissimilar concept cluster and an inclusion of a propositional link should not have been included. Andrew was asked his opinion of judgement aids modelling. He responded positively, indicating that there is a link that it is based on perceptions and that judgement would define how a person may model risk. The concepts of judgement, model and perception were closely clustered. This knowledge cluster indicated a strong relationship between these concepts,
supporting spatial relationship and further discussion in assertion four (see Chapter 4.4.4).

The concepts of risk, statistics and risk management formed a cluster. It could be argued that although empirical evidence would indicate a close proximity of risk and risk management, statistics produced an unusual triangulation. Both experts were asked their opinion on this formation. David agreed that risk and risk management are closely linked or “slightly overlap”, however, recommended that statistics should link into probability and consequence. David appeared to be proposing Australian Risk Management Standard definition of risk, such as risk = probability * consequence (Standards Australia, 2004a). On further questioning, he stated that “statistics can be extracted from a risk” and that “you can break down a risk and represent it statistically.” After some further discussion on risk and statistics, David considered that security professionals attempt to quantify risk and concluded, “I would personally see risk as being statistics.” When Andrew was asked his opinion, he stated that statistics is related to risk management more so than risk, however it is “certainly not a bridge if that is what it suggests [pointing to the psychometric security risk management concept map].”

David indicated that he considered the structure of the map was appropriate, stating that the “pattern is fine.” Andrew did not entirely agree, nevertheless he expressed the view that “certainly some linkages are quite valid in their relationship and are fine, in other cases though I would say a few people would question that.” However, when Andrew was asked a question regarding the appropriateness of the concept relationships, he agreed and also commented that “the idea put forward encompasses risk.”

It would appear that the psychometric MDS security risk management map presented an appropriate sequential representation of subordinate concepts. Representation was demonstrated through the agreement of both experts in the significant relationship of risk, threat, consequence and decision linkage. Judgement forms threat demonstrated an error in the concept map, which appeared to indicate how dissimilar spatial separation demonstrated weak propositional linkage. This spatial relationship was further supported
by the cluster concepts of *judgement aids modelling*. It would appear that the sequential nature of the majority of subordinate concepts, based on spatial proximity, demonstrated some degree of expert decision-making. Also, these concepts appeared to demonstrate the complexity of the security risk management concepts and their propositional relationships.

4.4.3 Assertion 3: Experts considered that although the map represented the category risk, there was greater complexity than shown

Both experts were asked a number of questions resulting in indicators that the psychometric MDS concept map did not fully represent the security risk management category. Analysis commenced with a discussion on missing security risk management category concepts, the central theme of *threat* and that all subordinate concepts could have interrelated propositional linkages.

David indicated that there should be subsections to *decision*, although he did state that the map only represented “major concepts’ and that a subset of *decisions* would be “irrelevant”. On the other hand, Andrew put forward assets, vulnerabilities, intent and capabilities as additional subordinate security risk management concepts. Neither expert proposed the same or similar additional security risk management concepts, which indicated that the more significant security risk management subordinate concepts were included.

When discussing the central theme of *threat*, Andrew stated that “you would say analysis should only point to threat or it should also have a relationship with risk .. and if you are looking at probability are you looking at risk probability or something to do with threat?” When asked whether the map was hierarchical in nature, Andrew proposed that all concepts can have a “direct relationship” to risk. In addition, when Andrew was asked about the relationship of concepts, he stated that “you would say that this doesn’t seem like a good way to define a relationship, but this depends on what the context is.”
Andrew also stated that he “would view the diagram as a lot more complex, there would be just more linkages depending on how you look at it.” This view was reaffirmed when Andrew attempted to draw a map. After sketching approximately five security risk management category concepts (see Appendix C), he said “I sort of view this as a lot more complex, with I guess a lot more linkages.” However, he did later state that “I guess it’s not black or white through, because you could draw an arrow but it might be a really weak link, but you could sort of justify it from one point of view.”

These expert comments indicated that there could be many potential propositional linkages within the psychometric security risk management concept map. Therefore, it would appear that both experts considered that although the map represented the security risk management category, there was greater complexity than shown within the concept map.

**4.4.4 Assertion 4: The security risk management concept map propositional linkages did not effectively represent concept linkage**

Both experts considered that the security risk management map propositional linkages did not fully reflect valid linkages between concepts. When asked whether the relationship encompassed security risk management, Andrew indicated in some cases they are “fairly sound’. However, in others the map did not represent a “good way” to define relationships, although this was dependant on the context. Andrew did state that if “you were going to draw arrows, I would have the arrows going the other direction.” When asked if the concept map represented his ideas of security risk management, Andrew generally agreed, nevertheless he did propose different propositional linkages between some concepts. Later in the interview he presented an example, with the propositional linkage that *risks are threats*. He argued that this indicated that risk and threats are interchangeable and are therefore the same concept. In addition, he claimed that a threat should lead to a risk, concluding that “in my own opinion I wouldn’t say risks are threats, but once again depending on the expert you are talking to they may have a different viewpoint.”
In a more explicit approach, both experts were asked if there were any propositional linkages that they considered were inappropriate. David indicated only one statement – the link between perception and judgement should read *determines* instead of *configures*. Andrew proposed different propositional linkages – judgement and decision-making, cultural risk and perception, and statistics and modelling. Judgement and decision should have a “more clearly related” link, however without offering a propositional statement. According to Andrew, “I would have cultural risk more clearly related to perception.”

The security risk management concept map presented the link that *judgement forms threat*. This link was relatively long and therefore indicated a degree of propositional weakness. The experts were asked if judgement should be linked to threat and to justify their response – David responded with “judgement doesn’t form a threat .. consequence can be variable, determining your perspective.” Therefore he did not consider that this link was valid. Andrew supported this response, with “I don’t see a strong link .. you can think about it and in some ways you can say that that links to that, but .. judgement and threat wouldn’t be something that would come off the top of my head.” In summary, the experts concurred that when MDS presented weak or dissimilar concepts through spatial separation, a propositional linkage should not be considered.

Although the importance of propositional linkages cannot be wholly ignored, it can be argued that structure development and definition are important. Considering the number of propositional linkages used within the psychometric MDS security risk management concept map – all linked and labelled by the researcher – it could be argued that overall these linkages were in general valid. However, to improve future studies expert opinions with the propositional linkages were sought. Also, greater emphasis was placed on the spatial strength or similarity of concepts when developing further propositional linkages.

### 4.4.5 Phase three: Assertion conclusion

The psychometric MDS concept map structure, spatial representation, sequential nature of concepts and the inclusion of the more significant security risk management concepts
provided evidence that the concept map appeared to represent a valid knowledge structure for the security risk management category. The map’s structure was strongly supported by both security experts. Therefore, the psychometric MDS structure appeared to provide a suitable spatial representation of the security risk management knowledge category.

It also appeared that the security risk management concept map presented an appropriate sequential representation of subordinate concepts. Concept sequencing was demonstrated through the agreement of both experts in the significant relationship of many security risk management concepts. A core representation was risk, threat, consequence and decision. In contrast, concept mapping errors were also demonstrated with spatial separation demonstrating weak propositional linkage. It appeared that the sequential nature of the majority of subordinate concepts, based on spatial proximity, demonstrated expert decision-making. Both experts indicated that there could be greater potential propositional linkages and relationships within the concept map. Although both experts considered that the map represented the security risk management category, each expert believed that there was greater complexity than shown within the concept map.

The psychometric MDS security risk management concept map did not wholly represent effective propositional linkages, which according to Novak (n.d.) assist in conceptual relationship and provides meaning. However, within the pilot study the initial propositional linkage development and insertion was completed by the researcher. These propositional linkages reduced the validity of the psychometric concept map, which in the primary study required security expert input to develop and label. Greater emphasis should have also been placed on the spatial strength or similarity of concepts for the insertion of propositional linkages. It can be argued that developing and defining a map structure was most critical in understanding underlying knowledge within concept maps. Nevertheless to improve the primary study, further expert opinion on the propositional linkages was sought.
The pilot study Phase three appeared to demonstrate that:

- MDS did effectively represent a suitable foundation knowledge structure.
- Spatial location of concepts provided an indication of propositional relationships.
- Sequential location of concepts provided an indication of expert conceptual decision-making.
- The security risk management category was more complex than the pilot study psychometric MDS security risk management concept map effectively presented.
- Propositional linkages, although important in aiding understanding, cannot be entirely defined through psychometric MDS concept mapping technique.

4.5 Pilot study: Phase four Expert validation of the MDS concept map

The research questions for Phase four required the presentation of the psychometric MDS concept map of security risk management constructed from the knowledge category and subordinate concepts. Phase four analysis used a comparative study (Cohen, et al., 2002) between Phase two and Phase three outcomes – to quantify the knowledge categories and subordinate concepts represented within the psychometric concept security risk management concept map. Finally, this phase also defined and quantified the appropriateness of the psychometric MDS concept mapping technique to develop and represent knowledge structure as psychometric concept maps. Phase four followed the same methodology as Phase three, with assertions formed in response to Research Question four: Can a consensual psychometric concept map of the security risk management knowledge category and subordinate concepts be developed and represented? and Research Question five: Is multidimensional scaling an appropriate psychometric technique to develop and represent consensual concept maps?

4.5.1 Assertion 1: The security risk management concept map presented a valid knowledge structure of the category security risk management

As the findings from Phase three demonstrated, there appeared to be significant evidence to indicate that the psychometric MDS concept map provided a valid knowledge structure for the security risk management category. The map’s structure was supported by a number of significant results discussed within the assertions presented in Phase
three, including the map’s spatial knowledge structure, sequential nature of concepts and concept clusters. However, the map did not fully represent the complexity of security risk management or provide effective propositional linkages.

Both experts supported the general structure and visual representation of the psychometric security risk management concept map, especially with the central theme of threat. According to the experts, all appropriate concepts were included within the concept map’s structure. However, there were a number of concepts that the experts considered were not appropriate within the security risk management category, for example, hazard.

The sequential nature of the concept clusters appeared to represent expert decision-making, with conceptual relationships demonstrated by a number of significant expert decision-making ideas. A particularly significant linkage was risk, threat, consequence and decision, and another was the cluster risk, statistics and risk management. Both of these linkages appeared to support valid conceptual clusters. The experts did agree that although the map represented the security risk management category, it did not fully represent the complexity of the category and supporting concepts. As indicated, Andrew attempted to draw a security risk management concept map (Appendix C), however, after a number of attempts stated that it would require considerable greater thought and iterations.

According to the experts, the map’s propositional linkages did prove to be unreliable in representation. These linkages had been inserted into the concept map by the researcher, resulting in subjective interpretation of the propositional linkages. Nevertheless, significant findings were made in regard to concept relationships with the degree of spatial proximity, as both experts agreed that closer spatially related concepts demonstrated a stronger conceptual relationship – findings that are supported in previous research (Trochim & Cook, 1994).
4.5.2 Assertion 2: MDS can be used to develop and structure concept maps

It appeared that the MDS measure and spatial presentation of the security risk management category presented a valid knowledge construct because to a degree, both experts concurred in the support of the concept map’s structure. The construct was further validated when Andrew attempted to draw his own version of the map, which highlighted the complexity of the category and also supported the MDS concept map structure. Other areas of validation included the hierarchical structure of concepts, demonstrated conceptual relationship of concepts by spatial proximity and support for the structural linkage of concepts.

MDS produced a hierarchical structure of concepts, in particular supported by risk and risk management located at the upper section of the concept map. As mentioned, it is acceptable to rotate MDS representation’s (Trochim & Cook, 1994) and this concept map was rotated approximately 50°. Rotation represented the most effective image axis for interpretation, with the structure appearing to demonstrate an implicit to explicit concept construct. It also appeared to effectively represent an appropriate structure for a complex and subjective category. Both experts agreed that the concept map did not wholly demonstrate the complexity of this category, although they could not effectively produce another conflicting structure.

Strong conceptual relationships appeared to be demonstrated by spatial proximity and concept clusters. The greater the relationship between the concepts, the closer their spatial proximity. Initially, this strength was not fully appreciated until both experts questioned propositional links that were at an extended distance, an example such as judgement forms threat. This spatial relationship facilitated the formation of propositional linkages, however, proximity did not provide effective linking statements or labels. Although linkages could be inserted effectively, based on spatial proximity, written labels were far more subjective. MDS could not provide this data, only domain experts through a consensual approach.
Both experts agreed that the concept map’s construct appeared appropriate and that the map also appeared to demonstrate, through structural linkage of concepts, expert decision-making. This view was supported by a number of significant concept clusters and their supporting structures. These included the sequential linkage of risk, threat, consequence and decision; judgement, model and perception; risk is statistics and statistics forms risk management clusters and the general integration of the security risk management subordinate concepts.

The psychometric MDS concept mapping technique appeared to effectively demonstrate consensual knowledge structure, supported through hierarchical order, proximal concept relationships and structural linkage, supporting expert decision-making. Therefore, it was argued that MDS provided an appropriate technique to develop and construct psychometric MDS concept maps.

The outcome from the pilot study appeared to demonstrate a number of significant findings. These supported the viability of the research questions, with bounded evidence to claim that with regards to security risk management:

- Psychometric MDS concept mapping represented an appropriate technique to provide structure in the foundation of concept maps.
- Within the psychometric MDS concept map, the spatial location of concepts provided an indication of conceptual relationship.
- Within the psychometric MDS concept map, the sequential structure and concept clusters provided an indication of expert conceptual decision-making.
- Informed insertion of propositional linkages can be based on the spatial proximity of concepts.
- Propositional linkages supporting labels, although important in aiding map comprehension, cannot be labelled through the psychometric MDS concept mapping technique.
- Propositional linkages and supporting labels require consensual domain expert input.
Based on the above findings, an appropriate psychometric MDS concept map of the security risk management category and supporting subordinate concepts can be presented (Figure 4.3).

Figure 4.3 Pilot study: Psychometric MDS security risk management concept map

Note: comms = communications
4.6 Pilot study: Reliability and validity

The validity and reliability of the research methodology and instruments were measured, allowing improvements to be made. Subsequent improvements ensured that the methodology and instruments were acceptable for progression to the primary study. Each of the four phases of the study was tested, with different techniques based on the methodology of each phase.

Using Cronbach’s Alpha reliability measure, the survey instruments were tested to demonstrate that the “measure will produce the same result from one occasion to another” (Clark-Carter, 1997, p. 27). As Malim and Birch stated “it is very important that any test used in a piece of research should be reliable” (1997, p. 46). This measure demonstrated that the survey instruments produced an acceptable reliability measure before progression onto the primary study.

The validity of the survey instruments were tested through measures of face and concurrent validity. These items were tested to demonstrate the “extent to which the research instrument measures what the developers purport it to measure” (Angus & Gray, 2001, p. 23). Face validity used academic security experts, who assessed whether the instrument measured security risk management knowledge categories and supporting subordinate concepts. Concurrent validity used Pearson product moment correlation coefficients because it “measures the extent to which two variables are related to one another” (Malim & Birch, 1997, p. 42). This measure demonstrated the consistency between respondents’ comments on each instrument and at each study phase.

Phase one reliability and validity applied expert review of the security risk management category subordinate concepts. This expert review reduced the initial Phase one critiqued data set from 21 concepts to a final pilot study use of 15 concepts. When reviewed by security experts in Phase three, only one concept was highlighted as being inappropriate for that category, producing highly consistent (93.32%) results.
Phase two used Cronbach’s Alpha reliability, producing a moderate ($\alpha=0.64$) value. Face validity was measured by security experts reviewing the research instrument, producing a highly consistent value ($M=1.00; SD=0.00$). In addition, concurrent validity using Pearson two tailed correlation at $\geq95\%$ confidence level produced a moderate total result ($r=0.40, SD=0.13$) between participant’s responses.

The psychometric MDS knowledge structure map (Figure 4.1) goodness-of-fit value iterations ceased at $\leq0.001$, with a moderate stress value (STRESS1=0.35, RSQ=0.27). A moderate result for a two-dimensional representation is considered to be between 0.39-0.15 (Cheng, 2004; Kruskal & Wish, 1978). It could be claimed that this moderate STRESS1 measure was a result of the low sample size ($N=2$), that the psychometric MDS knowledge structure representation was not a reliable measure or “the existence of additional structure in the data” (Kruskal & Wish, 1978, p. 33). In contrast, the proceeding phases appeared to indicate that the knowledge structure did represent an appropriate security risk management knowledge structure, opposing the moderate STRESS1 result.

Phase three used expert judgement to access the reliability of the instrument. Both face and convergent validity were measured, with experts reviewing the research instrument and psychometric MDS security risk management concept map. These measures appeared to produce a moderate result, based on the security expert’s review. Triangulation of Phase two and Phase three appeared to produce an appropriate psychometric MDS concept map, generally supported by the domain experts (see Section 4.4). Finally Phase four, being a comparative study, relied on the reliability and validity of the previous data collection phases and did not apply specific measures beyond consideration of expert judgement.

### 4.7 Study modifications

The completion, analysis and interpretation of the pilot study resulted in a number of amendments to the research methodology and supporting survey instruments. The research methodology proved to be both valid and reliable, with minimal changes
necessary. However, research methodology changes did include the involvement of security experts at Phase two, in principle, to construct the propositional linkages. Research survey instrument changes included format, structure and a reduction in the number of survey questions.

To ensure that the participants completed the Phase two instrument within a suitable time period (see Table 4.4), a preferred 13±2 subordinate concepts per knowledge category was applied. This concept limit also minimised MDS STRESS1 and reduced the complexity of the psychometric MDS concept map, while retaining the most used subordinate concepts. From the results of the pilot study, this concept number proved to be appropriate as the security experts considered that there was no significant concept excluded from the security risk management category.

During Phase three, experts generally questioned the propositional linkages, not necessarily the category knowledge structure or concept clusters. To reduce this limitation, the primary study used additional Phase two security experts to insert propositional linkages with the Delphi method. Phase three expert interview questions were reduced from an initial 19 questions (Appendix A) to 13 questions (see Appendix I), with the final questions considered more suitable to support the assertions and reduce repetition. Also, the theoretical outcome of the study was to both develop an applied knowledge structure and test the ability of MDS to develop and construct psychometric concept maps. It was therefore considered that the Phase three expert interview survey would provide greater investigation on structural knowledge format. Therefore the primary study Phase three expert interview (Appendix I) retained the following format and questions:

- Overall structure of category
- Spatial relationships of concepts
- Knowledge category subordinate concepts
- Propositional linkages
- Two main themes based on concept clusters and sequence
- Instrument conclusion
The outcomes of Phase three also produced a number of additional changes to the expert interview survey. These changes included a greater explanation to the participating expert on how the psychometric MDS concept map was produced, that there was awareness that the majority of the concepts could have some form of propositional linkage, the need to only consider prominent statements and that the survey should be more specific in achieving the outcome of Phase three.

During the pilot study, Phase four initially comprised three assertions. Nevertheless, there was significant repetition between Phase three and Phase four, in data analysis and synthesis, because the preceding phases had effectively critiqued the security risk management category and subordinates concepts. Therefore Phase four assertions were reduced from three to two, with According to experts, the category risk contained appropriate concepts removed. Finally, with input from the experts during Phase three and comparative Phase four, the security risk management concept map was adjusted to produce the final pilot study psychometric MDS security risk management concept map (Figure 4.3).

4.8 Pilot study limitations

Pilot study limitations need to be addressed. The first was the small pilot study Phase one sample size comprising of three West Australian undergraduate university security courses, which was inappropriate to demonstrate both reliable and valid results. Nevertheless, the pilot study did test the appropriateness of the study’s methodology. The second limitation was the pilot study’s Phase two method of using the researcher to develop and insert initial concept map propositional linkages. During Phase three, this method resulted in greater security expert comment than general concepts and knowledge structure. An issue that led to a change in study design and the requirement of security experts to develop and insert Phase two propositional linkages using the Delphi method, ensuring a greater consensual approach.

The Delphi method, a written form of the Nominal Group Technique (Cohen, et al., 2003), facilitates a group decision-making process without the participants having to come face-to-face. The participants, in isolation, are presented with a series of open-
ended questions for which they provide a response. These responses are summarised, distributed back to the participants and the process is repeated – polarising responses and resulting in a majority opinion. The benefits of the Delphi technique is that responses are anonymous, there is no ego or domineering personalities, and the halo effect is reduced (Cohen, et al., 2003; Ethigie & Ehigie, 2005).

Phase two concurrent validity used Pearson moment mean measure, producing a moderate \( r=0.40, \ SD0.13 \) result and indicating that the participants produced differing responses within the Phase two survey instrument. However, this variance did not appear to be reflected in the expert opinion of the psychometric security risk management concept map and additional phase triangulation. Finally the psychometric MDS security risk management concept map produced a high \( \text{STRESS1}=0.35, \ \text{RSQ}=0.27 \) measure.

**4.9 Conclusion**

This chapter presented the pilot study, including resulting outcomes, reliability and validity, and study limitations. The pilot study allowed the research methodology to be tested and improved, leading to a number of study changes. These changes included the inclusion of additional security experts at Phase two to insert propositional linkages, a prescribed category concept size \( (13\pm2) \) and the development of assertions. Outcomes from the pilot study provided a number of significant results, supported by assertions.

Pilot study results included the development of a draft category of security risk management, supporting subordinate concepts of security risk management (Table 4.3) and the pilot study psychometric MDS security risk management concept map (Figure 4.3). Evidence from the pilot study appeared to indicate that MDS represented an appropriate technique to present knowledge structure in the formation of psychometric concept maps and that the spatial locality of concepts provided an indication of conceptual relationship.
In addition, sequential structure and concept clusters provided an indication that expert conceptual decision-making and propositional linkages could be considered based to some degree on spatial proximity of concepts. However, propositional linkages supporting statements could not be labelled through the psychometric MDS technique, as this required consensual input from domain experts. The pilot study also demonstrated that the study’s methodology was both reliable and valid, although the MDS measure of STRESS1 was high. Nevertheless, the study was appropriate for progression onto the primary study.
CHAPTER 5
PHASE ONE: SECURITY KNOWLEDGE CATEGORISATION

5.1 Introduction
Phase one of the study, describing the development of the security knowledge categorisation in response to Research Question one: What are the knowledge categories and subordinate concepts of security? is presented in this chapter. To achieve this outcome, the chapter is divided into a number of distinct sections. The first section (5.2) investigated and critiqued international security-related tertiary courses. Once appropriate security courses were selected, supported by security experts, the courses had their title structures analysed, concepts extracted and listed (5.3). Concept extraction allowed the operationalism of the security category definitions (5.4), supported through literature critique (5.5). Course contents were analysed, subordinate concepts extracted and listed (5.6), allowing the security risk management category to be tabulated (5.7). Finally, security experts validated the security risk management category concepts (5.8).

5.2 Investigation and critique of national and international tertiary courses
This section investigated and critiqued a list of national and international English speaking institutions that offered tertiary security courses at all levels, including undergraduate and post graduate awards. Search methods used the world-wide-web (WWW), American Society for Industrial Security (ASIS International, 2007a), Security Institute (Kidd, 2006), Australian University Guide (Good Guides, 2004) and Association of Universities and Colleges of Canada (2005). There was initially no limitation placed on the search criteria, as all institutions that offered security and allied industry courses were assessed (Table 5.1). In the WWW search engines, data strings used were security; security course; security management.
Table 5.1

*Location and number of security related courses*

<table>
<thead>
<tr>
<th>Country of origin</th>
<th>Number of institutions offering security related courses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>11</td>
</tr>
<tr>
<td>Canada</td>
<td>8</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>5</td>
</tr>
<tr>
<td>United States of America</td>
<td>74</td>
</tr>
<tr>
<td>New Zealand</td>
<td>5</td>
</tr>
<tr>
<td>South Africa</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>104</strong></td>
</tr>
</tbody>
</table>

During May to July 2005 a list of courses and supporting data were gathered (Appendix D), which were independently reviewed by two tertiary security academics and an industrial expert. From the 104 awards found (Table 5.1) and diversity (see Appendix D), only undergraduate tertiary Bachelor Degree (pass) level courses were critiqued. There could be many more security courses as a recent web site now lists “more than 300 participating two and four year institutions” (Davidson, 2005, p. 74), however, this includes “research programs, technological developments, services activities, training and degree programs” (Davidson, 2005, p. 74). Due to the breadth of security awards, college certificates, diplomas and postgraduate courses were not considered further. Course data were then compared and based on this course data, the three security experts selected seven courses that contained what they considered to be most appropriate security content.

During this examination, both academic and industry experts claimed a large majority of these courses did not effectively represent *organisational or corporate security*, however, were focused on allied or supporting industries. These allied industries included, but were not limited too, justice studies, police studies, political studies, criminology, law, social studies, management, business, technology and engineering. This breadth opposed the ASIS International list of security programs, which stated that they only included “security programs; those with criminology or criminal justice programs are not included unless a security speciality is also offered” (ASIS International, 2007a, p. 1).
Once the final seven courses (Table 5.2) were identified and assessed as containing a security major structure, full course syllabi and unit outlines were sourced. Course syllabi included the course overview and units of study descriptions, objectives and overview of content.

Table 5.2
Critiqued security courses

<table>
<thead>
<tr>
<th>Country</th>
<th>Institution</th>
<th>School</th>
<th>Award</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>Edith Cowan University</td>
<td>Engineering &amp; Mathematics</td>
<td>BSc (Security)</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>University of Portsmouth</td>
<td></td>
<td>BSc Hons (Risk &amp; Security Management)</td>
</tr>
<tr>
<td>United States</td>
<td>Eastern Kentucky University</td>
<td>Loss Prevention &amp; Safety</td>
<td>BSc (Assets Protection &amp; Security)</td>
</tr>
<tr>
<td>United States</td>
<td>John Jay College of Criminal Justice</td>
<td>Criminal Justice</td>
<td>BSc (Security Management)</td>
</tr>
<tr>
<td>United States</td>
<td>Farmingdale State University</td>
<td>Criminal Justice</td>
<td>BSc (Security Systems)</td>
</tr>
<tr>
<td>United States</td>
<td>Lewis University</td>
<td>Criminal/Social Justice</td>
<td>BA (Private Security &amp; Loss Prevention Management)</td>
</tr>
<tr>
<td>South Africa</td>
<td>University of South Africa</td>
<td>Public Safety &amp; Criminal Justice</td>
<td>BTech (Security Management)</td>
</tr>
</tbody>
</table>

5.2.1 Critiqued institutions and awards

From Table 5.2, an overview of each institution and their security award is presented. Each institution’s primary security course objectives, major topic of study, number of major units offered and related higher degrees are discussed.

5.2.1.1 Edith Cowan University, Perth, Australia

Edith Cowan University offers a suite of awards from three undergraduate degrees to a PhD and these awards are located within the School of Engineering and Mathematics. The three undergraduate awards include the Bachelor of Science (Security), Bachelor of Science (Security and Justice Studies) and Bachelor of Science (Security Management). All awards up to Masters level are offered both on campus and through distance learning. The study examined the Bachelor of Science (Security) as this award had been
offered for 12 years, was the initial award developed and contained the majority of students (School of Engineering and Mathematics, n.d.).

The Bachelor of Science (Security) award included studies in physical security, electronic security, information security and facility management, and according to Smith the “security .. curriculum has been developed on a science and technology foundation” (2001b, p. 10). The program also included studies in risk management, security management and a final year research project (School of Engineering and Mathematics, n.d.), offered within the 14 unit security major.

5.2.1.2 University of Portsmouth, Portsmouth, United Kingdom

The University of Portsmouth offers a Bachelor of Science, with Honours, in Risk and Security Management within the Institute of Criminal Justice Studies. The Department of Electronic and Computer Engineering also offers a degree in security technology, however due to the technology focus this award was not considered further. The Bachelor of Science (Honours) in Risk and Security Management award offers studies in security management, risk management and criminology, with supporting studies in health and safety, and computer security.

The Institute of Criminal Justice also offers a recommended pathway for stadium and arena safety specialist (University of Portsmouth, n.d.), which combines the security majors and sports management studies. The University of Portsmouth offers 11 major security units, with allied discipline supporting units. The award is only offered through remote learning (Institute of Criminal Justice Studies, 2005).

5.2.1.3 University of Eastern Kentucky, Kentucky, United States

The University of Eastern Kentucky offers a Bachelor of Science in Assets Protection and Security, with the award located within the College of Justice and Safety. The award is designed to provide students with fundamental knowledge to protect personnel, physical and information assets of corporations against loss caused by criminal activity, unethical practices and disaster (Eastern Kentucky University, 2005). Major security
categories of study are asset protection and investigations, supported with studies in security systems integration, computer and information security, and government security and auditing. University of Eastern Kentucky offers nine major security units, with six security electives.

5.2.1.4 John Jay College of Criminal Justice, New York, United States
The City University of New York offers a Bachelor of Science in Security Management, located within the John Jay College of Criminal Justice. The award “concentrates on the analysis of security vulnerabilities and the administration of programs designed to reduce losses in public institutions and private corporations” (John Jay College of Criminal Justice, n.d., p. 2). The major security category of study is security management, supported with studies in investigations, computer and information security, emergency planning, fire science and administration. John Jay College offers nine major security units, with five electives.

5.2.1.5 Farmingdale State University, New York, United States
Farmingdale State University offers a Bachelor of Science in Security Systems, located within the Department of Criminal Justice. The award takes a technology approach to “treat the technical aspect of the discipline” (Kostanoski, n.d., p. 1). The major security units of study consider computer security and security technology, with security technology comprising physical security, access control and intrusion detection. Farmingdale State University offers 16 major security units, with four supporting units of study in computer networking.

5.2.1.6 Lewis University, Illinois, United States
Lewis University offers a Bachelor of Arts in Private Security/Loss Prevention Management, located within the Criminal/Social Justice Department. The award offers a “broad base of knowledge through professional courses such as private security investigation, security organisation and management, and safety and risk analysis” (Lewis University, 2004, p. 1). The major security category of study is private security, supported with studies in investigations, fire science, criminology and architectural
design. Lewis University offers 11 major security units, with eight of these being dedicated security units.

5.2.1.7 University of South Africa, Pretoria, South Africa

The University of South Africa offers a Bachelor of Technology in Security Management, located within the Division of Public Safety and Criminal Justice. The award’s main objectives are to provide professional education to all sectors of the security industry and South African community. It is considered that the security industry protects the interests and assets of commerce and industry to maintain profitability, economic growth and job creation, as well as to develop welfare and stability (Division of Public Safety and Criminal Justice, 2004). The major security category of study is private security, supported with studies in risk management, investigations and law. The University of South Africa offers 11 major security units.

5.3 Concept extraction from the selected undergraduate courses

Concept extraction used Linguistic Inquiry and Word Count (LIWC) (Pennebaker, et al., 2001) and commenced with an initial analysis of each critiqued course and their individual unit of study titles, allowing initial concept categorisation. The course transcripts were sanitised to retain only security-related titles, as generic study or research skills were not considered within the concept extraction analysis. Concepts were counted each time they were used within the course title, although redundant words were not consider as a count (Hiemstra, 1996). The unit title concept count resulted in a summation of security concepts and a frequency count (f) of how often a concept was used (Table 5.3).
Table 5.3

Concepts count extracted from course units of study titles

<table>
<thead>
<tr>
<th>Concept</th>
<th>Concept descriptor</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>Information security</td>
</tr>
<tr>
<td>9</td>
<td>Criminology</td>
</tr>
<tr>
<td>7</td>
<td>Security management</td>
</tr>
<tr>
<td>6</td>
<td>Law</td>
</tr>
<tr>
<td>5</td>
<td>Security</td>
</tr>
<tr>
<td>4</td>
<td>Asset protection</td>
</tr>
<tr>
<td>3</td>
<td>Fire science</td>
</tr>
<tr>
<td>2</td>
<td>Facility management</td>
</tr>
<tr>
<td>2</td>
<td>Access Control</td>
</tr>
<tr>
<td>1</td>
<td>Administration</td>
</tr>
</tbody>
</table>

5.4 Development of the security knowledge categories

Concepts were tabled for possible inclusion as a category if they produced a word frequency of two or greater (see dotted demarcation line in Table 5.3). Considering Table 5.3, the most used concepts were information security (14), followed by criminology and investigations (9), and security management (7). To support the assumptions that these concepts were appropriate category descriptors, Table 5.3 was compared to the ASIS security common knowledge categories (American Society for Industrial Security, 2000). Excluding security and asset protection, the comparison from the initial list of 17 concepts resulted in 13 (76.5%) concepts being considered appropriate categories, with only minor clarification in category definition. For example in Table 5.3 the category technology was put forward, whereas the ASIS common knowledge category used integrated security systems. These terms resulted in a final category label of security technology.

The remaining four (23.5%) concepts were not inclusive in either Table 5.3 or the ASIS security common knowledge categories, resulting in these concepts considered subordinate concepts. These concepts comprised accounting, access control, government security and intrusion detection. Accounting was considered a generic business function. Access control and intrusion detection were considered subordinate concepts of security technology. Government security was considered a subordinate concept of industrial
procedures. These concepts were therefore suitable for inclusion as more explicit concepts, not as knowledge categories.

During the course concept extraction, it was found that a number of subordinate concepts could not be located within predefined knowledge categories. As concepts were considered to be mutually inclusive, an additional category of principles was included in Table 5.3. Although this category had a low frequency count (1), the ASIS common knowledge category list did have a concept defined security concepts (American Society for Industrial Security, 2000). Analysis resulted in a final 14 security knowledge categories (Table 5.4) being tabulated.

Table 5.4

<table>
<thead>
<tr>
<th>Security knowledge categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security categories descriptors</td>
</tr>
<tr>
<td>Criminology</td>
</tr>
<tr>
<td>Facility management</td>
</tr>
<tr>
<td>Investigations</td>
</tr>
<tr>
<td>Safety</td>
</tr>
<tr>
<td>Security management</td>
</tr>
</tbody>
</table>

5.5 Operationalise category demarcation

The security knowledge categories were considered to have the following demarcation, as it was not the intent of the study to provide concept definition:

- **Criminology**: Theories, principles and concepts that consider the scientific study of crime (The Angus & Roberston, 1992) and victimology, particularly why crime is committed. This category did not consider situational crime prevention (see principles).

- **Emergency/contingency planning**: Disaster, crisis, incident and business continuity management that generally requires an initial response from government emergency services and support by site security, followed by further action from the organisation itself. The purpose of emergency planning is to allow “the organisation to achieve basic resumption of its business processes” (American Society for Industrial Security, 2000, p. 29) and includes business continuity management.
(Standards Australia, 2004c). This category did not consider risk management, however, it could be implied that this category is a subset on risk management – a risk mitigation strategy.

- **Facility management**: The technique, process and practice of managing or controlling organisational resources to deliver the function of the built environment, in particular, an organisation’s facilities (Langston & Lauge-Kristensen, 2002). The category was considered to include facility technology and management practices, for example facility design, strategic planning, fixed plant and equipment, plant maintenance, energy management, etc.

- **Fire science**: Theories, principles and concepts that consider the scientific study and treatment of fire, including building technology and the management of life safety and fire protection.

- **Industrial security**: Application of security within specific industries, for example aviation security, critical infrastructure protection, government security, campus security, retail security, etc.

- **Information and computing**: Theories, principles, concepts and practices that consider protection methods within the digital environment, including computer technology, hardware and software. Examples may include firewalls, viruses, honey-pots, etc.

- **Investigations**: Theories, principles, concepts and practices of security investigations, both process and technology. For example, the legal requirement during a private investigation, evidence admissibility, covert surveillance management, etc.

- **Physical security**: Theories, principles and concepts that use people, equipment (Garcia, 2001) and the built environment to control access to an organisation’s assets, for example lock and keys, grills, etc.

- **Principles**: Theories, principles and concepts that consider the scientific study of security, for example defence in depth (DinD), deter, detect, delay and respond (D³R), crime prevention through environmental design (CPTED), security decay, etc.

- **Security risk management**: Theories, principles, concepts and practices that considers risk and risk management. Risk management may combine many
disciplinary areas including, however not exclusively, mathematics, management, business and psychology. According to the Risk Management AS/NZS4360 Standard, risk management “is an integral part of good management … an iterative process of continuous improvement that is best embedded into existing practices or business process” (2004a, p. 7).

- Safety: Theories, principles, concepts and practices that considers a process for a safe and healthy work environment (American Society for Industrial Security, 2000). In the context of the study, this concept is considered to be Occupational Health and Safety, not necessarily the provision of safety provided by the function of security.

- Security law: Theories, principles, concepts, process and practices that consider how law affects organisational security, including civil, criminal, liabilities, counter strategies, etc.

- Security management: Theories, principles, concepts, technique, process and practice of managing or controlling organisational resources to deliver the function of security (American Society for Industrial Security, 2000; The Angus & Roberston, 1992). This category may include policy and procedures, training, awareness, finance, contracting, resource allocation, etc.

- Security technology: Specific security technology applied in the protection of assets, for example intruder detection systems, closed circuit television (CCTV), access control, biometric systems, etc.

The position and frequency of a word has a relevance on its importance; nevertheless, the word title did not necessarily represent content or indicate importance (Fresno & Ribeiro, 2004). Therefore, the previous examination of the course titles only provided an initial analysis, with additional concept extraction and analysis of the seven course contents necessary.

5.6 Extracted security concepts from the seven selected security courses

The seven security course transcripts (Table 5.2) comprised the award’s major units of study and included unit title, learning objectives and content overview. Each course transcript was further sanitised to retain only security related concepts and placed in
alphabetical order. Course list of concepts were amalgamated and repeated concepts removed to produce a final list of 2001 security concepts (Appendix E) referred to as the *source document*. Concepts were retained with the following considerations:

1. All concepts have a *security* context, unless otherwise specified. Examples include *facility management* listed as *facility management*, whereas *security management* was listed as *management* and *physical review* refers to a *physical security review*.

2. Security guard included the amalgamation of the concept *security officer*.

3. Concepts retained hierarchical concept order, for example *access control systems components*.

### 5.7 Development and tabulation of the security risk management knowledge category with subordinate concepts

The security risk management concepts required extraction from the *source document* concept list (Appendix E) and insertion under the security risk management category. The extraction process applied an approach that ensured that this phase resulted in a reliable and valid security risk management category. Analysis applied a convergence approach, using Risk Management AS/NZS4360:2004 Standard, the pilot study results (Chapter 4) and source document (Appendix E). To provide further support to the security risk management category concept list, experts validated the final list. An overview of the security risk management category concept extraction and tabulation methodology is provided (Figure 5.1).
In examining Appendix E, concepts that were considered relevant to security risk were tabulated under the security risk management category. To support the assumption that concepts should be located within the security risk management category, concepts were compared to concepts used in AS/NZS4360 Risk Management Standard (Standards Australia, 2004a). The Australian Standard is considered “almost a de facto global standard” (Jay, 2005, p. 2) and has become “recognised internationally as best practice” (Jones & Smith, 2005, p. 23) on dealing with risk, having been used in Canada, United Kingdom and translated into Cantonese, Mandarin, Japanese, Korean, French and Spanish (Jay, 2005). The standard is widely used by security professionals within Australia (Jones & Smith, 2005).

Concepts were extracted from Appendix E into the security risk management category, resulting in a subordinate concept list of 55 concepts. LIWC was applied to the course transcripts and resulted in the concept frequency analysis (Table 5.5).
Table 5.5

*Initial security risk management category and supporting concept frequency count*

<table>
<thead>
<tr>
<th>Concept</th>
<th>No.</th>
<th>%</th>
<th>Concept</th>
<th>No.</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>162</td>
<td>6.48</td>
<td>Record/s</td>
<td>8</td>
<td>0.32</td>
</tr>
<tr>
<td>Risk</td>
<td>110</td>
<td>4.40</td>
<td>Authority</td>
<td>7</td>
<td>0.28</td>
</tr>
<tr>
<td>Control</td>
<td>78</td>
<td>3.12</td>
<td>Decision-making</td>
<td>7</td>
<td>0.28</td>
</tr>
<tr>
<td>Identify</td>
<td>78</td>
<td>3.12</td>
<td>Regulation</td>
<td>7</td>
<td>0.28</td>
</tr>
<tr>
<td>Analysis</td>
<td>63</td>
<td>2.48</td>
<td>Model</td>
<td>7</td>
<td>0.28</td>
</tr>
<tr>
<td>Policy</td>
<td>30</td>
<td>1.20</td>
<td>Framework</td>
<td>5</td>
<td>0.20</td>
</tr>
<tr>
<td>System</td>
<td>30</td>
<td>1.20</td>
<td>Probability</td>
<td>5</td>
<td>0.20</td>
</tr>
<tr>
<td>Process</td>
<td>26</td>
<td>1.00</td>
<td>Consequence</td>
<td>4</td>
<td>0.16</td>
</tr>
<tr>
<td>Legal</td>
<td>24</td>
<td>0.96</td>
<td>Perception</td>
<td>4</td>
<td>0.16</td>
</tr>
<tr>
<td>Environment</td>
<td>23</td>
<td>0.92</td>
<td>Society</td>
<td>4</td>
<td>0.16</td>
</tr>
<tr>
<td>Implement</td>
<td>20</td>
<td>0.80</td>
<td>Statistic</td>
<td>4</td>
<td>0.16</td>
</tr>
<tr>
<td>Loss</td>
<td>19</td>
<td>0.76</td>
<td>SWOT</td>
<td>3</td>
<td>0.12</td>
</tr>
<tr>
<td>Organisation</td>
<td>19</td>
<td>0.76</td>
<td>Activity</td>
<td>2</td>
<td>0.08</td>
</tr>
<tr>
<td>Plan</td>
<td>19</td>
<td>0.76</td>
<td>Audit</td>
<td>2</td>
<td>0.08</td>
</tr>
<tr>
<td>Awareness</td>
<td>17</td>
<td>0.68</td>
<td>Monitor</td>
<td>2</td>
<td>0.08</td>
</tr>
<tr>
<td>Assessment</td>
<td>16</td>
<td>0.64</td>
<td>Business continuity planning</td>
<td>1</td>
<td>0.04</td>
</tr>
<tr>
<td>Data</td>
<td>16</td>
<td>0.64</td>
<td>Cost analysis</td>
<td>1</td>
<td>0.04</td>
</tr>
<tr>
<td>Identification</td>
<td>14</td>
<td>0.56</td>
<td>Hazard</td>
<td>1</td>
<td>0.04</td>
</tr>
<tr>
<td>Business</td>
<td>13</td>
<td>0.52</td>
<td>Issue</td>
<td>1</td>
<td>0.04</td>
</tr>
<tr>
<td>Calculate</td>
<td>12</td>
<td>0.48</td>
<td>Measurement</td>
<td>1</td>
<td>0.04</td>
</tr>
<tr>
<td>Impact</td>
<td>12</td>
<td>0.48</td>
<td>Objective setting</td>
<td>1</td>
<td>0.04</td>
</tr>
<tr>
<td>Communication</td>
<td>10</td>
<td>0.40</td>
<td>Politics</td>
<td>1</td>
<td>0.04</td>
</tr>
<tr>
<td>Evaluation</td>
<td>10</td>
<td>0.40</td>
<td>Potential</td>
<td>1</td>
<td>0.04</td>
</tr>
<tr>
<td>Culture</td>
<td>9</td>
<td>0.36</td>
<td>Qualitative</td>
<td>1</td>
<td>0.04</td>
</tr>
<tr>
<td>Operations</td>
<td>9</td>
<td>0.36</td>
<td>Quantitative</td>
<td>1</td>
<td>0.04</td>
</tr>
<tr>
<td>Decision</td>
<td>8</td>
<td>0.32</td>
<td>Treatment</td>
<td>1</td>
<td>0.04</td>
</tr>
<tr>
<td>Value</td>
<td>8</td>
<td>0.32</td>
<td>Validate</td>
<td>1</td>
<td>0.04</td>
</tr>
<tr>
<td>Threat</td>
<td>8</td>
<td>0.32</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

It was intended that concept inclusion into a knowledge category be mutually inclusive, however, this approach proved to be difficult due to concepts that could have various context. As indicated (see Chapter 3.5.1), the concepts had to be reduced to 13±2 concepts requiring further reduction of Table 5.5. Initial selection was based on concept frequency, supported by concept use within the course transcripts.

Considering Table 5.5, low frequency counts (≥1, 0.04%) were included even though they were not considered significant concepts. This approach was taken to allow the reader to be aware of the possible complex and diverse nature of security risk
management. For example, control was not selected to progress into the final security risk management category when control presented a high frequency count (78, 3.10%). However, on examination of the course transcripts, control was used in the context of access control, key control, CCTV image control, area control, facility management, information and social control. Control was also used within a risk context, nevertheless, this was considered insignificant when compared to other usage. The data concept was also not maintained, as it was used within the context of information security, computer security, law and intelligence. As with control, data was presented within a minimal risk context of “perception, biases and heuristics, and data evaluation” (School of Engineering and Mathematics, 2004b).

Context approach was applied to concepts that had a significant frequency (≥3, 0.12%), resulting in the removal of policy, system, process, legal, environment, implement, loss, organisation, plan and awareness. The examination of course transcripts and concept context resulted in a security risk management category list of concepts (Table 5.6).

<table>
<thead>
<tr>
<th>Security risk management category</th>
<th>Analysis</th>
<th>Assessment</th>
<th>Calculate</th>
<th>Communication</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Culture</td>
<td>Decision</td>
<td>Evaluation</td>
<td>Loss</td>
<td>Risk management</td>
<td></td>
</tr>
<tr>
<td>Perception</td>
<td>Policy</td>
<td>Probability</td>
<td>Threat</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To ensure the reliability of both frequency count and concept context, data were validated by the author’s Associate Supervisor. Ten concepts were selected at random from Table 5.5 and frequency and context measures confirmed, resulting in a high reliability measure of total agreement (100%).

5.8 Expert validation

To further validate the security risk management category and supporting subordinate concepts, four security experts reviewed the category list (Table 5.6) for
appropriateness. Security risk management experts were selected based on the study’s definition of expertise (see Chapters 2 and 3). Experts comprised two academics with international research in security risk and two experienced security risk practitioners. Each expert was individually interviewed, either face-to-face or by telephone, with no contact between participating experts.

The experts were presented with Table 5.6 and asked three questions (Appendix F). The first question proposed that the domain of security risk management could be described by the concepts listed in Table 5.6 and therefore, which of the following concepts did they believe should not belong in the domain of security risk management? This first question was supported by a second question, asking the expert to provide a reason why a concept may not be appropriate for inclusion into the security risk management category. The third and final question asked the experts if they considered if there were any other significant concept they recommend should be included, with a pool of possible security risk management concepts provided to assist the expert?

The experts considered that the list of security risk management concepts were appropriate, with significant agreement (93.1%) between experts. Nevertheless, three of the four experts did state that policy was not a relevant security risk management category concept, with one of the expert’s indicating that policy was an organisational theory (K. Foster, January 18, 2006, personal communication). The only other concept that one of the experts considered may not have been suitable was loss. However, as the exclusion of this concept was put forward by only one of the four experts, loss remained in the risk category. Additional concepts that the experts felt may be appropriate were vulnerability, warnings, control, surprise and indicators.

The concept vulnerability was proposed by two of the four experts, indicating that this concept was an appropriate security risk management concept, although not necessarily significant. Other additional concepts were only recommended by one of the four experts, indicating that these were not significant security risk management concepts. Therefore the low expert consensus removed the need to add these additional concepts to
the category list. Finally, the experts did indicate that a number of the tabulated concepts were subordinate to others, however, once the idea of the hierarchical nature of concepts was put forward, this satisfied the experts. Supported by expert consideration of the risk concepts, the final security risk management concept list was produced (Table 5.7).

Table 5.7

<table>
<thead>
<tr>
<th>Security risk management category</th>
<th>Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis</td>
<td>Evaluation</td>
</tr>
<tr>
<td>Assessment</td>
<td>Loss</td>
</tr>
<tr>
<td>Calculate</td>
<td>Risk management</td>
</tr>
<tr>
<td>Communication</td>
<td>Perception</td>
</tr>
<tr>
<td>Consequence</td>
<td>Probability</td>
</tr>
<tr>
<td>Culture</td>
<td>Risk</td>
</tr>
<tr>
<td>Decision</td>
<td>Threat</td>
</tr>
</tbody>
</table>

5.9 Conclusion

This chapter described Phase one of the research study, being the extraction and tabulation of the security knowledge categories and subordinate concepts of security. In addition, the most relevant concepts were inserted into the security risk management category. To achieve this outcome and respond to Research Question one, international undergraduate tertiary security courses were sourced and examined (N=104), with seven final courses selected for content analysis. The security course transcripts were sanitised to provide the source document and concepts extracted, using Linguistic Inquiry and Word Count (LIWC) (Pennebaker, et al., 2001) and resulting in a list of 2001 security concepts (Appendix E).

According to the selected security courses, further analysis resulted in the development and presentation of 14 security knowledge categories (Table 5.4). These knowledge categories comprised criminology, emergency/contingency planning, facility management, fire science, industrial security, information and computing, investigations, physical security, security principles, security risk management, safety, security law, security management and security technology.
From the 2001 security concepts (Appendix E) and using LIWC (Pennebaker, et al., 2001), further analysis extracted the draft security risk management concepts list (Table 5.5). Convergence between Risk Management AS/NZS4360:2004 Standard and the pilot study (Chapter 4) resulted in a final security risk management concept list (Table 5.7). In addition, four security experts provided significant validation (93.1%) of the security risk management concept list, ensuring progression onto the study Phase two MDS knowledge structure.
CHAPTER 6
PHASE TWO: MDS KNOWLEDGE STRUCTURE

6.1 Introduction

Phase two of the study, describing the development of the psychometric MDS security risk management concept map, is presented in this chapter. Research Question two asked: What is the expert knowledge structure and subordinate concepts of security risk management as measured by multidimensional scaling? To achieve this outcome, the chapter is divided into a number of discrete sections. The first section (6.2) embedded the security risk management category subordinate concepts into the psychometric MDS concept mapping survey. The MDS concept mapping survey was then completed by 29 security experts and the proceeding data analysed (6.3), resulting in the presentation of the MDS spatial knowledge structure of the security risk management (SRM) category. An overview of Phase two psychometric MDS concept map development is presented (Figure 6.1).

![Diagram of MDS concept mapping methodology](image)

Figure 6.1 Phase 2: Psychometric MDS concept mapping methodology

With insertion of propositional linkages into the security risk management knowledge structure, section (6.4) developed and presented the psychometric MDS security risk management concept map. The primary and pilot study psychometric concept maps
were then compared for concept structure (6.5), resulting in significant structural commonality. Finally, the psychometric security risk management concept map reliability and validity values are presented (6.6), followed by the conclusion of the chapter (6.7).

6.2 Research instrument: Psychometric MDS concept mapping survey

From the security risk management category and subordinate concepts (Table 5.7), the psychometric MDS concept mapping survey was developed. The MDS concept mapping survey embedded the 14 security risk management concepts to allow paired comparison between each concept (Appendix H). The MDS survey also was supported by an introductory letter (Appendix G), providing an overview of the study and completion instructions for the expert participants. The MDS survey incorporated the changes as recommended in the pilot study (see Chapter 4.3). Experts indicated on a sliding scale the concepts that they considered were related (similar) or unrelated (dissimilar). These measures were then averaged as a method to identify and understand group perceptions (Tull & Hawkins, 1993).

Security risk management experts were selected by non-probability dimensional sampling and based on the study’s definition of expertise (see Chapter 2 and Chapter 3). An initial number of experts were sourced, based on their known standing in the security risk management community. Each expert was asked to recommend additional leading security risk management practitioners or academics. From the peer recommendations, these additional experts were contacted until the proposed study sampling size (N=30), with consideration of non-completion, was attained.

On contact, each expert was given a synopsis of the study and requested that they participate in the MDS concept mapping survey. The MDS survey was administered to the experts via a number of methods, dependant on geographical location of the expert from the researcher. Administration generally comprised of the MDS survey and supporting introductory letter being emailed direct to the expert. On completion of the MDS survey, experts returned the survey by post, facsimile or email. A total of 42
surveys were sent to selected experts with a total of 29 completed, resulting in a 69% completion rate.

Two of the 29 experts provided comment on the MDS concept mapping survey. Both experts indicated that in their opinion, the survey was difficult to complete. Draper found the survey difficult in discerning the differences between ideas, as in his opinion all concepts were highly related (R. Draper, personal communication, April 20, 2006). However, once the research methodology was explained in greater depth than was presented by the introductory letter, Draper considered that the survey was appropriate. Cross stated that she “sees most of the words as overlapping areas in a knowledge space” (J. Cross, personal communication, March 20, 2006) and was therefore unable to complete the survey. Cross also rightly stated that some of the concepts “in the English language mean several things or have different implications” (J. Cross, personal communication, March 20, 2006).

In addition, the completed MDS concept mapping surveys did not meet the intended sampling number (N=30) recommended in Chapter 3. The original sample size was selected to reduce the MDS STRESS1 measure (Cheng, 2004; Cohen, et al., 2002), however, not exceeded due to the non-probability sampling method applied to expert selection. Nevertheless, completed MDS surveys reached 97% of the original proposed number allowing commencement of data analysis.

6.3 MDS data analysis
Data were extracted from the completed psychometric MDS concept mapping surveys and inserted into a spread sheet, becoming the Phase two source data. Data were summed and MDS analysis applied. Primary analysis, in response to Research Question two, required MDS ALSCAL to present the psychometric MDS knowledge structure of the security risk management category and resulted in the MDS spatial map (Figure 6.2).
In the context of the study, the MDS spatial map presented the knowledge structure or *framework* of the security risk management category and supporting subordinate concepts. The MDS *metric* structure was retained throughout the security risk management concept map development, as it was proposed that concept proximity measures indicated conceptual relationships. From the spatial knowledge structure, propositional linkages and labels could be inserted to give the map meaning (Bennett & Rolheiser, 2001).

### 6.4 Psychometric concept map development

Five additional security experts were asked to insert propositional linkages and supporting labels to develop the psychometric MDS security risk management concept map (see Chapter 4). These security experts were selected based on non-probability dimensional sampling and expanded from the previous expert peer group, although these experts were all based in the same geographical locality as the researcher. The MDS
security risk management knowledge structure (Figure 6.2) had both dimensional x and y axis data removed, leaving only knowledge structure. The structure was then rotated by approximately 35°, locating the concept *risk* upper most and resulting in Figure 6.3.

Figure 6.3 MDS concept knowledge structure ready for propositional linkage insertion
A Delphi (Cohen, et al., 2003; Ethigie & Ehigie, 2005) or convergence approach was then used, where the researcher independently presented three of the five experts with the MDS security risk management knowledge structure (Figure 6.3) and asked each expert to insert their proposed propositional linkages and supporting labels. The three expert annotated maps were then compared with each other, common linkages retained and placed onto a single concept map. This single concept map was again presented to two additional experts for their propositional linkage comment.

The three expert annotation of the security risk management knowledge structure resulted in a number of diverse propositional linkages and supporting labels. Between the 14 security risk management concepts, there were a number of linkages that were common between at least two or more of the three experts (Table 6.1).

Table 6.1

<table>
<thead>
<tr>
<th>Concept linkages</th>
</tr>
</thead>
<tbody>
<tr>
<td>risk - risk management</td>
</tr>
<tr>
<td>evaluation – analysis</td>
</tr>
<tr>
<td>culture – perception</td>
</tr>
<tr>
<td>perception – threat</td>
</tr>
<tr>
<td>risk management - communication</td>
</tr>
<tr>
<td>consequence – loss</td>
</tr>
<tr>
<td>loss – decision</td>
</tr>
<tr>
<td>assessment – evaluation</td>
</tr>
<tr>
<td>assessment - threat</td>
</tr>
<tr>
<td>culture - threat</td>
</tr>
<tr>
<td>communication - threat</td>
</tr>
<tr>
<td>probability – consequence</td>
</tr>
<tr>
<td>consequence - analysis</td>
</tr>
</tbody>
</table>

The more common linkages (≥67%) provided justification for the insertion of a propositional linkage into the initial draft psychometric MDS security risk management concept map. This approach also considered the conceptual relationships of concepts, based on spatial proximity. The result produced the initial draft psychometric MDS security risk management concept map (Figure 6.4).
Once the initial psychometric MDS security risk management concept map was produced, two additional experts provided opinion on the propositional linkages. These two experts did not indicate that the structure was inappropriate or that the linkages were generally invalid. However, both experts inserted additional propositional linkages and
proposed alternative labels. One of the two experts inserted an additional propositional linkage between the concepts *analysis* and *threat*, stating that “I would see the linkage here [as] analysis occurs before loss” (Z. Gurdon, personal communication, 16 May 2006).

The two additional experts provided significant disagreement on the security risk management map propositional labels, with limited commonality between experts. From the 16 labels the map presented, one expert recommended eight alternatives (50%) and the second expert recommended four alternatives (25%). Label changes (Table 6.2) were made on the advice of the two additional experts and on reflection to the previous three expert annotated concept maps.

Table 6.2

<table>
<thead>
<tr>
<th>Concept link</th>
<th>Initial label</th>
<th>Final label</th>
</tr>
</thead>
<tbody>
<tr>
<td>culture to threat</td>
<td>can influence</td>
<td>can influence awareness of</td>
</tr>
<tr>
<td>perception to threat</td>
<td>can influence</td>
<td>can influence awareness of</td>
</tr>
<tr>
<td>probability to consequence</td>
<td>is an impending</td>
<td>is measured with</td>
</tr>
<tr>
<td>threat to loss</td>
<td>lead to</td>
<td>may result in</td>
</tr>
<tr>
<td>analysis to loss</td>
<td>mitigates against</td>
<td>defines</td>
</tr>
</tbody>
</table>

The low validity of the propositional labels were significant because the labels were designed to provide understanding (Bennett & Rolheiser, 2001; Eysenck & Keane, 2002) and reflected the results found in the pilot study (Chapter 4). There appeared to be no previous research that had addressed this issue in concept mapping, resulting in a need for future research into this aspect (Chapter 9.3.2). However, in considering the final result from the pilot study, it was decided that the most robust labels would be retained and that the security risk management map could progress onto the next study phase. Consequently, the final psychometric MDS security risk management concept map was presented (Figure 6.5).
6.5 Primary and pilot studies concept maps comparison

Where common subordinate concepts had been examined, the knowledge structure of the psychometric MDS security risk management concept map (Figure 6.5) was compared with the pilot study psychometric security risk management concept map
The psychometric security risk management structures had both been rotated to locate the concept risk at their upper most spatial points, nevertheless, both concept maps demonstrated similar significant structural characteristics.

The concepts of risk and risk management exhibited close proximity, with risk management located subordinate to risk. In both maps, threat displayed a relative central spatial location. Communication maintained a moderate proximity and subordinate locality to threat. Probability and consequence displayed a spatial sequential and adjoining proximity structure. Decision was outlying on the opposing extreme of both concept maps. From the 10 common concepts used between the pilot and primary studies, seven concepts displayed close or moderate structural proximity.

The remaining three concepts that did not provide a spatially similar structure included the concepts culture, perception and analysis. Between concept maps, perception displayed a moderate change in spatial proximity, whereas analysis and culture were both outlying. Metric distances between both pilot and primary studies concept maps were not compared, because these measures were not appropriate with differing MDS spatial structures. However, ranking measures could have been applied. Metric measurements were not further considered within the context of the study, however, this technique could be considered for further research (Chapter 9.3.2).

**6.6 Phase two: Reliability and validity**

The source data (see Section 6.3) from the psychometric MDS concept mapping survey were compiled and tested for reliability and validity. Reliability was tested using Cronbach’s Alpha, which produced a high (α=0.93) value. Concurrent validity was tested using Pearson’s two tailed correlation at ≥95% confidence level between expert’s responses, producing a moderate total result (r=0.32, SD0.19).

MDS ALSCAL stress measured an inappropriate high goodness-of-fit (STRESS1=0.28, RSQ=0.64), as ≤0.15 represents a moderate two-dimensional representation (Cheng, 2004). Therefore according to the MDS STRESS1 measure, not all concepts were
necessarily in the most appropriate spatial locality. Nevertheless, this measure had to be considered in relation to the expert validation (see Section 6.4), and how both pilot and primary studies appeared to produce robust psychometric concept maps (see Section 6.5). The MDS STRESS1 was not ideal, with other mitigating factors appearing to reduce the importance of this measure. However, the MDS STRESS1 did indicate that further analysis was required, which was completed through reviewing Phase two source data measures.

As indicated by the MDS STRESS1, a number of concepts appeared to be less reliable than others. On review of the Phase two source data, the concepts of communication and culture produced higher than average (M1.77, SD0.14) expert standard deviation measures between concepts. Between communication and the other 14 risk management concepts, 79% of measures produced a high ($\leq$M2.00) standard deviation (M2.42, SD0.18). With culture, 64% of the comparison measures produced high ($\leq$M2.00) standard deviation (M2.32, SD0.16). The remaining concept measures were not significantly different [t(14)=1.77, p=\textless0.000].

6.7 Conclusion
Phase two of the research study, being the development of the psychometric MDS security risk management concept map, was described in this chapter. To achieve this outcome and respond to Research Question two, the security risk management category subordinate concepts were embedded into the MDS concept mapping survey and completed by 29 security experts. The data analysis resulted in the presentation of the psychometric MDS knowledge structure of the security risk management category.

The psychometric security risk management concept map was then developed with five security experts inserting propositional linkages and supporting labels. Propositional linkages and labels insertion employed data convergence (Delphi method) to produce a final psychometric concept map. The experts did provide significant disagreement on propositional labels at each stage of the map’s development, indicating a low degree of label validity. Nevertheless, from expert opinion it was concluded that the most robust
labels would be retained and the security risk management concept map progressed onto Phase three of the study. Following Phase two, the final psychometric MDS security risk management concept map was presented (Figure 6.5).

The primary study (Figure 6.5) and pilot study (Figure 4.3) psychometric concept maps also were compared for concept knowledge structure, resulting in significant structural commonality between concept maps. The structural similarity appeared to support the robustness of the psychometric security risk management map’s structures and propositional linkages, reinforcing the decision to progress the study to Phase three. Finally, the psychometric security risk management concept map’s reliability and validity were presented, producing a high ($\alpha=0.93$) Cronbach’s Alpha measure and a moderate ($r=0.32$, SD0.19) Pearson’s two tailed correlation. MDS STRESS1 did produce an inappropriate high stress measure (STRESS1=0.28, RSQ=0.64), nevertheless this was negated when considering the other measures, namely, a comparison between the primary and pilot study concept maps, and expert opinion.
Chapter 7
Phase Three: Expert Knowledge Structure Validation

7.1 Introduction
Phase three of the study, describing the expert inquiry of the psychometric MDS security risk management concept map is presented in this chapter. Research Question three asked: What is the expert knowledge structure and subordinate concepts of security risk management as measured by interviews? To achieve this outcome, the chapter is divided into a number of discrete sections. The first section (7.2) developed the expert interview to enable discussion that could confirm or deny the predefined assertions. Once the instrument was developed, the opinions of security experts were sourced through semi-structured interviews to validate the assertions (7.3). Each of the four pre-defined assertions are considered, with the expert opinion presented as supporting or contradictory evidence (7.4 to 7.7). The chapter is summarised with a conclusion (7.8).

7.2 Development of the expert interviews
The semi-structured expert interview was developed from the pilot study instrument (Appendix A). As with the pilot study, this interview was a paper-based analysis of the psychometric MDS security risk management concept map presented in Phase two (Figure 6.5). The interview was designed to further examine the assertions which were developed in response to Research Question three. The assertions developed during the pilot study were retained, as they proved to be appropriate at that stage of the study. The four assertions are presented below:

- Assertion 1: Experts considered that the psychometric MDS concept map for the category of security risk management presented a suitable foundation knowledge structure.
- Assertion 2: The sequential nature of the concept clusters represented expert decision-making.
 Assertion 3: Experts considered that although the psychometric concept map represented the category security risk management, there was greater complexity than presented.

Assertion 4: The psychometric security risk management concept map propositions did not effectively represent concept linkage.

The expert interview (Appendix I) comprised 13 questions (Table 7.1), providing guidance to the interviewee and expert. The instrument focused on various aspects of the security risk management concept map and a number of questions related to each assertion (Table 7.2). In addition, the overall map structure, spatial proximity of concepts, concept relationships and clusters, and propositional linkages were considered.

Table 7.1

Phase three: Expert interview questions

<table>
<thead>
<tr>
<th>No.</th>
<th>Interview question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The concept map shows an overall structure for security risk management. Do you consider that this whole structure describes the ideas underlying risk?</td>
</tr>
<tr>
<td>2</td>
<td>On the concept map, do you consider if there are any inappropriately located ideas?</td>
</tr>
<tr>
<td>3</td>
<td>Do the think that the ideas represented in the security risk management concept map represents your thoughts on this topic?</td>
</tr>
<tr>
<td>4</td>
<td>From your knowledge of security risk management, are there any other important ideas that could be included?</td>
</tr>
<tr>
<td>5</td>
<td>Do you believe that this structure shows appropriate relationships in the ideas of security risk management?</td>
</tr>
<tr>
<td>6</td>
<td>On the concept map threat would appear to be a central theme, what are your comments regarding this?</td>
</tr>
<tr>
<td>7</td>
<td>Consider the ideas risk, risk management, calculate/assessment, threat, loss and decision. Do you think that this structure and/or links are justified? Why?</td>
</tr>
<tr>
<td>8</td>
<td>Consider the ideas probability, consequence and analysis. In your opinion, does this structure appear appropriate?</td>
</tr>
<tr>
<td>9</td>
<td>Culture and perception are clustered in close proximity to threat. What are your thoughts on this cluster?</td>
</tr>
<tr>
<td>10</td>
<td>Would you like to add or change any link (explain link)?</td>
</tr>
<tr>
<td>11</td>
<td>Would you like to add or change any linking label (explain label)?</td>
</tr>
<tr>
<td>12</td>
<td>Do you consider that this concept map provides a general consensus of security risk management ideas and their relationships?</td>
</tr>
<tr>
<td>13</td>
<td>Do you have any final comments?</td>
</tr>
</tbody>
</table>
Table 7.2

**Phase three: Expert interview – assertion relationship to questions**

<table>
<thead>
<tr>
<th>Assertion</th>
<th>Interview questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assertion 1</td>
<td>1, 2, 3, 4, 12 and 13</td>
</tr>
<tr>
<td>Assertion 2</td>
<td>5, 6, 7, 8 and 9</td>
</tr>
<tr>
<td>Assertion 3</td>
<td>10, 11, 12 and 13</td>
</tr>
<tr>
<td>Assertion 4</td>
<td>10, 11, 12 and 13</td>
</tr>
</tbody>
</table>

### 7.3 Administration of the expert interviews

Six experts (Table 7.3) were selected by non-probability purposive sampling (Chapter 3.3), with initial experts providing further peer selection. As previously discussed, consideration was given to who may be defined as expert and group heterogeneity.

Table 7.3

**Phase three: The six expert’s profiles**

<table>
<thead>
<tr>
<th>Expert pseudonym</th>
<th>Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Andrew</td>
<td>Engineer, security consultant and author, with 9 years experience in commercial security, security engineering design and development, and security education.</td>
</tr>
<tr>
<td>Frazer</td>
<td>Security consultant with a tertiary undergraduate degree in security and 14 years commercial security experience.</td>
</tr>
<tr>
<td>Greg</td>
<td>Security manager, having 28 years experience in Federal Government security and with postgraduate tertiary degrees.</td>
</tr>
<tr>
<td>Kate</td>
<td>Security director with 15 years experience with an international gaming and entertainment company, and postgraduate degrees. Actively involved in many security associations and government bodies.</td>
</tr>
<tr>
<td>Kerran</td>
<td>Engineer, security consultant and company owner with 31 years experience in commercial security and correctional facility design. Actively involved in many security associations and government bodies.</td>
</tr>
<tr>
<td>Zack</td>
<td>Regional corporate security manager with tertiary postgraduate degrees and 10 years experience. Manages the security function for a large telecommunications company.</td>
</tr>
</tbody>
</table>

The experts were presented with the psychometric security risk management concept map one week prior to the programmed interview. This approach allowed the expert to consider the psychometric concept map in greater depth and allow opportunity for reflection. Through one-to-one semi-structured interviews, which were audible recorded and transcribed (see Appendix J for one of the six expert interview transcripts), the expert’s opinions on the map were analysed and interpretations made. Subtle non-verbal
language was also noted and inserted into the transcriptions. Data were identified and used to respond to the assertions.

7.4 Assertion 1: Experts considered that the MDS concept map for the category of security risk management presented a suitable foundation knowledge structure

Assertion one sourced the expert opinion on whether the psychometric concept map represented a suitable foundation knowledge structure for security risk management. Experts were asked a number of discrete questions regarding the map’s structure, spatial location of concepts, concept clusters, appropriateness of concepts and whether, in their opinion, additional security risk management concepts should have been included.

7.4.1 Concept map structure

When the experts were asked if the concept map represented an overall structure of security risk management, there was generally an affirmative agreement. As Andrew stated “it certainly is a good representation of how the concepts fit in … I would absolutely agree”. This opinion was supported by Zack who stated that “I think it does cover the key elements of risk management” and Kate who stated that “the time I’ve spent looking at it I believe that it does, it is a fair representation.”

In contrast, Frazer indicated that the map only covered “the main overlying principles … there are other areas where you might be able to delve down even more” however, later Frazer did state that “I think it provides a general overview of the whole [security risk management] process”. Frazer also considered that additional ideas could include concepts that attempt to explain why people commit crime. Nevertheless, among the six experts, Frazer was the only expert to propose this aspect. Generally, there was strong agreement that the concept map described the ideas underlying security risk management.

Further to the map’s structure, the opinions of each expert were sought on whether the concept map represented their thoughts on security risk management? Again, all experts agreed that the map generally presented their views on security risk management. Kerran
stated that “yes, to a large degree the map does reflect my thoughts on this topic” and Kate stated that “I agree ... it makes a lot of sense”. Andrew also agreed that the map was “a good model” and that the map did generally represent his ideas of security risk management, supported by Zack who stated that “I think it’s pretty fair”. Frazer also agreed “to a certain extent”, although “you might be able to go down a bit further … with differing ideas or perceptions”, indicating that risk is “very subjective”. When considering all expert opinions, there was a high degree of common and independent consensus from the experts that the concept map did represent their idea of security risk management.

7.4.2 Spatial locality of concepts
As a central theme, threat appeared to be well supported by the experts. As Kerran stated “identification of threat is critical and threat is a central theme”. Andrew and Kate both commented that “threat is an essential thing … if there’s no threat ... there is no risk” and that “the nature of threat is that without it the need for risk management doesn’t exist”. This proposition was supported by Zack, who stated that threat “is a key concept”, although he did propose that it should have been located closer to risk and risk management, and that threat should come before calculate, assess and evaluate. It was Zack’s opinion that you need to understand and identify threat before you can calculate risk. Kate, as a security practitioner, highlighted the central theme of threat in applied security risk management:

I’ve just completed my risk matrix review for the next financial year and it started out ... with a whole serious of threats to the organisation that were oriented towards security. Over the last 12 months we’ve been putting processes and strategies in place to reduce those threats or put us in the position where we’re willing, as an organisation, to accept them.

7.4.3 Concept clusters
The experts were asked if they considered if any concept was inappropriately located within the concept map, resulting in discussions on two concept clusters and a discrete concept. Clusters of assessment, calculate and evaluation, and probability, consequence and analysis were discussed, with loss as the discrete concept.
Frazer indicated that there should be a link from *assessment* to the cluster of *probability, consequence* and *analysis*. Andrew recommended *analysis*, as according to Australian Standard AS4360:2004 these functions are part of risk assessment and could have been located closer to *assessment* and *evaluation*. Whereas the concept map presented *assessment* and *evaluation* as a close proximity cluster, with *analysis* as an outlier. This broad spatial separation between these concepts was also queried by Zack, when he “questioned the position of assessment and calculation, with probability, consequence and analysis”.

However, Kerran proposed that *assessment/calculate* could be integrated as a single idea and that perhaps these two ideas consider the quantitative and qualitative aspect [of security risk management]”. To some degree the clusters of *calculate/assessment* and *probability, consequence and analysis* were raised by the majority of the experts, indicating that the map has some degree of error in the presentation of these concepts. Nevertheless, the majority of experts considered the cluster *probability, consequence and analysis* was valid.

Andrew indicated that the concept map could have presented *loss* and *consequence* in closer spatial proximity. Later Andrew proposed that individuals may argue the validity of this locality, concluding that there were no concepts “glaringly out”. Frazer also mentioned *loss*, considering the interpretation of meaning and whether *loss* referred to “treatment plans to mitigate that loss”. This idea was supported by Kerran, who stated that “loss is not the right word … as this considers only negative cogitations”.

### 7.4.4 Additional security risk management concepts

When the experts were asked if, in their opinion, there were any important concepts not presented or were inappropriate, five concepts were proposed, namely *treatment, vulnerability, control, calculate* and *human element*. Of these five concepts, only two common concepts were raised by two or more experts; for example, Kate proposed that “I would have liked to have seen … treating threat [italics added].” Andrew and Frazer also both considered that *treatment* could have been included. However, Andrew did
conclude that “everything else that I would have included is already in here”. Kerran took another approach and proposed mitigation; mitigation and treatment could be considered similar concepts and are therefore interchangeable. Two experts also indicated that vulnerability was an important security related concept. Andrew stated that security risk management could be considered a “triangle, with threat, assets and vulnerability”, while Zack put forward vulnerability as “most relevant” in security risk management.

Kerran stated that “calculate and assessment could be looped as a single item”. Andrew also proposed a similar idea; that calculate may be an appropriate risk concept, however, calculate could “probably be a subset of assessment”. This proposal appeared relevant when considering the close proximity of these concepts, however, these two experts were the only ones to propose this amalgamation. In addition, Kerran proposed that “there is no consideration of control, although I am not sure where this would go”. Finally, Kate raised her belief that the human aspect should be considered and that from a “top down perspective, the human aspect of risk management can influence [security risk management]”. However, Kate and Kerran were the only experts to explicitly recommend these two discrete concept issues.

7.4.5 Assertion 1 conclusion
Assertion one stated that security experts considered that the psychometric MDS security risk management concept map presented a suitable foundation knowledge structure. There was strong evidence to support this assertion, as according to the experts MDS developed and structured an appropriate valid concept map of security risk management. Evidence considered the expert’s opinion on the map’s general structure, spatial representation, central theme of threat, and discrete concept locations and inclusion (Table 7.4).
Table 7.4

*Phase three: Assertion one – expert comments*

<table>
<thead>
<tr>
<th>Supporting evidence</th>
<th>Expert support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Representation of the psychometric security risk management concept map</td>
<td>100%</td>
</tr>
<tr>
<td>The psychometric concept map described their ideas of security risk management</td>
<td>100%</td>
</tr>
<tr>
<td><em>Threat</em> – an appropriate central idea of security risk management</td>
<td>100%</td>
</tr>
<tr>
<td>Security risk management concept map structure</td>
<td>67%</td>
</tr>
<tr>
<td>Concept cluster – varying expert support dependant on cluster</td>
<td>100% - 50%</td>
</tr>
<tr>
<td>Inclusive nature of security risk management concepts</td>
<td>100%</td>
</tr>
<tr>
<td>Missing concepts - <em>treatment</em> and <em>vulnerability</em></td>
<td>50% - 33%</td>
</tr>
</tbody>
</table>

All six experts generally supported the psychometric security risk management concept map representation, with only Frazer commenting that the concept map only represented the “principal ideas of risk”. The concept map’s representation was also supported by the individual expert’s agreement that the map generally described their ideas underlying security risk management. *Threat* proved to be a fundamental and pivotal idea underlying security risk management. The map located *threat* within a spatially central location, with all other concepts surrounding *threat*. All experts strongly supported the fundamental nature and central conduit that *threat* appeared to represent within security risk management.

Generally there were concurrent comments on the concept map’s structure that implied that the spatial locality and therefore the map’s structure was only moderately appropriate. This indicated two propositions; the first supported the MDS STRESS1 measure and the second supported the implicit nature of the knowledge category. MDS stress (STRESS1=0.28) did indicate an inappropriate high measure, indicating that according to the Phase two expert measures not all concepts were located in the most ideal spatial location (see Chapter 6.6). In addition, the implicit nature of some of the concepts may also result in heterogeneous interpretation, in both concept understanding and structural integrity. Both of these factors are likely to decrease the ability of experts to read and understand the concept map, therefore resulting in varying interpretation.
Two concept clusters were primarily considered by the experts. These clusters included the concepts *assessment*, *calculate* and *evaluate*, and *probability*, *consequence* and *analysis*. Three of the six experts proposed that the cluster of *calculate* and *assessment* contained some degree of presentation error. However, no consensus was reached by the experts, with one expert proposing additional propositional linkages to explain the cluster. In addition, the majority of expert’s considered the cluster *probability*, *consequence* and *analysis* was valid.

The experts put forward additional concepts, nevertheless these were only by individuals in isolation. However, both *treatment* and *vulnerability* were proposed by two or more experts, indicating that both discrete concepts appeared to be important ideas within the knowledge category of security risk management. These two concepts were not identified or included in the security risk management map. Finally, based on the evidence presented (Table 7.4) it can be demonstrated that assertion one can be supported, namely, that the experts considered that the psychometric MDS security risk management concept map presented a valid foundation knowledge structure.

### 7.5 Assertion 2: The sequential nature of the concept clusters represented expert decision-making

Assertion two sourced the expert opinion on whether the psychometric MDS security risk management concept map concept clusters represented a degree of expert decision-making? As with assertion one, the experts were asked a number of discrete questions relating to the security risk management map. The concept map’s relationship structure, location of a number of risk concepts, the sequential nature of concepts, spatial concept clusters and the spatial relationships of concepts were considered.

#### 7.5.1 Spatial relationship structure

The experts were asked if they believed that the concept map’s structure represented appropriate relationships for the idea of security risk management? There was strong supportive agreements from the majority of expert’s like “99%, I agree”, “overall, I think it does”, “globally, the relationships are good” and “yes ... I think it flows with a
fairly good structure”. From the six experts, five provided affirmative support for this idea, with the sixth expert stating that – “ask 100% of people and you would get 100% different answers”. However, this expert did conclude with the statement that “I think it is quite good”.

7.5.2 Concept locality

As previously discussed, threat, when compared with the other risk concepts occupied a spatially central location. When the experts completed the MDS concept mapping survey (Chapter 6) it could be argued that from the MDS spatial outcome, the experts considered that threat held a greater relationship with all other security risk concepts then any other single concept. Therefore MDS analysis resulted in the central location of the concept threat within the security risk management concept map. When the experts were asked to comment on this spatial locality various comments were made, however, all considered that threat was a “key concept” or “an essential thing”. All experts strongly supported this idea, with Andrew indicating that “if there’s no threat then there is no risk … so if you’re looking at security risk, having threat in the middle is a good idea”. This idea was supported by Frazer who stated that “risk assessment is based on the threat”, “the other risk concepts underlie threat” and “it is a central point of all … risk assessments”.

Kerran proposed that “threat is a fundamental item that drives risk” and Kate supported this view, when she stated that the “nature of threat is that without it [threat] the need for risk management doesn’t exist”. Greg considered that threat provided the “context of risk” and that “awareness” of a threat supported risk. All experts strongly supported the validity of threat, being a significant and important concept within security risk management. In addition, the experts supported the idea that threat spatially occupied the central location within the concept map. However, as discussed later whether this locality is wholly appropriate is further questioned.
7.5.3 Spatial sequence of concepts

The experts were asked to comment on the sequential concepts of risk, risk management, calculate and/or assessment, threat and loss to decision. Three of the experts indicated that these linkages were “linear” and they “make sense”. However, with regard to the linear sequence all the experts considered that threat should be considered first, as opposed to risk. As Greg and Frazer proposed, threat could be considered “top down”, with Frazer indicating that risk and threat could replace each other. In addition, both Kate and Zack offered threat before risk. These ideas were also supported by Kerran and Andrew, as Andrew stated “I think of threat first, as being a cause of a risk”. Greg felt that this sequence “confirmed process, shown in the real world”. However, Kerran opposed this idea, stating that he did “not believe it was necessarily a thought process”.

Zack stated that the concept map presented “closely grouped” clusters of “risk management, assessment [and] evaluation as key concepts”, that “culture, perception [and] communication ... are key components” and “you’ve got the analytical side of things with probability, consequence and analysis”. Zack concluded that “all of which lead to an actual and a perceived potential view point of loss to a decision”. Zack also indicated that security professionals, due to the nature of the business, focus on pure risk (loss) and that “threat in 99% of cases is going to be a loss”. This view appeared to support the threat to loss proposition.

There appeared to be mixed opinion on whether the experts believed that the sequential structure of the map demonstrated their thought process. Half of the experts agreed that the sequential nature of concepts were valid, although all experts recommended that threat should be considered first – these ideas appeared to contradict each other. Nevertheless, the importance of threat and its central location in the concept map was strongly supported. This aspect opposed, to a degree, the sequential nature of concept location validated by some of the experts. The position of threat in the concept map may indicate that MDS may be more appropriate to develop mental map structure, as opposed to hierarchical concept maps.
7.5.4 Spatial concept clusters

The experts were asked to consider the cluster of probability, consequence and analysis. The majority of expert’s agreed that this cluster was appropriate with comments that included “it’s quite good, quite correct” and “probability, consequence and analysis definitely go together and them being really close together is really good”. As Kerran stated “probability and consequence is measured, resulting in analysis … leading to outcome or loss”. Andrew advised that presenting consequence and probability concepts together “really shows the independence of the two, but the way the two needs to come together to form the overall level [of risk]”.

Frazer proposed that consequence and probability have a “direct relationship” and security professionals must “look at both”. Greg indicated that the cluster was appropriate, as analysis could be overlaid on both consequence and probability, and that analysis has a degree of commonality to both these concepts. Zack stated that the process of security risk management can result in a threat assessment “dealing with consequence and not probability equally”. He further indicated that the sequential nature of probability as measured with consequence was appropriate. There was generally strong support for the probability to analysis cluster of concepts.

Some concept clusters did generate adverse expert discussion, in particular, calculate, assessment and evaluation. The experts all had differing opinions on this cluster, some supportive with the majority adverse. As Frazer stated, “I would like to place a loop around all three concepts and perhaps call this risk assessment”. Also Kerran put forward that “with calculate and assessment, the link between risk management and these two could be considered quantitative and qualitative”. In the opinion of two of the experts, some or all of these concepts should be located spatially closer to the concept analysis, however, no more than two experts provided consensus.
7.5.5 Spatial relationship

Greg, Zack and Frazer all indicated that the organisational background will define the level of perception to threat based on cultural acceptability. This consideration was addressed by Kate, when she stated:

I could put a threat on the table and my boss could say, look that’s never going to happen, don’t worry about it, because his perception of it is that it’s unlikely .. but in reality there may be only two things that need to change within the organisation for it to become a probability, so I think that those communication, culture and perception are absolutely fundamental to risk management.

Kerran supported Kate’s comments, when he stated that “the whole issue of threat is related to perception” and reinforced this consideration with “the cluster is right and more than logical”. Andrew agreed “100%” with culture and perception being closely located, however did not immediately agree with the close relationship to threat. As Andrew stated, “it’s not something I would have immediately thought ... but I certainly agree with the idea that they’re in the middle of all the rest [of the concepts], that makes perfect sense to me”. Nevertheless, this cluster received a strong degree of validity from the six experts.

7.5.6 Assertion 2 conclusion

Assertion two stated that the psychometric security risk management concept map’s sequential nature of concept clusters represented expert decision-making. There was bounded evidence presented in the opinions of the experts to claim that assertion two could not be significantly validated. This evidence included the map’s relationship structure, spatial location of a number of risk concepts, the sequential nature of concepts, spatial concept clusters and the spatial relationships of concepts (Table 7.5).
Table 7.5

Phase three: Assertion two – expert comments

<table>
<thead>
<tr>
<th>Supporting evidence</th>
<th>Expert support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Structure and concept relationships of the psychometric security risk management concept map</td>
<td>100%</td>
</tr>
<tr>
<td>Sequential nature of security risk management concepts, opposing the Pilot Study (see Chapter 4.4.2)</td>
<td>50%</td>
</tr>
<tr>
<td>Sequential nature of security risk management concepts indicating expert decision-making</td>
<td>17% - 0%</td>
</tr>
<tr>
<td>Spatial locality of security risk management concepts</td>
<td>100% - 67%</td>
</tr>
<tr>
<td>Clustering of similar security risk management concepts</td>
<td>100% - 83%</td>
</tr>
</tbody>
</table>

There was strong evidence from the six experts to support the general spatial relationship structure of the concept map, as initially demonstrated by assertion one. Some structural relationship areas of validity were raised, however, these were generally by individual experts and in isolation. There appeared to be mixed opinion by the experts regarding the sequential nature of concepts, particularly risk, risk management, calculate and/or assessment, threat and loss to decision. Half of the experts considered that in their opinion this sequence was valid, in contrast, the other experts considered that threat is considered first. This outcome resulted in only moderate support for the sequential structure of risk to decision concepts, opposing the pilot study (Chapter 4.4.2) where this sequence of concepts was supported.

The importance of threat and its central location in the concept map appeared to be strongly supported, opposing the moderate support for the sequential nature of concept location. The experts presented consensual support for the central locality of threat, with all six experts considered that this location was most appropriate. This degree of conflict resulted in moderate support for the sequential nature of concepts and strong support for the central location of threat. A result which indicates that MDS, in addition to hierarchical structured concept mapping, may be appropriate to develop and present mental maps (see Chapter 2.3).

There was strong agreement by all experts on a number of concept clusters, particularly probability, consequence and analysis, and threat, probability and culture. However,
some concept clusters, primarily those of \textit{calculate}, \textit{assessment} and \textit{evaluation}, did generate adverse discussion, though these comments were generally put forward by single experts, with no consensus.

Assertion two stated that the map’s sequential nature of concept clusters represented expert decision-making. However this assertion was not supported by the majority of experts, although they all strongly supported the map’s structure and the supporting concept relationships. Nevertheless, what may be concluded from this assertion was the degree of interpretation regarding the validity of the map and that the map did not represent an appropriate degree of decision-making. However, the concept map did represent strong concept relationships.

\textbf{7.6 Assertion 3: Experts considered that although the map represented the category security risk management, there was greater complexity than presented}

Assertion three sourced expert opinion regarding the structural complexity of the psychometric MDS security risk management concept map. As with the previous assertions, the experts were asked discrete questions in the interviews relating to the security risk management concept map. The concept map’s structure, inherent complexity and concept understanding were considered.

\textbf{7.6.1 Map structure}

As demonstrated in the previous assertions, the concept map did appear, to a degree, to appropriately represent the category of security risk management. Nevertheless, all experts proposed some degree of change within the concept map’s structure. When Kerran was asked if the map described the overall structure of what he believed security risk management was, he stated that “it’s not dissimilar, but it depends on the type of [risk] assessment”. He went on to propose that “generally I feel the map applies to all security situations, although some concepts may move depending on the issues.”

Andrew supported this idea, when stating that “I could look at it one way and say this relates to that and that, and then look it a different way and say this relates to that”.

152
Nevertheless, Andrew indicated that the map did represent his thoughts on security risk management, however the map would still required “a little bit of tweaking”. This approach was generally taken by all the experts, as in their opinion the map was in general appropriate, with a small degree of erroneous structure.

7.6.2 Structural complexity
As Kerran proposed earlier, the concept map does apply to “all security situations”, however, application will be dependant on the security issue. This idea was supported by Frazer, who stated that “whilst I think it covers the main overlying principles ... there are areas where you might want to delve down even more.” Frazer also went further, by questioning the “extent of how deep you go … do you break up probability ... communications and culture”, concluding with criticism that the map is “a kind of jumble ... [without] logical flow”. Andrew stated that “each individual person is going to have their own description on how things link up” and questioned how much detail is useful, proposing he “could add more to this, but I don’t disagree with the majority of what’s on [the map]”. Andrew concluded with the statement that “I think this overall placement works, but each individual may argue.”

The majority of experts indicated that although risk was appropriately located at the top of the map, that they would consider threat first. As Andrew stated “in the first instance ... I think of threat first as being the cause of a risk.” This view was supported by Kate, who stated that the “nature of threat is that without it, the need for risk management does not exist”, however, she did comment that the map could be rotated 45° to place threat uppermost. In contrast, Kerran strongly supported the “fundamental” importance of threat, nevertheless he also claimed that “threats can be divided by 4 or 5 aspects or sub-categories”. Zack initially was “a little surprised that threat represents such a central theme”, however, then stated that “threat is a security concept … only really encountered … in dealing with models applied by security agencies”. He later concluded that threat “is a key concept” and “it’s not totally unsurprising to see it as a central concept”.

153
Greg made the point that the individual concepts were not necessarily a “once off activity”, moreover that there may be a measure of “incremental change”. He later reinforced this idea by stating that there “should be possibly more circular”, making reference to the “linear” nature of the concept map’s propositional linkages. Kate also took this approach, questioning whether one should consider risk management from a “top down perspective”.

7.6.3 Concept understanding

The experts had diffuse ideas of some concept meaning, in particular, calculate, assessment, analysis, evaluation and communication. The diffusion was not only focussed on the more implicit concepts, but also appeared with ideas that, according to the experts, were not necessarily explicit to security risk management. The study did not attempt to provide concept definition – allowing the experts to define their own understanding through relationship of concepts or knowledge structure. Greg demonstrated an example, when he stated that “analysis is probably something I would see being applied in between probability and consequence, rather than having analysis on the other side [of the map] ... therefore, is that defining analysis or is it part of the journey to get between probability and consequence?”

Kate raised the “human aspect” of security risk management and “where the map was coming from in terms of whether it [the human aspect] was important”. Frazer put forward the following argument:

If I went into a building I might look at things completely differently to the way you look at it. So it comes back to a lot of other things, like your background, knowledge of the area or knowledge of the operation of the building or operation of the facility. To someone with a background in defence, going onto a defence site may see completely different threats than someone without that background going on that site. And then you look at their experience and knowledge that they have in that area as well can affect that, so although that covers it all, there’s all those, I guess, I don’t know whether you would call them a motive or just knowledge and experience ... everyone may come up with different ideas.

Zack discussed the spatial spread of assessment, calculate and evaluation, in respect to probability and consequence. He “questioned the position” of these concepts, indicating
that they should be more closely associated with *probability* and *consequence*. Andrew opposed this view, by stating that “in my mind the analysis/evaluation go right with assessment ... they have a box around all three”. Nevertheless Andrew did summarise what most experts proposed, that “I could look at it one way and say that this relates to that ... then look at it a different way and say this relates to that”. For example, Frazer stated that “everyone may come up with different ideas” and that “it’s very subjective” when considering security risk management.

### 7.6.4 Assertion 3 conclusion

According to Assertion one, the experts considered that the MDS concept map represented a suitable foundation knowledge structure of security risk management. Assertion two was opposed, with the proposition that the sequential nature of the concept clusters did not generally represent expert decision-making. Assertion three considered that although the map represented the security risk management category, there was greater complexity than presented.

Assertion three was supported through evidence of the expert’s understanding of the concept map structure, the differing expert views and the individual understanding of concepts. As Andrew stated, “I don’t have a problem with the way it’s laid out because there’s different interpretations”. Assertion three indicated that the concept map has a degree of individual interpretation, leading to a level of greater complexity than the concept map could fully represent.

### 7.7 Assertion 4: The security risk management concept map propositions did not effectively represent concept linkage

Assertion four measured the degree of expert concurrence to the propositional linkages, being both the map’s concept links and informing labels. The primary study’s concept map propositional linkages appeared to have a higher degree of expert acceptance, when compared to the linkages presented in the pilot study (Chapter 4.4). However, in the primary study the propositional linkages were developed and refined through the Delphi or convergence method, where experts proposed linkages in isolation and these were
summed. These propositional linkages were then reviewed and amendments made by additional experts. This method went through a number of iterations before the map’s final propositional linkages were refined (see Chapter 6.4). The iteration approach appeared to significantly reduce the expert’s strong and generally adverse comments regarding the pilot study concept map’s propositional linkages.

7.7.1 Propositional concept links

When the experts were asked if they would like to amend or add any linkages, no common recommendations were made. There was no single link that the majority of experts wished to alter, however, most experts proposed additional links or modification to existing links (Figure 7.1). For example, Andrew did not agree with the links between loss and decision, and between communication and threat. Whereas Kate recommended a link between culture and communication, and culture and risk management. Kate elaborated on the additional cultural links, as she stated that there needs to be an appropriate “culture of risk management within the organisation”.

In Frazer’s opinion “there should have been a link from assessment to probability, consequence and analysis”, as without some degree of one you cannot have a risk. Andrew also recommended a link between both analysis and consequence, and analysis and probability, as opposed to a single link between analysis, consequence and probability. Nevertheless, Andrew did consider that in regard to risk, consequence and probability are mutually inclusive.

Greg asked whether the arrows indicated “a one way flow?” It was indicated that they do, to which Greg stated that he considered that risk management is an iterative process, where “components” may be revisited. Finally, when Kerran was asked if there should be additional or modified links he said “No, I tried but could not add any links. This is not a practical method of risk assessment, but I consider it a theoretical approach”. However, as Andrew concluded, “you can always add links ... in terms of the existing links ... I think they make good sense” and went on to “99% agree ... depending on interpretation”. Later Kerran stated that the “globally the relationships are good”, an
aspect supported by Zack who claimed that the “links are pretty accurate representation”.

![Diagram](image)

Figure 7.1 Individual experts additional recommended propositional linkages

Note 1: Concept map has been spatially adjusted to size

### 7.7.2 Propositional informing labels

Each expert was asked if he or she considers if any propositional informing label should be changed in any way? Unlike the concept map’s linkages, there was one common label that two or more experts questioned, namely the label *control* between the concepts
communication and threat. However, from the 17 total labels used within the map, the control label was the only label that two or more of the expert’s recommended changing. Both Greg and Andrew questioned the label control, indicating that this term was “quite strong” and that the label manage may be more appropriate. Greg also indicated that the label defines, between calculate and threat was “not quite right”, for which he could not provide an alternative.

Frazer questioned that “probability is measured with consequence”; however, he did “think there is a link between the two”. He concluded that probability and consequence should be a product and is mutually inclusive. However, Frazer also indicated that the other labels were “quite appropriate”. Andrew stated that “loss requires a decision, which doesn’t make immediate sense”, commenting that this label was not wholly appropriate. When Greg was asked whether the map represented his thoughts on security risk management, he stated:

> It appears to be labelling … quite well and there are certain areas there, for instance the culture, how that may affect perception, that’s very much true when you make that assessment of the environment you’re in. So if you don’t know the culture it’s pretty hard to understand necessarily why people react to certain things or not reacting, so it seems to fit well.

Kerran did propose additional linkages between risk management and calculate labelled quantitative, and risk management and assessment labelled qualitative. This idea was to a degree supported by Andrew, who stated “if you’re looking at probability in terms of quantitative analysis then that would involve calculation”. Andrew also proposed that “each individual person is going to have their own description on how things link up.” Nevertheless, in Kate’s opinion there were no changes which she needed to make and Zack supported this approach, when he stated “I think they’re all fair comments in terms of those concepts”.

### 7.7.3 Assertion 4 conclusion

The experts generally strongly supported the propositional linkages, at a far higher rate than found during the pilot study. This improved insertion of propositional linkages appeared to be due to the method of linkage development, which was different between
the pilot and primary studies. The pilot study had the researcher insert linkages, causing a high degree of adverse comments from the pilot study experts. In contrast the primary study used a Delphi method, where independent experts were presented with a blank MDS knowledge structure and asked to insert their own linkages. On completion, these individual maps were summed and again expert refined. This approach significantly improved the expert validation of these linkages, resulting in no single link being identified as inappropriate by more than one expert. Nevertheless, a majority of experts did recommend the insertion of additional linkages.

The propositional informing labels had a majority of expert support. Again, the main study’s expert support opposed the pilot study results, which produced significantly adverse comments from the pilot study experts. As with the propositional linkages, it appeared that the Delphi method reduced this previous high degree of adverse comment. However, each expert still had alternative proposals for some of the concept map’s labels, demonstrating that the map is open to a degree of individual interpretation. These individual recommendations were isolated; only one label having two experts put forward an alternative label. Nevertheless, diffuse interpretation of the concept map propositional linkages could reduce the validity of the psychometric MDS security risk management concept map.

7.8 Conclusion
Phase three of the research study, being the expert validation of the psychometric MDS security risk management concept map, is described in this chapter. Validation was achieved through Research Question three, which asked: What is the expert knowledge structure and subordinate concepts of security risk management as measured by interviews? To respond to the research question, four assertions were formed and expert opinion on these assertions considered as supporting evidence.

Assertion one indicated that security experts considered that the MDS security risk management concept map presented a suitable foundation knowledge structure. There was strong evidence from all experts to support this assertion, as according to the
experts, MDS developed and structured a valid psychometric concept map of security risk management. The evidence considered the experts’ opinion’s to reach this conclusion with the security risk management map’s general structure, spatial representation, concept clusters, fundamental and central theme of threat, and discrete concept localities. However, concurrent comments on the concept map’s structure indicated that there was a degree of expert interpretation. In addition, interpretation was supported by a high MDS STRESS1 measure and the implicit nature of the knowledge category. Both factors are likely to alter expert understanding and interpretation of the concept map.

Assertion two indicated that the map’s sequential nature of concept clusters represented expert decision-making, with bounded evidence presented in the experts’ opinion’s that assertion two could not be significantly validated. This evidence included the map’s relationship structure, spatial locality of a number of risk concepts, the sequential nature of concepts and spatial concept clusters. Some validity of structural relationships were raised, however, these were generally by individual experts in isolation. There was only moderate support for the sequential nature of concepts, a finding that opposed the pilot study. The importance of threat and its central locality was strongly supported by all six experts, resulting in a degree of conflict between the moderate support for the sequential nature of concepts and the strong support for the central locality of threat. In addition, there was strong expert agreement on a number of concept clusters. Some concept clusters did generate adverse discussion, however, these were generally proposed by single experts in isolation. Nevertheless, the concept map represented strong conceptual relationships.

Assertion three considered that although the concept map represented the category of security risk management, there was greater complexity than presented. Assertion three was supported through evidence of expert understanding of the concept map structure, the differing expert views and the individual understanding of concepts. Assertion three indicated that the map has a degree of individual interpretation, leading to a level of greater complexity than the map could fully represent.
Assertion four considered that the security risk management concept map did not effectively represent propositional linkages. In contrast, the experts strongly supported the propositional linkages at a far higher rate than found during the pilot study. The improved validity of links and labels appeared to be due to the use of the Delphi method, with independent expert development, summation and refinement of propositional linkages. This approach appeared to significantly improve the validity of the map’s propositional linkages, nevertheless, a majority of experts still recommended the insertion of additional individual links and labels.
CHAPTER 8
PHASE FOUR: EXPERT VALIDATION OF THE PSYCHOMETRIC MDS CONCEPT MAP

8.1 Introduction
Phase four of the study, describing the comparative inquiry between the development of the psychometric MDS security risk management concept map (Chapter 6) and expert validation (Chapter 7) is presented in this chapter. This comparison allowed a response to Research Questions four and five. Research Question four asked: Can a psychometric multidimensional scaling (MDS) concept map of the security risk management knowledge category and subordinate concepts be developed and represented? Research Question five asked: Is MDS an appropriate psychometric technique to develop and represent concept maps? As with the proceeding chapter, assertions were formed to respond to these research questions.

To achieve these outcomes, the chapter is divided into a number of discrete sections. The first section (8.2) presents assertion one, which considers the validity of the psychometric security risk management concept map and responds to Research Question four. Assertion two considers the use of MDS to develop and structure consensual concept maps (8.3). MDS analysis technique is considered in its ability to develop and present psychometric concept maps, responding to Research Question five. The reliability and validity of the study (8.4), and the final psychometric MDS security risk management concept map are presented (8.5). The chapter is summarised with a conclusion (8.6).

8.2 Assertion 1: The psychometric concept map presented a valid knowledge structure of the category security risk management
Assertion one considered the expert opinion on whether the psychometric MDS concept map represented a suitable knowledge structure for security risk management and responded to Research Question four: Can a psychometric MDS concept map of the security risk management knowledge category and subordinate concepts be developed
and represented? In consideration of study Phase three results (Chapter 7), assertion one was validated to an appropriate degree. This supporting evidence considered the strong expert opinion in response to the security risk management concept map structure, the category complexity and propositional linkages (Table 8.1).

Table 8.1
Phase four: Expert evidence in support of assertion one

<table>
<thead>
<tr>
<th>Supporting expert evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Concept structure – see section 8.2.1</strong></td>
</tr>
<tr>
<td>Strong expert agreement for the concept map structure</td>
</tr>
<tr>
<td>Expert support for the majority of concept clusters</td>
</tr>
<tr>
<td>Concept map did not inclusively present all security risk management concepts</td>
</tr>
<tr>
<td>Expert agreement that the concept map represented the experts’ view of security risk management</td>
</tr>
<tr>
<td><strong>Category complexity – see section 8.2.2</strong></td>
</tr>
<tr>
<td>Strong expert support for the concept map’s spatial relationships</td>
</tr>
<tr>
<td>Moderate expert support for the sequential structure of concepts</td>
</tr>
<tr>
<td>Each expert recommended some degree of structural modification, however,</td>
</tr>
<tr>
<td>with no expert consensus</td>
</tr>
<tr>
<td>MDS STRESS1 measured high – indicating the implicit nature of the security risk management knowledge category</td>
</tr>
<tr>
<td>The concept map did not represent expert decision-making</td>
</tr>
<tr>
<td><strong>Propositional linkages – see section 8.2.3</strong></td>
</tr>
<tr>
<td>Strong expert agreement for the majority of propositional linkages</td>
</tr>
<tr>
<td>Each expert proposed additional propositional linkages</td>
</tr>
<tr>
<td>Each expert provided some degree of individual concept map interpretation</td>
</tr>
</tbody>
</table>

8.2.1 Concept map structure

The psychometric MDS security risk management concept map represented a suitable foundation knowledge structure. Strong expert opinion supported this result, with evidence considering the expert’s opinion on the map’s general structure, spatial representation, central theme of threat, and discrete inclusive concept localities.

The six experts supported the psychometric security risk management concept map representation, with individual expert agreement that the concept map in general described their ideas underlying security risk management. Threat proved to be both fundamental and pivotal within the map, with MDS locating threat within a spatially central location. This position placed all other concepts surrounding threat, with the
experts strongly supporting the fundamental nature and central location of threat. The map’s concept clusters were considered by the individual experts, with the least appropriate cluster (calculate/assessment) still generally supported by three of the six experts. Nevertheless, it was found that in general the concept clusters were well supported by the experts, in particular, the clusters of probability, consequence and analysis, risk and risk management, and threat, perception and culture.

When considering the security risk management concepts (Table 5.7), two or more experts proposed two additional concepts – treatment and vulnerability. Expert opinion indicated that both discrete concepts appeared to be relatively important ideas within the knowledge category of security risk management and should have been included within the concept map. However, during study Phase one (Chapter 5) these concepts were not identified as significant, resulting in the exclusion of these concepts from the security risk management knowledge category and concept map.

8.2.2 Category complexity

According to the experts there was bounded evidence presented to consider that the concept map represented expert decision-making. In addition, there was indication that the knowledge category was complex in structure. Evidence included the map’s structural relationships of concepts, the spatial location of a number of concepts, the sequential nature of concepts and spatial concept clusters.

The six experts supported the general spatial relationship structure of the concept map. However, a degree of validity of some structural relationships were raised, nevertheless, these relationships were generally by individual experts in isolation. There were various opinions put forward by the experts regarding the sequential nature of some concepts, in particular, risk, risk management, calculate and/or assessment, threat and loss to decision. Half of the experts indicating that threat is considered first, with the other half indicating that risk commences the sequence. As discussed later, the latter position was opposed by the experts though the central spatial locality of threat. These relationships
resulted in only a moderate support for the sequential structure of concepts, indicating that the map could only demonstrate bounded concept sequence.

There was strong agreement from the experts regarding a number of concept clusters — probability, consequence and analysis, and threat, perception and culture. All six experts agreed that these concept clusters were justified, nevertheless, other concept clusters did generate adverse discussion. These adverse comments regarded the concepts of calculate, assessment and evaluation, however, these comments were generally proposed by individual experts with no consensus between experts. The importance and central locality within the map of the concept threat was strongly supported by the experts, opposing the moderate support for the sequential nature of concept location.

All experts proposed some degree of structural change to the concept map that no other expert considered, even through the experts strongly supported the map’s structure and supporting concept relationships. However, according to the experts the map represented strong concept relationships. This relationship issue indicated a degree of individual expert interpretation, reducing the map’s validity. As discussed in the following paragraph, this outcome implied that either the MDS STRESS1 was an appropriately high measure (STRESS1=0.28) or the implicit nature of the knowledge category increased interpretation.

As previously indicated, the MDS STRESS1 did indicate an inappropriate high measure. This measure indicated that according to Phase two, the expert MDS measure did not locate all concepts in their most ideal spatial locality. In addition, the implicit nature of the category may have resulted in greater individual interpretation, in both concept understanding and structural integrity. As Andrew stated, “I don’t have a problem with the way it’s laid out because there’s different interpretations”. These factors implied that the concept map has a degree of individual interpretation, leading to a level of greater complexity than the map could fully represent. Both factors are likely to decrease expert understanding of the concept map and therefore lead to differing expert interpretation. Nevertheless, the MDS STRESS1 measure was not as high as other concept mapping
8.2.3 Propositional linkages
The experts strongly supported the majority of the concept map’s propositional linkages, demonstrated by no single link being identified as inappropriate by more than one expert. Nevertheless, the majority of experts still put forward the insertion of additional links and had alternatives for some of the map’s labels. However, these individual proposals were isolated with only one propositional linkage having two experts put forward an alternative and common label. This result would appear to further demonstrate the degree of individual map interpretation – reducing the face validity of the psychometric security risk management concept map.

8.2.4 Assertion one conclusion
Assertion one considered the expert opinion on whether the concept map represented a suitable consensual knowledge structure for security risk management. This assertion responded to Research Question four: Can a psychometric MDS concept map of the security risk management knowledge category and subordinate concepts be developed and represented? Based on the evidence presented, it can be demonstrated that assertion one was supported. The security experts considered that the concept map for the category of security risk management presented a valid foundation knowledge structure. Therefore, the psychometric MDS security risk management concept map (Figure 6.4) provided an appropriate representation of this knowledge category.

8.3 Assertion 2: MDS can be used to develop and structure concept maps
Within the context of the study, assertion two considered whether MDS developed and structured a valid psychometric concept map and responded to Research Question five: Is MDS an appropriate psychometric technique to develop and represent concept maps? In addition, the methodology to develop and structure psychometric MDS concept maps was considered. The evidence to support assertion two was based on the security risk
management concept map developed during the study and other similar reported psychometric concept mapping studies. In support of the evidence, knowledge structure, concept clustering, conceptual relationships and the MDS mapping methodology are discussed (Table 8.2).

Table 8.2

Phase four: Evidence in support of assertion two

<table>
<thead>
<tr>
<th>Supporting study evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge structure – see section 8.3.1</td>
</tr>
<tr>
<td>Strong expert agreement for the concept map knowledge structure, concept complexity and propositional linkages</td>
</tr>
<tr>
<td>Other studies reported similar outcomes to support MDS concept mapping structure</td>
</tr>
<tr>
<td>Concept clusters – see section 8.3.2</td>
</tr>
<tr>
<td>Closer the spatial proximity of concepts – stronger the conceptual relationship</td>
</tr>
<tr>
<td>Strong expert agreement for the spatial locality of concepts within the map</td>
</tr>
<tr>
<td>Repeated MDS concept maps between pilot study and primary study</td>
</tr>
<tr>
<td>Conceptual relationships – see section 8.3.3</td>
</tr>
<tr>
<td>Appropriate presented spatial locality of concepts i.e., threat, risk, risk management</td>
</tr>
<tr>
<td>Strong expert agreement for the majority of conceptual relationships</td>
</tr>
<tr>
<td>Inclusiveness and expert ratification of the concepts within the knowledge category</td>
</tr>
<tr>
<td>MDS mapping methodology – see section 8.3.4</td>
</tr>
<tr>
<td>Strong expert agreement on the concept map</td>
</tr>
<tr>
<td>Restricted reporting in similar concept mapping studies in the development and presentation of propositional linkages</td>
</tr>
<tr>
<td>Effectiveness of the Delphi method to develop and present propositional linkages</td>
</tr>
<tr>
<td>Ability of MDS in the spatial presentation of knowledge structure</td>
</tr>
<tr>
<td>Comparable concept mapping studies reported similar outcomes – excluding propositional linkages</td>
</tr>
</tbody>
</table>

**8.3.1 MDS presented suitable knowledge structure**

Within the context of the study, it appeared that the MDS measure and spatial presentation of the security risk management category presented a valid knowledge construct. A view supported by evidence demonstrated in prior sections (see Table 8.1), in particular, the strong expert support for the security risk management concept map in knowledge structure, category complexity and propositional linkages. In addition, other authors have reported comparable evidence – that MDS develops and structures valid concept maps (Kealy, 2001; Martinez-Torres, et al., 2005; Streveler, et al., 2001; Trochim, 2005b; Turns, et al., 2000).
Lukuge, Gilbert and Richards used MDS to “structure and ... build user-centered [sic] information structures” (1996, p. 1) – considering the domain of tourist attractions and the need to present customised tourist information mapping interfaces. Their research resulted in the conclusion that MDS provided a robust technique and “an excellent basis for measuring … information structures” (Lokuge, et al., 1996, p. 6). In addition, Martinez-Torres, et al. (2005) used MDS concept mapping to define teaching methodologies in digital signal process techniques. The study used teachers to develop concept maps of their knowledge using 82 concepts, resulting in the understanding of the “relative importance of the concepts to be covered [and] used to program the course” (Martinez-Torres, et al., 2005, p. 422).

Lay persons or novice-learners are more likely to have far less complex conceptual maps than experts, demonstrated by a previous study where non-major students produced “less extensive and complex [concept maps] than those advanced biology students” (Markham, et al., 1994, p. 94). Conceptual complexity included the number of concepts used, frequency and creation of propositional linkages, and the cross-links between concepts, indicating that a domain expert would produce a more complex concept map when compared to a domain practitioner. This view may be supported by a study that used a longitudinal measure of novice-learner concept maps compared to domain expert concept maps, concluding that the complexity and internal consistency of novice-learner maps correlated to the level of the novice-learner’s achievement (Aidman & Egan, 1998).

8.3.2 Closer concepts indicated stronger knowledge relationships
One significant problem with concepts maps is their individualist nature (Bennett & Rolheiser, 2001), which is enhanced when combined with an individual’s knowledge complexity. These individual concept maps may have diffuse structure and variance in propositional linkages, with little consensus between concepts. Therefore, the use of MDS to measure and represent consensual understanding within a concept map could be considered beneficial as concept maps can display distinguished structural complexity (Markham, et al., 1994). Also, using MDS to measure concept map similarities has
provided a means of inverse concept testing or knowledge assessment (Aidman & Egan, 1998).

As measured in the security risk management concept map, there were concepts that demonstrated close spatial proximity. These concepts included the concepts of risk management and risk, probability and consequence, and probability and communications. Likewise, there were concepts that demonstrated spatial separation, including concepts like risk and decision-making. These spatial measures were repeated between the pilot study (Chapter 4) and primary study (Chapter 6), using different cohorts of experts. In addition, during the interviews the experts generally strongly supported the spatial locality of most concepts within the security risk management concept map. Within the context of the study, these expert opinions provided a degree of validity in claiming that MDS did represent appropriate knowledge clustering of similar concepts. Conversely, dissimilar ideas were spatially separated.

Appropriate MDS knowledge clustering can be supported by Lokuge et al. (1996), who found that similar sites were spatially located nearer each other when measured by MDS. However, their MDS concept map was distorted when compared to the physical geographical map – with distortion considered to be due to the participants differing familiarity to the sites or from considering distance as travel time, opposed to geographical distance (Lokuge, et al., 1996). MDS has been shown to spatially locate similar objects closer to each other (Cox & Cox, 2000; Kruskal & Wish, 1978), nevertheless, only recent research has applied MDS to implicit knowledge concepts (Cheng, 2004; Trochim, 2005b; Turner, 2002). As Bennet and Rolheiser concluded “from our experience and observations, we hypothesise that concept mapping more precisely pushes concept formation and concept attainment” (2001, p. 277).

8.3.3 MDS presented conceptual relationships

The assumption proposed that MDS presented conceptual knowledge relationships through spatial concept proximity – based on supporting evidence comprising both data from the security risk management concept map and other comparable reported studies.
Evidence found that the security risk management concept map was valid, that other authors had reported similar outcomes within their own knowledge domains, that MDS represented implicit knowledge structure and that MDS may be used to validate concept occupation within knowledge categories. However, the study found that MDS knowledge representation did not indicate expert decision-making.

In considering the evidence presented in the prior sections, it would appear that within the context of the study MDS demonstrated underlying conceptual relationships. Supporting evidence, validated during the interviews with the security experts, included the central theme of threat, the structure of concepts, the clustering of similar concepts and the spatial separation of dissimilar concepts. There were limited adverse comments from the experts regarding the majority of the concept map’s structure and spatial conceptual relationships. It should be noted that different cohorts of security experts completed the MDS concept mapping survey (Chapter 6) and provided expert opinion on the psychometric security risk management concept map (Chapter 7).

There is little doubt that MDS represented similar rated objects spatially closer when compared to more dissimilar objects. However, knowledge concepts may be both implicit and complex, which could result in unreliable and invalid MDS presentations due to differing individual knowledge structures. As Trochim stated “concept mapping may result in both a representation of reality and an interesting suggestive device” (1989a, p. 1). Nevertheless in considering the result from the security risk management concept map, it would appear that complex and implicit concept relationships can be effectively represented. A claim reported by Aidman and Egan (1998) who found appropriate MDS mapping structure, correlation in internal consistency and complexity, and similarity to independent novice-learner and expert established concept maps.

In addition, MDS concept mapping has the ability to ratify whether discrete concepts do belong to a certain knowledge category. It was considered likely that concepts that may be perceived to be exclusive to the majority of measured concepts would cause that particular concept to be represented as an outlier within the MDS concept map. As the
study has demonstrated, similar concepts do cluster. Knowledge ratification is further supported by the work of Aidman and Egan, who stated that “the efficiency of mapping task dramatically improves when its concept set is hierarchically levelled. That is, all the concepts that are being mapped belong to the same generic category” (1998, p. 291). Knowledge category ratification had also been raised by Martinez-Torres et al. (2005) who found that MDS provided information relating to the relative importance of domain concepts, indicating that the use of MDS would be an effective methodology to develop or support domain knowledge categories.

The use of MDS to develop knowledge categories could be an appropriate methodology. This study used Linguistic Inquiry and Word Cont (LIWC) (Pennebaker, et al., 2001) and expert opinion to extract and develop knowledge categories. Located within the knowledge category were supporting subordinate concepts. It had been found that through an iterative process and validated expert opinion, the final knowledge category list proved to have appropriate concepts (Chapter 5.7 and Chapter 5.8). However, it was claimed that there were two security risk management concepts missing from the security risk management category (see Chapter 8.5). Nevertheless there were generally no concepts presented as outliers in the MDS security risk management presentation (Figure 6.5), however, it could be implied that to a degree the concepts of decision and loss may have been. There were bounded expert opinions regarding the locality of these two concepts, which do provide a degree of support for their exclusion in the security risk management knowledge category.

The use of MDS to represent concept relationships has been demonstrated. However, can additional knowledge be extracted from the MDS concept maps? During the study, the sequential structures of concepts were considered and whether these structures showed any cognitive expert decision-making. The pilot study appeared to indicate a degree of decision-making (see Chapter 4.4.2). In contrast, the primary study did not support expert decision-making (Chapter 7.5). Therefore, MDS concept mapping did not demonstrate expert decision-making.
Within the context of the study, the proposed assumption was that MDS provided concept relationships based on spatial proximity. This assumption can be supported within both the context of the study and from other reported studies (Aidman & Egan, 1998; Martinez-Torres, et al., 2005). As Markham et al. put forward “concept mapping provides a theoretically powerful and psychometrically sound tool for assessing conceptual change” (1994, p. 91).

8.3.4 MDS mapping methodology

The methodology of using MDS to develop, structure and present consensual psychometric concept maps was examined. There appeared to be affirmative evidence to claim that MDS concept mapping was effective – evidence included both the security risk management concept map and comparable supporting concept mapping studies. The security risk management concept map, the use of the Delphi method to define propositional linkages, the ability of MDS to represent concept clusters to define knowledge categories and in addition, other reported studies are further considered.

As previously discussed, the evidence presented in prior sections demonstrated that within the context of the study MDS proved an appropriate technique in developing, structuring and presenting psychometric concept maps. During the expert interviews, the security experts did not present any significantly adverse comments regarding the security risk management map, both in the pilot study and primary study. Both the pilot study and primary study produced relatively similar knowledge structures for the common concepts. Each study used different expert cohorts, both to develop and validate the concept maps. Evidence is further supported by Markham, et al., who stated that “these results offer further evidence … of [MDS] concept mapping as a research and evaluation tool in science education” (1994, p. 100).

MDS did appear to provide appropriate knowledge structure. However, knowledge structure did not result in a complete psychometric concept map. Additional input had to be made with the insertion of propositional linkages, resulting in a degree of expert interpretation and compromising the concept map’s validity. The study used a number of
methods to develop propositional linkages, with apparent improvement between methods. A significant improvement appeared to be the use of the Delphi method in propositional linkage insertion, where experts independently developed the linkages and supporting labels. In the primary study the experts strongly supported the propositional linkages (Chapter 7.7), opposing the result found during the pilot study (Chapter 4.4.4). The Delphi method appeared to significantly improve the validity of the concept map’s propositional linkages.

It was proposed that the use of MDS would be an effective methodology to develop domain knowledge categories. As Kealy stated when using MDS, “analysis revealed common student perceptions about dimensions that characterized [sic] the conceptual relationships involved” (2001, p. 325). If a list of concepts are measured by MDS similarity concept clusters would form, whereas dissimilar clusters would be spatially separated. Given a relatively diverse number of concepts, these concept clusters would form knowledge categories. As Markham, et al. claimed, more advanced learners “displayed an array of domain-specific, implicit, superordinate concepts that organised much of their knowledge structure” (1994, p. 97).

A manual approach to develop knowledge categories was recommended by Trochim (2005b), using paper sorting cards. Each sorting cards would list a different concept, sorted and stacked by each participant according to their perceived conceptual similarity. The cards stacked onto a single pile would indicate concept similarities from which an MDS concept map may be developed. It could be implied that each card stack is a form of knowledge category, so why not let the participant rate the initial concept list and have MDS form knowledge category clusters? However, a limitation with this psychometric MDS approach would be the excessive number and diversity of concepts (see Chapter 3.5.1).

Trochim (1989b) has for over a decade studied the use of MDS to develop and construct concept maps, with more recent studies also using MDS to develop and present concept map structures (Kealy, 2001; Martinez-Torres, et al., 2005; Trochim, 2005b; Turns, et
These studies have generally supported Trochim’s findings, building a consensus in MDS concept mapping methodology. A recent example was the use of MDS concept mapping to develop a teaching methodology in a basic digital signal processing course (Martinez-Torres, et al., 2005). Evidence has generally concluded that MDS is a suitable methodology for the development and construction of concept maps. As Turner (2002) stated, MDS analysis revealed clear structure in technique, clear typology and served to confirm the findings of past studies. Nevertheless, further research into psychometric MDS concept mapping is still required.

8.3.5 Assertion two conclusion
Assertion two considered whether, within the context of the study, MDS developed and structured a valid psychometric MDS concept map. In addition, the methodology to develop and structure MDS concept maps was considered. The evidence to support assertion two was based on the security risk management concept map developed during this study and other comparable reported concept mapping studies. As supporting evidence, knowledge structure, concept clustering, conceptual relationships and the MDS mapping methodology was presented. In considering the evidence, assertion two was confirmed – MDS did develop and represent a valid psychometric security risk management concept map and the MDS concept mapping methodology appeared appropriate, limited only by the ability to insert valid propositional linkages.

In response to Research Question five: Is multidimensional scaling an appropriate psychometric technique to develop and represent concept maps?, it appeared that the evidence presented indicated that MDS concept mapping is an appropriate methodology to develop and present psychometric concept maps, a conclusion supported by the works of previous researchers within this area of study (Kealy, 2001; Martinez-Torres, et al., 2005; Trochim, 2005b; Turns, et al., 2000).

8.4 Reliability and validity
Within the context of the study, measures of both reliability and validity of MDS to develop and structure psychometric concept maps were considered. Reliability was
considered the ability of a test to be “relatively free from measurement error” (Fink, 2005, p. 108) and produce repeatable measures over a period of time (Clark-Carter, 1997). Validity was considered to be “the degree to which a measure assesses what it purports to measure” (Fink, 2005, p. 111). Each phase of the study considered various reliability and validity measures, with each method used dependent on the phase methodology. Trochim stated that because “concept mapping is so complex, it is difficult to conceive of a single overall reliability coefficient” (1993, p. 5). Therefore, the study considered a number of reliability and validity measures. This targeted approach restricted unknown errors at each phase affecting proceeding phases, ultimately improving the overall study reliability and validity.

8.4.1 Reliability

Previous studies have reported that MDS concept mapping can be reliable (Markham, et al., 1994), based on defined reliability indicators. These indicators, initially tested by Trochim (1993), include individual-to-individual sort reliability, individual-to-total matrix reliability, individual-to-map reliability, average intersort reliability and split-half reliabilities (Martinez-Torres, et al., 2005). In addition, a study (Herl, Baker & Niemi, 1996) compared expert developed concept maps with novice-learner maps, proving a reliable method of assessment. Other studies claimed that concept maps, using MDS as a measure of comparison, provided “valid representations of conceptual knowledge” (Kealy, 2001, p. 325). The study considered reliability through MDS goodness-of-fit (STRESS1) measure and Cronbach’s Alpha reliability of the source data, with the additional consideration of interrater reliability and spatial repeatability.

The MDS ALSCAL STRESS1 index represents the square root of the normalised residual variance of the monotonic regression for the original similarity distance data, with lower values of goodness-of-fit indicating a better fit (Sireci & Hambleton, 2003). The study’s STRESS1 measure was relatively high (STRESS1=0.28, RSQ=0.64), indicating that not all concepts were located in the most appropriate spatial locality. However, expert opinion appeared to negate the value of this measure, as generally the security risk management concept map garnered a strong positive response from the
interviewed security experts. Trochim (1993) recognised this variance when he tested the reliability of 38 different concept maps. Results showed higher stress measures then is typically found with more stable phenomena, with the 38 concept maps producing a high (STRESS1=0.29, SD=0.4) measure (Trochim, 1993). Trochim’s result would indicate that this study’s MDS STRESS1 (STRESS1=0.28) measure was appropriate. In addition, MDS STRESS1 may not be the most indicative measure of reliability when presenting implicit concept maps.

Reliability was tested using Cronbach’s Alpha, a method proposed as “superior to the simple split half estimator, but there is no known way to estimate alpha for the matrix data used in concept mapping” (Trochim, 1993, p. 7). However, original similarity data gathered from the expert participants before conversion to half-matrix appeared to be suitable for Alpha testing (see Chapter 9.3.2.4) – resulting in an appropriate high (α=0.93) measure. Interrater reliability proven to be appropriate, demonstrated by the strong support from the experts when providing opinion on the security risk management concept map. Finally, both the pilot study and primary study concept maps produced most similar spatial structures, repeated by different cohorts of security experts.

8.4.2 Validity

Validity was assessed through face validity, concurrent validity and triangulation. There appeared to be limited related studies in the validity of MDS concept mapping, with only two articles found in this research area (Aidman & Egan, 1998; Kealy, 2001). Face validity was considered suitable, supported by the interview evidence of the strong expert support for the security risk management concept map. Nevertheless, the propositional linkages appeared to reduce the validity of the security risk management concept map to a degree, through variance of expert interpretation. Available literature did not appear to discuss the validity aspect of MDS concept map propositional linkages, arguable significant considering that the propositional linkages provide third party understanding.
Concurrent validity of Phase two expert MDS survey was tested using Pearson two tailed correlation at ≥95% confidence level between expert’s similarity responses, producing a moderate total result (r=0.32, SD0.19). This moderate result could have been higher, as previous research has shown “evidence of concurrent validity” (Aidman & Egan, 1998, p. 12) where novice to expert domain maps were measured as a means of assessment.

Validity was also illustrated by triangulation, put forward by Campbell and Fiske as a “powerful way of demonstrating concurrent validity” (cited by Cohen, et al., 2002, p. 112). Triangulation results between the pilot study (Chapter 4), Phase one Knowledge Categorisation (Chapter 5), Phase two MDS concept map development (Chapter 6) and Phase three expert interviews (Chapter 7) were considered. Each phase of the study used expert opinion, ensuring a degree of longitudinal validity in data. The pilot study and primary study concept maps both reflected a high degree of spatial similarity in content and structure. In content, the knowledge category extraction of security risk management concepts resulted in a moderate concept match (67%) between each study. In structure, concepts common between maps were located in similar spatial positions – demonstrated by concepts such as threat, risk, risk management, decision, probability and consequence.

8.4.3 Reliability and validity conclusion
In considering the various methods to test both reliability and validity throughout the study, it is claimed that the study produced an appropriate result in both measures. Results improved between the pilot study and primary study, demonstrating that the altered methodology to develop and construct MDS concept maps used in the primary study was more appropriate. MDS STRESS1 was not the most suitable method to demonstrate reliability, when considered against more stable phenomena. Cronbach’s Alpha reliability measure proved to be appropriate, however, further testing will have to be completed to consider the relationship between the original similarity data and final MDS spatial representation. The security risk management concept map’s validity was appropriate, tested with face validity, concurrent validity and triangulation.
Finally, MDS concept mapping required a more unusual approach than is generally proposed in reliability and validity literature, perhaps further considering greater triangulation of results. The need for diversity of both reliability and validity measures was supported, when “the traditional theory of reliability typically applied in social research does not fit the concept mapping model well” (Trochim, 1993, p. 2). Nevertheless, both reliability and validity appeared to be measurable and when considered within the context of the study, were appropriate.

8.5 Security risk management concept map
Through the exhibited evidence, the study has developed and presented an appropriate psychometric MDS concept map of security risk management. With an iteration process, the concept map had been constructed using concept extraction and knowledge categorisation, MDS concept mapping, expert validation and a final comparative assessment. Each phase applied some level of expert support (Chapter 6) and validation (Chapter 7), ensuring that to an appropriate degree proceeding phases were both reliable and valid. At each phase of the study, security experts did not present any adverse consensually comments against that particular assessed phase. Nevertheless, according to the experts, the concepts vulnerability and treatment should have been included within the security risk management concept map. The presentation of the psychometric concept map confirmed Research Question four, being the presentation of a psychometric MDS security risk management concept map (Figure 6.5).

8.6 Conclusion
This chapter presented Phase four of the research study, being a comparative assessment between study Phase two and Phase three. Phase two constructed the psychometric MDS security risk management concept map and Phase three considered expert validation of this concept map. To achieve these outcomes, research questions were formed. Research Question four asked: Can a psychometric MDS concept map of security risk management knowledge category and subordinate concepts be developed and represented? Research Question five asked: Is MDS an appropriate psychometric
technique to develop and represent concept maps? As with the proceeding chapter, assertions were formed to confirm or deny these research questions.

Assertion one considered if the concept map represented a valid knowledge structure of security risk management and responded to Research Question four. Based on the evidence presented, assertion one was supported. Evidence considered the interviewed security experts strong support for the security risk management concept map and that according to these experts, the concept map presented a valid foundation knowledge structure. Supporting the overall map structure was the knowledge category inclusion of appropriate subordinate concepts, the map’s conceptual complexity and supporting propositional linkages. The only significant limitations of the presented concept map were the exclusion of the concepts vulnerability and treatment, and the degree of individual interpretation of the propositional linkages. Nevertheless, the psychometric security risk management concept map (Figure 6.5) provided an appropriate representation to confirm Research Question four.

Assertion two considered if MDS concept mapping developed and structured an appropriate psychometric concept map and responded to Research Question five. Assertion two was supported, considering the evidence of the security risk management concept map and similar reported studies. Evidence to support knowledge structure, concept clustering, conceptual relationships and the MDS mapping methodology were demonstrated. The MDS concept mapping technique did develop and represent a valid concept map, limited only by the insertion of propositional linkages. This outcome provided an affirmative response to Research Question five, that from the evidence presented MDS concept mapping is an appropriate quantitative methodology to develop and present psychometric concept maps – a conclusion supported by the reported work of previous studies (Kealy, 2001; Martinez-Torres, et al., 2005; Trochim, 2005b; Turns, et al., 2000).

The study presented appropriate measures of both reliability and validity throughout the study, with results supported by similar reported studies. However, MDS STRESS1
measure was not the most appropriate reliability indicator, producing higher than normal results even through higher stress measures were reflected in a similar MDS concept mapping study (Trochim, 1993). Cronbach’s Alpha reliability was appropriately high ($\alpha=0.93$) and spatial structure between both pilot and primary studies proved comparable. Concurrent validity proved moderate ($r=0.32$, SD0.19), with expert opinion supporting face validity and in addition, spatial structure between both pilot and primary studies proving appropriate. Nevertheless, MDS concept mapping required a more unusual approach to the measures of both reliability and validity then would generally be reported in the literature. Due to the implicit nature of the data, the reliance on one measure would not necessarily be the most appropriate. Therefore, triangulation of results that used a number of methods proved to be more suitable.
CHAPTER 9
CONCLUSIONS, RECOMMENDATIONS AND LIMITATIONS

9.1 Introduction
This chapter presents the conclusions, recommendations and limitations of the study. A summary and conclusions of the study (9.2) are discussed in terms of the research questions and final study outcomes. Recommendations (9.3) consider how the psychometric multidimensional scaling (MDS) security risk management concept map could increase security risk understanding and also present potential avenues for further study. Limitations (9.4) of the study are presented and the chapter is summarised with a conclusion (9.5).

9.2 Summary of the study and conclusions
The five research questions resulted in a four phase study (Figure 1.1), which guided the inquiry in the quantitative development and presentation of the security risk management concept map. The phases of study and research questions were:

Phase one: Knowledge Categorisation (Chapter 5)
   Research Question 1: What are the knowledge categories and subordinate concepts of security?

Phase two: MDS Knowledge Structure Mapping (Chapter 6)
   Research Question 2: What is the expert knowledge structure and subordinate concepts of security risk management as measured by multidimensional scaling?

Phase three: Expert Knowledge Structure Validation (Chapter 7)
   Research Question 3: What is the expert knowledge structure and subordinate concepts of security risk management as measured by interviews?
Phase four: Expert Validation of the Psychometric MDS Concept Map (Chapter 8)

Research Question 4: Can a psychometric MDS concept map of the security risk management knowledge category and subordinate concepts be developed and represented?

Research Question 5: Is MDS technique an appropriate psychometric technique to develop and represent concept maps?

9.2.1 Phase one: Knowledge categorisation

Research Question one, incorporated within study Phase one, established the knowledge categories and subordinate concepts of security. As described in Chapter 5, 104 international tertiary level security courses were sourced and reviewed, with seven courses selected for content analysis. Course transcripts were sanitised and concepts extracted to provide the source document, being a list of 2001 security concepts (Appendix D). From the source document and using Linguistic Inquiry and Word Count (LIWC) (Pennebaker, et al., 2001), initial analysis extracted the draft security risk management concept list of 55 concepts. Using convergence between the Risk Management AS/NZS4360:2004 Standard, pilot study (Chapter 4) and expert validation, a final security risk management knowledge category was presented (Table 5.7).

According to analysis of the selected security courses, there were 14 security knowledge categories, comprising criminology, emergency/contingency planning, facility management, fire science, industrial security, information and computer security, investigations, physical security, security principles, security risk management, safety, security law, security management and security technology. These categories matched (76.5%) the ASIS common knowledge categories (American Society for Industrial Security, 2000).

9.2.2 Phase two: MDS knowledge structure mapping

Incorporated within study Phase two, Research Question two extracted the expert knowledge structure and subordinate concepts of security risk management, as measured by multidimensional scaling. As described in Chapter 6, the security risk management
knowledge category subordinate concepts were embedded into the MDS concept mapping survey and completed by the 29 security experts. The data were analysed and resulted in the presentation of the MDS knowledge structure of security risk management.

From the MDS knowledge structure, the psychometric MDS security risk management concept map was developed, with five security experts to insert propositional linkages and supporting labels using the Delphi method. The primary study’s concept map (Figure 6.5) and pilot study’s concept map (Figure 4.3) were compared for concept structure, resulting in significant structural commonality between maps. The structural similarity appeared to support the robustness of the psychometric security risk management concept map’s structure and propositional linkages.

9.2.3 Phase three: Expert knowledge structure validation

Incorporated within Phase three, Research Question three assessed the expert knowledge structure and subordinate concepts of security risk management, as measured by interviews. As described in Chapter 7, four assertions were formed and expert opinion on these assertions considered as supporting evidence. Assertion one claimed that there was appropriate evidence that the interviewed security experts considered that the psychometric MDS concept map presented a suitable foundation knowledge structure of security risk management. Evidence considered was based on the expert validation of the psychometric security risk management concept map’s general structure, spatial representation, concept clusters, fundamental and central theme of threat, and discrete concept locality. However, there was bounded evidence to claim that due to the implicit nature of the knowledge category there was a degree of individual expert interpretation.

In Phase three, assertion two claimed that the map’s sequential nature of concept clusters represented expert decision-making. However, there was bounded evidence presented by the interviewed security experts that assertion two could not be significantly validated. Evidence included the map’s relationship structure, spatial location of a number of risk concepts, the sequential nature of concepts and spatial concept clusters. Assertion three
considered that although the map represented the category of security risk management, there was greater complexity than presented. Assertion three was supported through evidence of expert understanding of the concept map structure, the differing expert ideas and the individual understanding of concepts.

Finally in Phase three, assertion four considered that the security risk management concept map did not effectively represent valid or reliable propositional linkages between the map’s concepts. Nevertheless, the experts strongly supported the propositional linkages, at a far higher rate than found during the pilot study. The Delphi method appeared to significantly improve the validity of the map’s propositional linkages, although a majority of experts still proposed the insertion of additional individual linkages. Again, Research Question three sourced the expert knowledge structure of security risk management. According to the interviewed security experts, the map developed and tested in this study presented an appropriately valid psychometric concept map of security risk management.

9.2.4 Phase four: Expert validation of the psychometric MDS concept map
Research Questions four and five were incorporated within Phase four of the study, being a comparative analysis between Phase two and Phase three. Research Question four was addressed through the development and representation of the psychometric security risk management concept map. Research Question five considered whether the psychometric MDS technique was an appropriate quantitative methodology to develop and represent concept maps. As described in Chapter 8, assertions were formed to confirm or deny these two research questions.

In Phase four, assertion one considered that the psychometric concept map represented a valid knowledge structure of security risk management. Based on the presented evidence – the interviewed security experts strong support for the security risk management concept map and that, according to these experts, this map presented a valid foundation knowledge structure – assertion one was supported. Supporting the overall map structure was the knowledge category inclusion of appropriate subordinate concepts, the map’s
conceptual complexity and supporting propositional linkages. The only significant limitations of the presented concept map were the exclusion of the concept vulnerability and the degree of individual interpretation of the propositional linkages. Nevertheless, the psychometric security risk management concept map (Figure 6.5) provided an appropriate representation to respond to Research Question four in the affirmative.

In Phase four, assertion two considered if MDS concept mapping developed and represented an appropriate knowledge structure, and responded to Research Question five. Assertion two was supported from evidence gained from the psychometric security risk management concept map and comparable concept mapping studies. Evidence of knowledge structure, concept clustering, conceptual relationships and the MDS concept mapping methodology was demonstrated in security expert interviews. MDS concept mapping methodology appeared to develop and represent a valid consensual map, limited only by the insertion of propositional linkages. These outcomes provided an affirmative response to Research Question five, that from the evidence presented MDS concept mapping is an appropriate quantitative methodology to develop and present psychometric concept maps – a finding supported by previous concept mapping studies (Kealy, 2001; Martinez-Torres, et al., 2005; Trochim, 2005b; Turns, et al., 2000).

Throughout the study, appropriate measures of both reliability and validity were found. However, the MDS STRESS1 measure was not the most appropriate reliability indicator, producing a higher measure than more stable phenomena and reflected in a similar MDS concept mapping studies (Trochim, 1993). MDS concept mapping would appear to require a more unusual approach to the measures of both reliability and validity, due to the implicit nature of data. Therefore the reliance on this single measure would not necessarily be the most appropriate, resulting in the need to consider a degree of triangulation.

9.3 Recommendations
In considering the findings from the study in conjunction with the literature review (Chapter 2), a number of recommendations indicate how knowledge and understanding
of the psychometric MDS security risk management concept map may benefit academia and professional understanding of security risk management, including pedagogy, security body of knowledge and security risk management application. The study has achieved the research objectives defined at the commencement of the study. However, there have been many potential avenues for further inquiry, where more thorough investigation of the study could be considered. Therefore, additional avenues of future research are presented.

9.3.1 Benefits of the psychometric security risk management concept map

The psychometric MDS security risk management concept map developed and presented in the study can provide a number of valuable benefits. Security lacks a definition (Tate, 1997) and yet is considered to be a distinct field of study (ASIS International, 2003). As this study has proposed, supported by professional security bodies (ASIS International, 2004), security risk management is a unique knowledge category of security. Nevertheless, the security industry is a diverse and a speciality industry that has a requirement for both generic and domain specific skills (Hesse & Smith, 2001; Manunta, 1996) and being a relatively young and emerging discipline, continues to expand (Fischer & Green, 2004; Tate, 1997).

Risk management, as proposed by AS4360:2004, has been the primary source for security practitioners. The Risk Management AS4360:2004 Standard is often considered “almost a de facto global standard” (Jay, 2005, p. 2) and has become an international template for dealing with risk, having been used in Canada and United Kingdom, and translated into Cantonese, Mandarin, Japanese, Korean, French and Spanish (Jay, 2005). In addition, the Risk Management AS4360:2004 Standard is used in diverse disciplines, from finance to engineering and is used extensively by security and risk professionals across Australia (Beard & Brooks, 2006; Jones & Smith, 2005).

Nevertheless, as Standards Australia stated in their recently released handbook of security risk management, “the field of security risk management is rapidly evolving and as such this Handbook cannot cover all aspects and variant approaches” (2004b, p. 2).
As the security risk management concept map has demonstrated, threat is a critical factor when considering security risk. However, the Risk Management AS4360:2004 Standard does not present the concept of threat or other security related concepts like vulnerability, even through Risk Management AS4360:2004 Standard is a primary resource for security practitioners when considering and applying security risk management.

The need to increase knowledge of security risk management can be shown through an Australian Federal Government supported initiative with the Risk Management Institute of Australasia (RMIA). These groups, among others, developed and in 2007 published the Security Risk Management Body of Knowledge guide for practitioners. The guide attempts to resolve security risk management elements such as “a framework for critical knowledge, competency and practice areas which managers, practitioners, students and academics alike can apply to recruit, train, educate and measure performance” (Risk Management Institute of Australasia, 2007b, p. 1).

Most tertiary security courses have been developed from related disciplines – police, justice or criminology studies (Smith, 2001b; Tate, 1997) – even through according to ASIS (2003) these disciplines should be separate and discrete from security. At the tertiary level there is a lack of academic security programs, with most focused on criminal justice, crime prevention or risk management (Jay, 2005; Manunta, 1996). This variability of the security discipline may result in security research that is not necessarily appropriate for the security industry. Security “is not merely a matter of intuition or common sense: it involves a complex body of knowledge, analytical abilities and know-how” (Simonsen, 1996, p. 229). Nevertheless according to Smith (2001), security knowledge is being established through the development of appropriate domain concepts, a view supported by Simonsen who stated that the “body of knowledge of security has grown rapidly in the past decade” (1996, p. 230).

The psychometric security risk management concept map provides, to some degree, a body of specialised security knowledge. Understanding the risk management concepts
that security experts consider when assessing security risk, how these relate and integrate, and why security experts consider these ideas, can aid pedagogy, the security body of knowledge and applied application. The security risk management concept map may assist in promoting knowledge and understanding on security risk management.

Finally, the study also developed and presented 14 security knowledge categories, developed from the critiqued security courses. In the past, security knowledge has focused on electronic, manpower and physical security categories. However, according to Yates (2007) this traditional categorisation does not consider a large range of security-related functions, including business continuity, emergency response, information security and risk management. Therefore, this study has furthered the development and understanding of security knowledge categories, aiding the development of a consensual security body of knowledge.

9.3.2 Future research
Recommendations for further investigations include the methodology of psychometric MDS concept mapping, propositional linkages, MDS knowledge clustering and the reliability of the MDS concept mapping technique.

9.3.2.1 Methodology of MDS concept mapping
Within the context of the study, the research demonstrated the ability of MDS to be used in the development and presentation of psychometric concept maps. Similar studies have also presented appropriate outcomes within their own knowledge domains (Kealy, 2001; Martinez-Torres, et al., 2005; Trochim, 2005b; Turms, et al., 2000). However, these research studies have approached the MDS concept mapping task with differing methodology, leading to possible criticism of results. For example, there is generally little comment by these researchers on the development and insertion of propositional linkages, a critical aspect in giving the map conceptual knowledge, as well as consensual understanding.
Longitudinal analyses of knowledge structure by means of concept mapping to assess conceptual change has been used in science education (Hewson, 1996; Markham, et al., 1994). Comparable studies could be also conducted in security science. In addition, the use of two independent homogenous expert groups who both complete the MDS concept mapping technique within the same knowledge category would result in a comparison on how spatially similar MDS concept maps may be. Other studies (Bennett & Rolheiser, 2001; Markham, et al., 19941) have prescribed concept mapping assessment and testing measures, which could be used to test the degree of concept map similarities.

Nevertheless, the methodology of MDS concept mapping does require further inquiry to establish this mapping technique, before being introduced into general pedagogical use. Pedagogy benefits may include the use of concept mapping in areas of curriculum development, course structure and assessment. As Wilson argued, concept maps are personal, however, when integrated with peer discussion are extremely useful in assisting students to verify and comprehend their understanding (Bennett & Rolheiser, 2001; Novak, 1996).

### 9.3.2.2 Propositional linkages

The propositional linkages developed and presented during the study had a degree of individual interpretation, an issue supported by Bennett and Rolheiser (2001). Therefore it could be claimed that the majority of concept maps would suffer from a degree of interpretation, particularly as the knowledge category becomes more implicit. This study reported the use of the Delphi method to improve propositional linkages, however, an alternative method could be the use of *propositional ranking* (Figure 9.1). Instead of presenting a single label when developing a concept map, a choice of *n labels* would be presented. Each participant could rank, in order of importance, their *most preferred* label.

The propositional ranking approach may provide an alternative approach to the Delphi method. In addition, a degree of analysis could be applied between participants and/or ranked labels. As Kealy stated, “in the past few years researchers have begun to combine
the practice of concept ratings with knowledge mapping procedures in innovative ways to improve map construction, as well as map assessment” (2001, p. 332).

![Propositional ranking diagram](image)

Figure 9.1 Propositional ranking

### 9.3.2.3 MDS mapping strength of concept relationship and clustering

The study claimed that based on spatial proximity, MDS represented a degree of strength of concept relationships. Research could consider a method to metrically graph MDS concept maps to measure the intensity of relationship between concepts. In addition, concept clusters could be used to indicate knowledge categories and subsume related concepts. MDS could be applied to a large list of concepts, which would group similar concepts in close spatial proximity or clusters – resulting in these clusters representing knowledge categories. The use of MDS to develop and present knowledge categories had been raised in the past (Edmondson, 2006; Martinez-Torres, et al., 2005), however, this has generally been within the context of curricula design and development. Both metric measurement of concept relationships and the clustering of knowledge categories are areas of research that could prove to be potential avenues for further research.
9.3.2.4 Reliability
Trochim stated that because “concept mapping is so complex, it is difficult to conceive of a single overall reliability coefficient” (1993, p. 5). To attempt to overcome this issue, this study considered a number of reliability and validity measures throughout the study. One such measure was Cronbach’s Alpha reliability, a model of internal consistency based on the average inter-item correlation (Cohen, et al., 2002). The study used the source data from the original expert similarity data (Appendix H), which had a degree of separation from the MDS analysis. Research could assess the level of correlation between expert validated concept maps, MDS goodness-of-fit (STRESS1) and Cronbach’s Alpha measure of source data.

9.4 Limitations
Limitations of the study were identified and include the provision of a conclusive definition of security, breadth of tertiary security undergraduate courses critiqued, the expert sample size and nature, the ability of MDS to develop cognitive knowledge structure, reliability and validity of concept mapping, and the interpretative nature of propositional linkages.

9.4.1 Defining security
Tertiary security courses were selected and validated by security experts. However, security has no clear definition (Horvath, 2004; Manunta, 1999; Tate, 1997) and “means different things to different people” (Davidson, 2005, p. 73). According to Hesse and Smith, security is diverse, without a defined knowledge or skill structure (2001, p. 89). Therefore, homogeneity in the selection and validation of expert groups at each study phase may have introduced a degree of distortion. To address this concern independent resources, where available, were used for data triangulation, for example the ASIS International 1997 to 2003 Academic/Practitioner Symposia (ASIS International, 2003).
In considering the security risk management category, two or more security experts did recommend additional subordinate concepts, namely *treatment* and *vulnerability*. Expert opinion indicated that both discrete concepts were relatively important ideas within the knowledge category of security risk management and should have been included within the psychometric concept map. Nevertheless during Phase one of the study (Chapter 5), these two concepts were not identified, resulting in the exclusion of these concepts within the psychometric security risk management concept map. Therefore, the security risk management concept map has to be considered in the context of the homogeneity of the expert validation groups and the exclusion of two security risk management concepts.

### 9.4.2 Course critique and date extraction

The course critique was completed in mid 2005 (Appendix D), resulting in an analysis of seven tertiary security undergraduate courses (Appendix E). Since then there has been an increase in security undergraduate course offerings in the critiqued countries, with a claim that in the United States there are “more than 300 two and four-year institutions that participate with homeland security programs” (Davidson, 2005, p. 72). Supported by the findings in Phase one of the study (Chapter 5), it could be argued that these are not necessarily appropriate organisational security undergraduate courses. However given the breadth of security, not all security categories or security risk management concepts were necessarily tabulated. Therefore, conclusions made in this study refer specifically to the presented knowledge categories and subordinate concepts.

### 9.4.3 Sample size and nature

For enhanced statistical confidence, the sample size of each phase of the study could have been larger. In addition, due to the non-probabilistic sampling approach, homogeneity of participants and experts in both Phase two MDS knowledge structure and Phase three Expert validation could have been experienced. Both factors may have resulted in a degree of error in the psychometric security risk management concept map. In an MDS concept mapping study on reliability (Trochim, 1993) an average of 14.62 participants were used, with the conclusion that MDS “stress values based on sample
sizes half as large are nearly as good as the full-size values, suggesting that even smaller samples ... may produce maps that fit almost as well as samples twice as large” (Trochim, 1993, p. 11). Therefore based on the supporting MDS knowledge mapping evidence and with the need to gain an appropriately valid MDS sample size, the Phase two sample size of 29 participants was appropriate. Nevertheless, conclusions made have to be considered within the context of the sample size and nature of non-probabilistic sampling.

9.4.4 Cognitive knowledge structuring

The study has demonstrated that an appropriate expert knowledge structure of security risk management can be presented. However, because knowledge is dynamic, complex and implicit (Lockhart & Craik, 1990; Rennie & Gribble, 1999), does the MDS concept mapping methodology demonstrate cognitive knowledge structure? Exemplar knowledge categorisation, which informed the study, indicated that concepts have relationship attributes based on similarity (Cohen, et al., 2002). Nevertheless, the ability of proximal data to represent knowledge structure has been criticised, both in its ability to represent cognitive structure and to provide useful pedagogy information (Smith, 1984). Therefore, conclusions made refer specifically to the psychometric security risk management concept map and should not be extrapolated to other knowledge categories.

9.4.5 Reliability and validity of MDS concept mapping

Reliability and validity limitations were considered throughout the study, although there was restricted literature on both measures within the context of MDS concept mapping. Measures considered MDS goodness-of-fit (STRESS1), Cronbach’s Alpha reliability, face and concurrent validity, and study triangulation.

MDS STRESS1 was a suitable MDS concept mapping measure, if a map achieved a value of less than 0.1 (Johnson & Wichern, 2002), of both reliability and validity. However this study, as discussed, achieved what Johnson and Wichern would consider an inappropriately high STRESS1 (STRESS1=0.28, RSQ=0.64) measure. Nevertheless, this measure replicated findings of a similar larger MDS concept mapping study
(Trochim, 1993). In addition, Kealy (2001) presented even higher STRESS1 results (STRESS1=0.36 to 0.35), with many other relevant MDS concept mapping studies not reporting their MDS goodness-of-fit measures (Lockhart & Craik, 1990; Markham, et al., 1994; Martinez-Torres, et al., 2005). Therefore, conclusions made were considered within the context of the MDS STRESS1 measure, which had bounded support from comparable MDS concept mapping studies.

The study used Cronbach’s Alpha reliability measure, producing a high ($\alpha=0.93$) value. In contrast, another researcher stated that “there is no known way to estimate alpha for the matrix data used in concept mapping” (Trochim, 1993, p. 7). However, this study used the original Phase two expert similarity source data, extracted from Appendix H, before summation and conversion to half-matrix data for MDS analysis. These original data comprised a measure from each participant for each paired concept, facilitating the Cronbach’s Alpha measure. Data summation and conversion to half-matrix separates, to some degree, the final half-matrix data and therefore, the MDS concept map from the original similarity data. Nevertheless, reliability measures of original similarity data had been used by another researcher to demonstrate reliability (Martinez-Torres, et al., 2005).

There appeared to be bounded studies on the validity of MDS concept mapping, with only two articles sourced in this research area (Aidman & Egan, 1998; Kealy, 2001). Previous studies had shown “evidence of concurrent validity” (Aidman & Egan, 1998, p. 12), where novice to expert domain maps were measured as a means of assessment. This study produced only a moderate Pearson two tailed result ($r=0.32$, $SD0.19$, $\geq95\%$). However, the importance of the Pearson two tailed validity measure may be abridged by the strong expert validation of the psychometric security risk management concept map, nevertheless, the study conclusions have to be considered within the context of the validity measures.
9.4.6 Propositional linkage validity
Through variance of expert interpretation, the propositional linkages reduced the validity of the psychometric security risk management concept map. Available literature did not discuss the development, insertion and assessment of the MDS concept mapping presentation, arguably important considering that propositional linkages allows an external person to read and understand the concept map. Therefore, conclusions made refer specifically to the security risk management knowledge category and resulting psychometric MDS concept map.

9.5 Conclusion
This chapter summarised the research questions raised in Chapter 1 and described the phases of study. Conclusions were presented, providing an overview of the study. Recommendations discussed the benefits of the study and proposed avenues for future research. Benefits of the study proposed that the psychometric security risk management concept map and security knowledge categories may further academia and professional understanding of security and security risk management, which included pedagogy, security body of knowledge and security risk management application. In addition, potential research avenues included the methodology of MDS concept mapping, methods to develop and insert propositional linkages, the use of MDS knowledge clustering and the reliability of the MDS concept mapping technique.

Limitations of the study were identified and presented, comprising the increasing breadth of tertiary security undergraduate courses, the bounded ability to provide a definitive definition for security, the non-probabilistic sample size, the homogeneity of the participating expert groups, the ability of MDS to develop cognitive knowledge structure, the reliability and validity of concept mapping, and the interpretative nature of propositional linkages.

The study has developed and presented a list of security knowledge categories and the psychometric security risk management concept map, both of which are rich in complexity and interpretation. Security experts, at every phase of the study, provided
greater implicit insight into their knowledge structure. However, the discipline of security still has much to learn in respect to its body of knowledge, nevertheless this study has aided, in part, the development and presentation of a consensual security body of knowledge.

Finally, psychometric MDS concept mapping proved to be a suitable study tool in the development and representation of the security risk management concept map. Research into MDS concept mapping will aid our understanding in augmenting insight into complex domain knowledge structures, assisting in furthering our understanding of how groups understand implicit concepts. Greater understanding will assist in better teaching our current and future generations.
REFERENCES


Erickson, F. (1986). Qualitative methods in research on teaching. In M. C. Wittrock (Ed.), *Handbook of research on teaching* (pp. 119-161). New York: Macmillian Publishing Company.


204


School of Engineering and Mathematics. (n.d.). *Bachelor of Science (Security)*. [Brochure]. Perth, Western Australia: Edith Cowan University.


212


APPENDIX A

PILOT STUDY: PHASE THREE EXPERT INTERVIEW

INTRODUCTION
As an expert in security, your participation and time in this study is greatly appreciated.

Approximately a week ago you were given the following concept map of security risk management, showing how these ideas may be linked and their possible relationships, and also an overview of my study.

Today, I intend to ask you some questions regarding the concept map. These questions will begin with some general questions on the overall structure of the concept map, leading into more specific relationships between the risk ideas.

Feel free to comment on what you consider are important issues at any time. We do not have to adhere to the order of the questions.

I intend to tape record our interview and once the tape is turned on, will request your permission. Data collected will remain confidential, you will not be identified and the only other people who will have access to the data will be my two academic supervisors.

INTERVIEW
Turn on tape - Can I request your verbal permission to tape record this interview?

Before we start, do you have any general questions regarding the study?

QUESTIONS
General concept questions

Q1. The map shows an overall structure for the security category of risk management. Do you consider that this whole structure describes the ideas underlying security risk?

Q2. Do you think that this structure shows the relationship in the ideas of security risk?

Q3. Do the think that the ideas in security risk represent your thoughts on this topic?

Q4. What do you feel are the three most important parts of security risk?
Q5. From your knowledge of security risk, are there any other important ideas that could be included?

Specific map questions
Q6. On the map threat would appear to be a central theme, what are your comments regarding this?

Q7. Consider the ideas risk, threat, consequence and decision. Do you think that these links are justified? Why?

OR

Q7. When you consider the risk management process, would you follow the thought of risk, threat, consequence and decision?

Q8. On the map consequence is shown aiding a decision. Would you consider that these two ideas are in the right order?

Q9. According to the map, cultural risk and perceptions are not related, occupying different areas of the map. Do you feel that these are correctly located and if so, what are your reasons?

Q10. Should judgement be linked to threat? Why do you say that?

Q11. Should judgement be linked to model? Why do you say that?

Q12. Would you place the idea of statistics between the ideas of risk and risk management?
Q13. Do you feel that the location of hazard is appropriate and why? How strong is the relationship between hazard and decision?

Concluding questions
Q14. Would you like to add or change any linking statements?

Q15. Now that we have spent some time considering this map, do you feel if there are any security risk ideas missing?

Q16. If you were asked to map the concepts of security risk, how would you do this?

Q17. Do you consider that this map provides a general consensus map of security risk ideas and their relationships?

Q19. Do you have any final comments?

END
Thank you for your time.
APPENDIX B

PILOT STUDY: PHASE THREE EXPERT INTERVIEW TRANSCRIPT

The following transcript was taken during the recorded interview of one of the two security experts, interviewed during Phase three of the pilot study.

<table>
<thead>
<tr>
<th>Interview participant</th>
<th>Recorded comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interviewer</td>
<td>Start time: 8.00am - Can I get your verbal permission to tape record this interview?</td>
</tr>
<tr>
<td>Expert 1</td>
<td>Yep, my name is XXXXX and I give permission for recording this interview.</td>
</tr>
<tr>
<td>Interviewer</td>
<td>Thanks, before we actually start have you got any questions on the study, do you feel you have a good idea of the study?</td>
</tr>
<tr>
<td>Expert 1</td>
<td>Yes, we had a look at it the other day just briefly, err … and it does look good. Just one quick one, this one here “configs” is?</td>
</tr>
<tr>
<td>Interviewer</td>
<td>Ah, configuration, configure.</td>
</tr>
<tr>
<td>Expert 1</td>
<td>Could you just explain this bit here, like judge, configure?</td>
</tr>
<tr>
<td>Interviewer</td>
<td>What, what this has been developed from is multidimensional scaling. I basically used three different people to fill out a quantitative survey and put it through multidimensional scaling and what that’s actually done … is position these ideas within this pattern.</td>
</tr>
<tr>
<td>Expert 1</td>
<td>Yep</td>
</tr>
<tr>
<td>Interviewer</td>
<td>What didn’t show was the actual arrow links.</td>
</tr>
<tr>
<td>Expert 1</td>
<td>OK</td>
</tr>
<tr>
<td>Interviewer</td>
<td>So what I’ve done is interpreted the position of each idea and shown the links. Now I have tried, tried to, aid the relationship between those ideas, sort of come up with these terms.</td>
</tr>
<tr>
<td>Expert 1</td>
<td>Sure, no problems.</td>
</tr>
<tr>
<td>Interviewer</td>
<td>So perception configures judgement or aids judgement, or.</td>
</tr>
<tr>
<td>Expert 1</td>
<td>Yep, yep, no problems.</td>
</tr>
<tr>
<td>Interviewer</td>
<td>Those are some of the areas I would like to talk about.</td>
</tr>
<tr>
<td>Expert 1</td>
<td>Yep, that’s fine.</td>
</tr>
<tr>
<td>Interviewer</td>
<td>[Question 1] So questions one, the map shows an overall structure for the security category of risk. Do you consider that this whole structure describes the ideas underlying risk?</td>
</tr>
<tr>
<td>Expert 1</td>
<td>Yep, I do. Erm … its including a lot of things that … normally aren’t included that a lot of people don’t think about err particularly the Intel part. I find that pretty good, but the relationships are very helpful.</td>
</tr>
<tr>
<td>Interviewer</td>
<td>How do you, some of those relationships, when you say relationship arm are you referring to the labels I have put on the links?</td>
</tr>
<tr>
<td>Expert 1</td>
<td>That’s right, the labels on the links, err, the directions of the arrows, err would make it very clear for somebody who, who wouldn’t know much about risk. Who would need to be given like a mind map, particularly this process here [pointed to the risk, threat, consequence, decision flow] that highlighted as well, because that’s really the very skeleton of it and these are really all of the things that really count as well.</td>
</tr>
<tr>
<td>Interviewer</td>
<td>We’ll actually talk about that that skeleton you sort of pointed out between risk, threat, consequence and decision, we’ll actually talk about that because from the study that actually came out as quite a strong linkage throughout the err analysis, but we’ll get into that in a little more detail.</td>
</tr>
</tbody>
</table>
Great.

[Question 2] Excellent, err do you believe that this structure shows .. a valid and correct relationship in the ideas of risk?

Yep, …

And I suppose sort off moving on from there do you err do you err the location of those ideas, what are you thoughts on the locations of these ideas as a general overall structure?

Err, my comments on it … it visually shows err where the core of this whole entire concept is. Err, as we said risk, threat, consequence and the arrangement of everything else around it err, really does simulate the importance of all the different areas, and where they lie and err, it does represent that.

[Question 3] Thanks XXXX. Do the think that the ideas in risk represent your thoughts on the topic? So all the ideas down there and I think you may have alluded to some of that idea.

Ya, this really represents what I would err what I would personally think and the whole concept of security risk.

[Question 4] Thanks good … a fairly sort of specific question, what do you feel are the three most important parts of security risk? Are they noted there [pointing to the map] or is there any missing or is there any particular aspect do you think are key aspects that are not only indicated in the map, but you know, are important aspects?

I suppose there are lots of aspects within decision err that you know don’t get included in here because its just err I suppose they just don’t belong in here because they are sub err .. sub-decision, such as err a decision would largely be based on how much control mechanisms are already in place err the likelihood of err of the threat occurring, the likelihood of the consequence re-occurring err .. But once again they’re decision things that to me to me the decision part, which is probably the most important parts .. the other one is really consequences.

[Question 5] Is the other particular idea that you feel is important within all of those ideas?

Err, .. I think the Intel part is important because that err .. that is where you would first of all, yep support identifying threats, but it once again Intel also links into your decision-making process as well, which allows you to determine consequences. So I think it really is important.

Interesting, do you think there should be a strong link between Intel and decision? Should it be shown or .. do you feel that Intel is probable in the wrong spot?

I say that there is a link between Intel and decision-making err whether or not it err that represents, I supports, yep it would be good for representation to be shown if possible err it really does support your decision-making even through you have identified your consequences, you’ve derived that from Intel you still get you key goal, which is justifying your decisions based on your Intel as well.

How do you feel Intel relates to threat? I suppose the question is, is Intel a stronger relationship with threat, or is it a stronger relationship with decision? What are your thoughts on that?

I think err there is still that definitely err a threat identification component of Intel, but just as much I think there’s a relationship with decision-making err .. because your decisions are still based largely on your Intel err and I’d say that we could put line all over the place and also largely based on statistics as well and analysis err decision-making is .. err as well so I would say that Intel does have a relationship with threat, just as much as it does with decision but err once again it decision also has comes from your analysis and your statistics part of it to, it’s a second based Intel developed yourself rather than what you get externally.

So, talking about things like analysis and comms and probability, Intel is shown...
here to feed into threat, .. do you think Intel is really just a way to define the threat as much as analysis and probability is, and in essence does it aids decision-making as much as probability, analysis, communication, .. that it’s a threat that actually defines a consequence and defines a decision? Do you think that this actually shows the thought process or is it all got to be taken out and put with decision?

Expert 1
I think err like you said at the very beginning Intel, analysis, comms, probability and I would also include statistics all support the threat identification err and then I would say that they also all support the decision-making as much as the consequence identification, .. because once again you are looking at things within decision such as your likelihood and err the other controls already in place and the value of the asset and the value of what you are trying to protect err the knock on consequences, the continuing value and they all come down to analysis and statistics as well and I think comms is important as well. So I say that even through they all support they also support decision.

Interviewer
So there are additional links that could be put in there?

Expert 1
There could be. Ya, but this structure is good you don’t want to destroy that. You want to some how get around that.

Interviewer
Ya, that the way it came out of the analysis program. So, it’s sort of tied by the consensus approach. [Questions 5] From your knowledge of security risk, are there any other important ideas that hasn’t been included? … Does any thing jump out, as you talked about control and that?

Expert 1
Ya I was going to say that there are definitely to me decision-making, there are subsections to decision, that really encompasses decisions so overall concepts are definitely included in there, even though to mine there are things in decision-making process pop out as important, I believe that’s irrelevant here because as we are looking at major concepts so I think that [pointing at map] does cover it.

Interviewer
[Question 6] What we’ll do is just move on to some specific idea within there, the first on is on the map threat would appear to be a fairly central theme in our risk map, what are your comments regarding this?

Expert 1
Risk is largely associated with managing threats err security risk is more associated with management threat, so I would say that that is quite a central theme, as the concept of risk is not only around the concept of threat, so are all the other processes.

Interviewer
So you are saying from a security risk aspect, threat is a vital aspect err

Expert 1
Without threat there is no need for whole of risk concepts

Interviewer
[Question 7] Excellent. .. Err, consider the ideas risk, threat, consequence and decision. Do you think that these links are justified and I suppose the next question is, why?

Expert 1
Err, I believe they are justified err why is because .. that is the process err you have a risk which is a threat, threats have consequence and consequence aids decision like its outlined here exactly and that the very basic concept of security risk and why we go about identifying risk and why we end up managing risk.

Interviewer
[Question 8] Great, on the map consequence is shown aiding a decision, so these links between consequence aids a decision, but would you consider that these two ideas are in the right order, in other words err could you swap those around, are they a valid sequential thought process or are they very closely linked and are in essence the same?

Expert 1
I think they’re in the right err they’re right order .. I wouldn’t say they were the same err .. I just think they’re in the right order.

Interviewer
[Question 9]. According to the map, cultural risk and perceptions are not related so on the map, perceptions or psychometric risk are quite different located on the map
as ideas. Do you feel that these are correctly located and if so, what are your reasons?

Expert 1
Ya, I do think they are correctly located err … from our point of view its hard because as security professionals err the perception side doesn’t really come into it when we go down to decision-making, but if we were to give our risk analysis to some body who wasn’t a security person their perceptions would be completely different. So that could affect the decision-making, but from our point of view the way we are trying to study it err I think they are all in the right place, .. once again depending on how the organization is structured and who makes the decision is based on perceptions. So I would still say that they are in the right place.

Interviewer
I was quite surprised by .. by the spread because I had always seen perceptions and cultural risk being very similar in .. in ideas, now wherever that’s the way we teach it because we teach it in essence in the same evening and I’ve always looked at cultural risk and psychometrics as being two ideas of the world, so I thought they’d be closely linked together.

Expert 1
Ya, I agree with you, they’re very close subjects err to the point they could be considered that same thing.

Interviewer
But when I saw that come out, I suppose gave it a little more thought and looked at what perception tends to be more of an individual or even up to a community, how people perceive things and how communities perceive things, where cultural tends to look at organizations, communities as well, in how they operate and how they go about processes, so it tends to be more removed from the individual. Now do you think that is a valid argument and if so, is that why perception is closely linked to judgement?

Expert 1
Ya I would agree with that, that perception is more personal and cultural is more of a collective, more of a group, more of err a way of doing things that’s evolved over time, so ya I would agree with that.

Interviewer
So from this map, has that changed your view of cultural risk and psychometric risk, in how you would possible look at those two ideas?

Expert 1
Ya, it does to some degree err … I suppose looking at the map it all about judgement after perception and err cultural risk and err it characterizes the consequences as well, which is definitely true.

Interviewer
Ya, it’s quite interesting, because when it came out I thought that’s wrong.

Expert 1
Ya.

Interviewer
But when you really start analysing it and possible thinking about it.

Expert 1
Most definitely.

Interviewer
[Question 10] Right question 10, should judgement be linked to threat? So judgement .. is actually quite a long line and in essence what .. this is spatially represented, in other words the closer the ideas are the more they relate to each other, the further they are away the further the thought process or idea is and judgement is actually quite a distance from threat. Do you think that’s a valid link here or do you think judgement should be linked down to consequence or down to hazard/decision?

Expert 1
I would definitely say that consequence er thinking of it now er because .. your threat is something that’s definite and err its something that’s there, whereas your consequence is something that’s variable depending on someone’s particular position er the way they think about things er there is a perception altogether. The consequence to one person may not be the same consequence as another, but with threat it is still definite, its still kind of the same er with the threat doesn’t change.

Interviewer
But would there be an aspect of subjectivity to threat? You could possible think of a threat as, are we going to be hit by terrorism and some people would say, we’re in
Perth and a safe environment and they would say very unlikely. But other people may say, well we could and we will be, so there's is a subjective aspect.

I would say that, that's more of a likelihood aspect er .. which I see isn't included in here, its kind of morphed into the decision-making, because the threat is we are going to be it by terrorists and that threat is still the same, but the judgement as to whether its going to happen or not, is a judgement thing, but the threat is still the same. I don't really think er it depends on where I suppose likelihood would be included in here.

I will make a note to raise likelihood, because you have raised that a few times. I've got probability in there, which is I suppose another term for likelihood.

Ya I think it would be, definitely er .. I would say it would be linked in a bit more. I would personally say err I have used likelihood as err a really big part of making a decision at the end.

So, if we change the term from probability to likelihood and .. probability is actually located quite close to consequence and decision, it actually flows through this way, so likelihood has a cultural aspect that is quite strongly linked to consequence which then defines your decision.

Yep, I would say so, yep. … Still I think that a threat is a definitely a thing, that’s just there and err and a judgement doesn’t form a threat, threat stays the same. Things like likelihood can be variable, consequence can be variable, determining on your perspective. But I still think that a threat is a definitive thing.

So in essence, the higher the likelihood .. the likelihood would be based on the consequence, in other words if it’s a very low likelihood than a very high consequence, so you can basically using the risk model.

That’s right, that’s what I would say.

[Question 11] Another unusual one judgement is shown linked to model. Now I suppose there is a lot of semantic aspects with what is modelling and what is a model er .. what are your feelings with that link between judgement and modelling or model?

There is a link err … between it and when you do model I suppose it comes down to your perception, which is basically your judgement and that will overall define how you go about your modelling processes, because once again it quite variable depending on those two factors.

Ya, so you feel quite comfortable?

Ya. .. As we can see spatially it quite distance, as well and that’s the way I would see it as well.

[Question 12], The idea of statistics sitting at the top of the model is located between of risk and risk management? If you had to draw this map, would you place it there or what are you thoughts of that location?

I would have statistics linking to possible .. ya to likelihood and risk management linking with decision, but then risk management linking back to threat. Because I would say based on the statistics you get from analysing, once again these are all kind of tied in. But err these all slightly overlap, but err from your statistics you
could to some degree determine the likelihood and consequence of an err threat and that would aid you in your decisions, which would also go back to your risk management plan. That’s what your decision would ultimately define, some form of risk management, which is managing your threat.

Interviewer: So in essence the link between risk management and threat is valid?

Expert 1: Ya.

Interviewer: As a concept or idea where do you see risk management? Is it encompassing all of those ideas or taking a few of those ideas?

Expert 1: I would say that risk management is the whole thing, no I wouldn’t say that actually, I would say that all of this brings about risk management. You follow this process in analysing and defining consequences and you take into account judgement, perception, you look at your intel, you look at the risk before it and you finally come to a decision [exaggerated] err and from there you come about a way of managing a threat. That’s how I would see it.

Interviewer: Ya. Why do you feel that with statistics actually ending up here, err . . . what are your thoughts this ending up here, is it valid or should this be some where else or is it a belief that people feel risk and statistics are possible one and the same thing?

Expert 1: I would say that statistics can be extracted from a risk. So ya a risk is extracted to be a statistic.

Interviewer: So when you say extracted?

Expert 1: You can break down a risk and represent it statistically.

Interviewer: But do you feel that people look at risk as a statistical process?

Expert 1: Some people do, ya. I would say that some people.

Interviewer: And would that be a security focus for security professionals to look at risk as a statistical process?

Expert 1: I would say that professionally and in order to be taken seriously then ya, definitely have to, really do.

Interviewer: That’s an interesting comment.

Expert 1: Just from what I have seen and what I’ve done and would do in the future, statistics would be a large part of it, because err statistics helps you in justifying risk and really laying down the law and saying this is what’s going to happen and I can prove it. So it’s more of a quantitative approach rather than a qualitative. I think that why that’s a lot more sound, so I would personally see risk as being statistics and that’s how you break and that aids heavily in err if you take that approach in easily identifying likelihood and consequences.

Interviewer: Ya. So you feel that there is quite a strong link between risk and statistics at a more abstract level?

Expert 1: Ya, definitely.

Interviewer: Even though statistics is quite a defined term, when in essence when you talk about statistics your think of numbers, but when you think of risk you think of things like threats and likelihood?

Expert 1: Ya that’s right, yep.

Interviewer: But in reality, do you think that it’s quite valid for people to think that risk and statistics are a very similar idea?

Expert 1: Ya, absolutely, practically in a process like this err.. and really doing it properly, and really properly identifying probability and consequences , once again basing it on facts and basing it on data, rather than basing it on what you think, I think statistics is pivotal.

Interviewer: [Question 13] With the location of hazard, which is right down the bottom next to decision, do you feel that the location is appropriate and have you got any comments on that?
I suppose I could do without it.

In other words, do without hazard?

Do without hazard, yep.

As an idea hazard, is there a better term within those ideas to define hazard and would people use

Say consequences for hazards?

No, just using the idea hazard, is there a better idea within this map that really defines hazards or is hazard just an idea within another idea?

I think the hazard aspect is a combination of consequences of your threat. That actually measures it as a hazard.

So a combination of threat and consequence?

Ya, a combination of threat and consequence, that’s right. I think its just included within decision, just a concept that should be in decision.

So from a security professional’s point of view, would you use hazard?

Hazards a good word.

Is it used in the industry?

It’s not used in the industry, it’s really associated with .. it’s embedded elsewhere.

You say it’s embedded elsewhere?

When people just talk about general things, the concept of hazards is included, but hazard itself is a concept, that’s important.

You say its embedded elsewhere and its an idea that, although used in security is actually outside security, is that a valid comment?

Ya, at the same time a lot of its health and safety, definitely. That’s what people see it as.

So from a security point of view, it probably not a valid term or idea?

That’s right.

And that really, we use threat and consequence?

That’s right, threat, consequence and probability together, give you your results.

Configures could be determines [between judgement and perception], other then the things we talked about before, we’re on track.

[Question 14]. Right to conclude thing, would you like to add or change any linking statements, in other words is there any particular statement is inappropriate, doesn’t give the right linkage or have you got any better idea for linkage?

[Question 15 not done]. [Question 16]. If you were asked to map the concepts of risk or the ideas of risk how would you do that, in other words, if you were given a pile of cards with all those ideas on, how would you lay them out?

Like I said before the analysis, the comms, the Intel, the statistics would be closer together and kind of grouped to one side. They would not only link to threat and be concerned with identifying threats, they would also be linked, or re-linked or somehow how a relationship would be shown that they also aid in decision-making.

… That’s probably about it.

Coming back to that, do you feel that when people make a decision that that aspect of threat, consequence/decision, they use these ideas to actually, not so much get a feel for threat, but because its subjective they use all these ideas to define threat, depending on the consequence of the threat they make a decision? Do you think this flow is more important than a decision being linked straight to communications and say probabilities selecting a decision? So it’s a fairly sequential thought process?

Yes, so the process is every things included and these concepts are still carried on and I would say that’s just fine. Coming to think of it now there’s probably no need to link if we are looking at the map saying this is how it all works out and you’re using all of these concepts over here to interrelate.
| Expert 1 | So I suppose the next is should these arrows be shown both ways, in other words, what we do, we actually have a closed loop process where you determine a possible threat based on some of these ideas and then depending on the consequence, make a decision that is a continual cycle and that these arrows fly both ways? |
| Interviewer | Er, is this in term that you keep on re-evaluating your risk all the time? |
| Expert 1 | Yes, because you are going around in a circle, you make a decision based on the consequence, so when you made a decision your then review the consequence, then review the threat and then you look at things like aspect of analysis and probability, the Intel. So would it make the map clearer if there’s arrows here? I don’t think it would make it clearer, but err .. because I think this is, looking at it like this, straight off I know that I’m going downwards and this is the way we are looking at it. But I think the pattern is fine. |
| Interviewer | [Question 17] Second to last question, do you consider that that map provides a general consensus, in other words a general idea of security risk and their relationships? |
| Expert 1 | Yep. |
| Interviewer | [Question 19]. Any final comments? |
| Expert 1 | Not really, that’s about it. |
| Interviewer | The time is 8.43am. |
| END | END |
APPENDIX C
PILOT STUDY: PHASE THREE EXPERT SKETCHED CONCEPT MAPS
OF SECURITY RISK MANAGEMENT

The following concept maps were sketched by one of the two security experts during the pilot study Phase three. However, only two (the most complex) of five attempted concept maps are presented.
### APPENDIX D

#### PHASE ONE: INTERNATIONAL LISTING OF TERTIARY SECURITY COURSES

<table>
<thead>
<tr>
<th>Institution</th>
<th>School/Department</th>
<th>Security</th>
<th>Programs</th>
<th>WWW site</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AUSTRALIA</strong></td>
<td></td>
<td>ug</td>
<td>cd</td>
<td>hd</td>
</tr>
<tr>
<td>Charles Sturt University</td>
<td>Information studies &amp; Criminology</td>
<td>N</td>
<td>Y</td>
<td><a href="http://www.csu.edu.au">http://www.csu.edu.au</a></td>
</tr>
<tr>
<td><strong>Edith Cowan University</strong></td>
<td><strong>Engineering &amp; Mathematics</strong></td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Griffith University</td>
<td>Criminal Justice</td>
<td>N</td>
<td></td>
<td><a href="http://www.griffith.edu.au">http://www.griffith.edu.au</a></td>
</tr>
<tr>
<td>Murdoch University</td>
<td>Social Sciences &amp; Humanities</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Queensland University of Technology</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Royal Melbourne Institute of Technology</td>
<td>Mathematical &amp; Geospatial Sciences</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td><strong>CANADA</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alberta, University</td>
<td>Business (Extension)</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Concordia University</td>
<td>Computer &amp; IT</td>
<td>N</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Regina, University</td>
<td>Justice Studies</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Royal Road University</strong></td>
<td>International Studies</td>
<td>N</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Ryerson University</td>
<td>Centre for Studies in Food Security</td>
<td>N</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Simon Fraser, University of Toronto, University</td>
<td>Computer &amp; IT</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>York University</td>
<td>International Studies</td>
<td>N</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td><strong>UNITED KINGDOM</strong></td>
<td></td>
<td>ug</td>
<td>cd</td>
<td>hd</td>
</tr>
<tr>
<td>Leicester, University</td>
<td>Criminal Justice</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Loughborough University</td>
<td>CHARM</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td><strong>Portsmouth, University of</strong></td>
<td>Defence Studies</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Royal Military College of Science</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

226
<table>
<thead>
<tr>
<th>University</th>
<th>Program</th>
<th>UG</th>
<th>CD</th>
<th>HD</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Southampton, University of</td>
<td>Management</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td><a href="http://www.soton.ac.uk/">http://www.soton.ac.uk/</a></td>
</tr>
<tr>
<td><strong>UNITED STATES</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Albany State University</td>
<td>Criminal Justice</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td><a href="http://www.asurams.edu">www.asurams.edu</a></td>
</tr>
<tr>
<td>Alliance University</td>
<td>International Relations</td>
<td>N</td>
<td>Y</td>
<td></td>
<td><a href="http://www.alliant.edu">www.alliant.edu</a></td>
</tr>
<tr>
<td>Auburn University</td>
<td>Justice/public safety</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td><a href="http://www.aum.edu">www.aum.edu</a></td>
</tr>
<tr>
<td>Appalachian State University</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td></td>
<td><a href="http://www.cas.appstate.edu">www.cas.appstate.edu</a></td>
</tr>
<tr>
<td>Arizona State University</td>
<td>Engineering</td>
<td>N</td>
<td>Y</td>
<td></td>
<td><a href="http://www.east.asu.edu/programs">www.east.asu.edu/programs</a></td>
</tr>
<tr>
<td>American Public University System</td>
<td>Criminal Justice</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td><a href="http://www.apus.edu">www.apus.edu</a></td>
</tr>
<tr>
<td>Bradley University</td>
<td>Risk Management</td>
<td>N</td>
<td>Y</td>
<td></td>
<td><a href="http://www.brady.edu">www.brady.edu</a></td>
</tr>
<tr>
<td>Carnegie Mellon University</td>
<td>IT</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td><a href="http://www.mism.cmu.edu">www.mism.cmu.edu</a></td>
</tr>
<tr>
<td>California State University</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td><a href="http://www.csulb.edu/depts/crim">www.csulb.edu/depts/crim</a></td>
</tr>
<tr>
<td>Central Missouri State University</td>
<td>Safety Management</td>
<td>N</td>
<td>Y</td>
<td></td>
<td><a href="http://www.cmsu.edu">www.cmsu.edu</a></td>
</tr>
<tr>
<td>Central Oklahoma, University of Colorado Technical University</td>
<td>IT</td>
<td>N</td>
<td>Y</td>
<td></td>
<td><a href="http://www.ctu-coloradosprings.com">www.ctu-coloradosprings.com</a></td>
</tr>
<tr>
<td>Coppin State College</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td></td>
<td><a href="http://www.coppin.edu">www.coppin.edu</a></td>
</tr>
<tr>
<td>Denver, University</td>
<td>International Studies</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td><a href="http://www.du.edu/gsis/iglos">www.du.edu/gsis/iglos</a></td>
</tr>
<tr>
<td>Detroit Mercy, University of</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td><a href="http://www.udmercy.edu">www.udmercy.edu</a></td>
</tr>
<tr>
<td><strong>Eastern Kentucky University</strong></td>
<td>Risk Prevention &amp; Safety</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td><a href="http://www.lossprevention.edu">www.lossprevention.edu</a></td>
</tr>
<tr>
<td>Eastern Michigan University</td>
<td>IT</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>bte.emich.edu/infosec.html</td>
</tr>
<tr>
<td>Embry-Riddle Aeronautical</td>
<td>International security</td>
<td>N</td>
<td>Y</td>
<td></td>
<td><a href="http://www.erau.edu/pr/index.html">www.erau.edu/pr/index.html</a></td>
</tr>
<tr>
<td>University</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Farleigh Dickinson University</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>fduinfo.com/majors/bytopic.php</td>
</tr>
<tr>
<td>Findlay, University</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td></td>
<td><a href="http://www.findlay.edu">www.findlay.edu</a></td>
</tr>
<tr>
<td>Florida, University</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td></td>
<td><a href="http://www.law.ufl.edu">www.law.ufl.edu</a></td>
</tr>
<tr>
<td>Florida State University</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td><a href="http://www.cob.fsu.edu">www.cob.fsu.edu</a></td>
</tr>
<tr>
<td>George State University</td>
<td>Risk Management</td>
<td>N</td>
<td>Y</td>
<td></td>
<td><a href="http://www.gsu.edu">www.gsu.edu</a></td>
</tr>
<tr>
<td>George Mason University</td>
<td>IT</td>
<td>N</td>
<td>Y</td>
<td></td>
<td><a href="http://www.gmu.edu">www.gmu.edu</a></td>
</tr>
<tr>
<td>George Washington University</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td></td>
<td><a href="http://www.gwu.edu">www.gwu.edu</a></td>
</tr>
<tr>
<td>Georgia, University</td>
<td>Risk Management</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td><a href="http://www.terry.uga.edu">www.terry.uga.edu</a></td>
</tr>
<tr>
<td>Georgia Institute of Technology</td>
<td>International studies</td>
<td>N</td>
<td>Y</td>
<td></td>
<td><a href="http://www.inta.gatech.edu">www.inta.gatech.edu</a></td>
</tr>
<tr>
<td>Grand Valley State</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td><a href="http://www.gvsu.edu">www.gvsu.edu</a></td>
</tr>
<tr>
<td>University</td>
<td>Study Area</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Hesser Collage</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Indiana State University</td>
<td>Criminology</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Indiana University of Pennsylvania</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Iowa State University</td>
<td>IT</td>
<td>N</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>James Madison University</td>
<td>IT</td>
<td>N</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>John Hopkins University</td>
<td>Business &amp; Education</td>
<td>N</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>John Jay College of Criminal Justice</td>
<td>Criminal Justice</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Keene State College</td>
<td>Safety Studies</td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kent State University</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Kentucky State University</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lewis University</td>
<td>Criminal/Social Justice</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Long Island University</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maryland, University of Massachusetts</td>
<td>International studies</td>
<td>N</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lowell, University Mercy College</td>
<td>N</td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Michigan State University</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Middle Tennessee State University</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Missouri Southern State College</td>
<td>Criminal Justice</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Naval Postgraduate School</td>
<td>Terrorism</td>
<td>N</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nichols College</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nevada, University</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>New Mexico State University</td>
<td>Engineering/Criminology</td>
<td>N</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Haven, University of New York, State</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New York, State University</td>
<td>Criminal Justice</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Farmingdale</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Northeastern University</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Northern Michigan</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
**University**  
Ohio State University  
Pennsylvania State University  
Pittsburgh, University of  
Pontificial Catholic University of Puerto Rico  
Saint Cloud State University  
Southern California, University of  
Southern Illinois University  
Southwest Missouri State University  
St. Ambrose College  
St. Edwards University  
St. John's University  
Utica College of Syracuse University  
Wartburg College  
Washington, University of  
Weber State University  
Webster University  
York College of Pennsylvania  
Youngstown State University  

**NEW ZEALAND**  
Auckland University of Technology  
Victoria University of Wellington  
Te Wananga o Aotearoa  
Waikato, University of  
Massey University  

**SOUTH AFRICA**  
University of South Africa  

<table>
<thead>
<tr>
<th>University</th>
<th>Program</th>
<th>ug</th>
<th>cd</th>
<th>hd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ohio State</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Pennsylvania State</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Pittsburgh</td>
<td></td>
<td>N</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Pontificial Catholic University of Puerto Rico</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Saint Cloud State</td>
<td></td>
<td>N</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Southern California, University of</td>
<td>Engineering / Policy</td>
<td>N</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Southern Illinois</td>
<td>Justice</td>
<td>N</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Southwest Missouri State University</td>
<td>Defence Studies</td>
<td>N</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>St. Ambrose College</td>
<td>Justice</td>
<td>N</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>St. Edwards</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>St. John's University</td>
<td>Professional Studies</td>
<td>N</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Utica College of Syracuse University</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Wartburg College</td>
<td></td>
<td>N</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Washington, University of</td>
<td></td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Weber State</td>
<td>IT</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Webster University</td>
<td>Business</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>York College of Pennsylvania</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Youngstown State University</td>
<td>Criminal Justice</td>
<td>N</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Auckland University of Technology</td>
<td>Computer and Information Sciences</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Victoria University of Wellington</td>
<td>Government</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Te Wananga o Aotearoa</td>
<td>Vocational Studies</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Waikato, University of</td>
<td>Arts &amp; Social Science</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Massey University</td>
<td>Humanities &amp; Social Sciences</td>
<td>N</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>University of South Africa</td>
<td>Justice</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**
1 ug Tertiary undergraduate degree
1 cd Tertiary post graduate Certificate or Diploma
1 hd Research or course-work higher degree
Bold lines Institutions (N=7) that were selected for content analysis (see Chapter 5)
Data Collected between May 2005 and July 2005
APPENDIX E

PHASE ONE: EXTRACTED SECURITY CONCEPTS FROM UNDERGRADUATE TERTIARY SECURITY COURSES

abandonment
abuse
access
access control
access control card encoding
access control credentials
access control device
access control elements
access control facial geometry
access control fingerprint
access control hand geometry
access control hardware device
access control history
access control iris pattern
access control levels
access control list
access control management
access control operation
access control principle
access control privilege
access control privilege limited
access control privilege unlimited
access control purpose
access control reader
access control retinal scan
access control system
access control system application
access control system components
access control system design
access control system electronic
access control system facility
access control system integration
access control system major component
access control system
access control system principle
access control system technology
access control technology
access control voice signature
access delay
accident
accident prevention
accomplice liability
accountability
accused
accused person
acquisition process
action plan
action planning
activity
actus reus
administration
administration proceeding
administration record
admissible
aesthetics
affidavit
age
agency
aggression
aid
air conditioning system
airport
alarm
alarm assessment
alarm communication
alarm display
alarm event
alarm initiating
alarm system
alarm system role
alcohol
analysis
analysis organic
analysis post incident
analysis profile
analysis sensitivity
anomie
application
applied
architectural
architectural concepts
architectural design
architectural planning
arena safety
arms and ammunition act
arrest
arrest lawful
arrest person
arrest private person
arrest resisting
arrest unlawful
arrest warrant
arrested person
arrested person search
arson
artefacts
articles seized
assault
assessment
asset
asset cost analysis
asset intangible
asset management
asset misappropriation
asset protection
asset protection liability
asset protection personnel
asset protection practice
asset protection program
asset tangible
asset value
assimilate
assist injured
attitude
dangerous event
data
data analysis
data communications
data integrity
data integrity validation
data mining
data network
data protection
data storage device
data storage device analysis
data type identification
database
decision
decision-making
decision-making tool
defamation
defect
defence
defence in depth
defensive environment
delegation
department
department accounting
department purchasing
department receiving
department shipping
design
design philosophy
desktop
detain
detained person
detect intrusions
detection
detection anomaly
detection audible
detection barrier
detection capacitance
detection exterior
detection heat
detection intrusion
detection intrusion analysis engine
detection intrusion architecture
detection intrusion legal
detection intrusion monitoring
strategy
detection intrusion sensor
detection light
detection metal
detection movement
detection open ground
detection sensor exterior
detection sensor interior
detection software
detection system
detection system computer
detection system intrusion
detection systems host based
detection techniques
detection technology
detection vibration
detection video motion
deter
deter acts
deterrent
deterrent physical
development
deviance
device
diagram
differentiate
digital age
digital certificate
digital imaging
digital video server
diminished capability
director
disaster
disaster arena
disaster management
disaster man-made
disaster natural
disaster recovery
disaster response
disc controller
disciplinary action
disciplinary case
disciplinary committee
disciplinary hearing
discipline
distance vector protocol
diversity
dna
docket management
docket register
document
document storage
driving record
drug
drug abuse
drug testing
drug trafficking
dual court system
due process
duress
duties
duty of care
dynamic routing operation
easi model
eavesdropping
economic
economic force
educate
education
education centre
efficiency
efficiency analysis
electronic
electronic commerce
electronic strategy
electronic transactions
e-mail
e-mail service
ebemzelement
emergency
emergency management
emergency personnel
emergency planning
emergency type
employee
employee current
employee prospective
employee theft
encryption
energy management
enforcing
entertainment
entrapment
entry control
entry point
environment
environmental
design
planning
use
equipment
auxiliary
record
screening
x-ray
escalator
espionage
economic act
electronic
ethics
etiquette
 evacuation
evaluate best practice
evaluate compliance
evaluation
evidence
evidence admissible
civil case
criminal case
disciplinary case
eaudio
chain
collecting
computer-based
generated
criminal
documentation
gather
giving
handling
hearsay
identification
in court
intrusion detection
label
list
material
opinion
oral
physical
collection
elements
preservation
protection
recording
relevance
report
rules of
search
secure
tamper
type
unreliable
videotape
examination
exit point
expenditure
experience
expertise
explosive
act
extinguisher
special
extortion
extranet
identification
facility
characterization
environment
management
standard
manager
planning
program
foundation
fail-safe
secure
imprisonment
pretence
technique
judiciary
fire
system protection
financial
control
prevention
planning
fingerprint
identification
fire
alarm sensor
signalling
system
audit
list
behaviour
brigade
crew
service act
building
by-products
chemistry
classes
code
control
department
detection
reaction
system
automatic
component
development
occupational health and safety performance
health and safety policy
health and safety practice
heritage
hiring
historical
historical perspective
history
hospital
hotel
housebreaking
housekeeping
http
human
human environmental factors
human resource
human rights
human weakness
identification
identification of suspect
identification target
identify
igrp implementation
ill health
imaging system
impact
impact factor
implement
incident
incident anonymous
reporting
incident command
incident critical
incident dangerous
incident detection
incident identify
incident investigation
incident irregularity
incident prevention
incident shooting
independent contractor
indicator
indictment
individualisation
industrial
industrial communities
industrial espionage
industrial sabotage
industrial system
industry
industry arena
industry petrochemical
industry stadium
industry standards
influence
informal group
information
information act
information classified
information computer generated
information corruption
information crime
information dealing
information demographic
information evaluate
information flow
information gather
information protection
information receiving
information security
information source
information source host based
information system
information technology
information transformation
informational privacy
informer
informer manage
infrastructure
innocence
inorganic
insanity
inspection
institutional
insurance
integrated electronic
integration
intelligence
intelligence analysis
intelligence based
intelligence collation
intelligence corporate
intelligence crime prevention
intelligence dissemination
intelligence documentary source
intelligence gathering
intelligence gathering process
intelligence human source
intelligence industrial
intelligence physical source
intelligence process
intelligence role
inter operability
interaction
interactionism theory
intercom system
internal dishonesty
internal theft
international organisation
internet
interpersonal skills
interrogation
interview
interview conduct
interview limitation
interview notes
interview plan
interview purpose
interview schedule
interview skill
interview technique
interview victim
interview witness
intoxication
intranet
intruder
intrusion
intrusion detection
intrusion detection history
intrusion detection justify
intrusion detection myths
The domain of security risk management could be described by the concepts listed below. Which of the following concepts do you believe should not belong in the domain of security risk management? Please provide a short reason.

<table>
<thead>
<tr>
<th>Risk Concept</th>
<th>Brief reason why concept should not belong</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis</td>
<td></td>
</tr>
<tr>
<td>Assessment</td>
<td></td>
</tr>
<tr>
<td>Calculate</td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td></td>
</tr>
<tr>
<td>Consequence</td>
<td></td>
</tr>
<tr>
<td>Culture</td>
<td></td>
</tr>
<tr>
<td>Decision</td>
<td></td>
</tr>
<tr>
<td>Evaluation</td>
<td></td>
</tr>
<tr>
<td>Loss</td>
<td></td>
</tr>
<tr>
<td>Risk management</td>
<td></td>
</tr>
<tr>
<td>Perception</td>
<td></td>
</tr>
<tr>
<td>Policy</td>
<td></td>
</tr>
<tr>
<td>Probability</td>
<td></td>
</tr>
<tr>
<td>Threat</td>
<td></td>
</tr>
</tbody>
</table>

Considering the above concept list of security risk management. Are there any other significant idea that you feel should be included? A pool of possible risk ideas are listed below for your assistance:

- Mitigation
- Prioritise
- Reduction
- Vulnerability

<table>
<thead>
<tr>
<th>Risk Concept</th>
<th>Brief reason why concept should be included</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Thank you for your time and assistance.
APPENDIX G
PHASE TWO: PSYCHOMETRIC MDS CONCEPT MAPPING SURVEY
INTRODUCTION LETTER

Insert date

SECURITY RISK MANAGEMENT CONCEPT MAPPING SURVEY

Dear name
Thank you for agreeing to complete the attached survey.

I am currently completing a PhD at Curtin University of Technology, to develop a concept map for security risk management. The study is using a mathematical process to present the consensual knowledge structure of security risk management.

As a security expert, it is requested that you spend approximately five minutes to complete the attached survey. The survey contains a number of questions, which seek to find how similar you consider some security risk management concepts may be. Please indicate with a mark, how related or unrelated you feel each item may be. An example is given below:

<table>
<thead>
<tr>
<th>Risk</th>
<th>when compared to</th>
<th>Threat</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>Highly related</th>
</tr>
</thead>
</table>

Answer each question from your initial feeling about that statement. Do not dwell on each question and please complete all questions. There are no wrong answers, as each term may have a different meaning to different people.

Participation in this survey will help to further the understanding of security risk management. You can contact me to discuss the study and its importance. You may also choose not to take part in the study or withdraw at any time. The study consists of this single survey, which is completed anonymously.

On completion, please fax the survey back to: 08 6304 5811

Your participation is greatly appreciated.

Regards, Dave Brooks
APPENDIX H

PHASE TWO: PSYCHOMETRIC MDS CONCEPT MAPPING SURVEY

Knowledge structure of security risk management

By completing the survey, I hereby give my consent to participate in the study to develop and define the knowledge structure of security risk management.

I understand that I can withdraw from the study any time.

<table>
<thead>
<tr>
<th>when compared to</th>
<th>Unrelated</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>Highly related</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis</td>
<td>Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis</td>
<td>Calculate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis</td>
<td>Communication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis</td>
<td>Consequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis</td>
<td>Culture</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis</td>
<td>Decision</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis</td>
<td>Evaluation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>when compared to</th>
<th>Unrelated</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>Highly related</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis</td>
<td>Loss</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis</td>
<td>Risk management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis</td>
<td>Perception</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis</td>
<td>Probability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis</td>
<td>Risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis</td>
<td>Threat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>when compared to</th>
<th>Unrelated</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>Highly related</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment</td>
<td>Calculate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessment</td>
<td>Communication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessment</td>
<td>Consequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessment</td>
<td>Culture</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessment</td>
<td>Decision</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessment</td>
<td>Evaluation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>when compared to</th>
<th>Unrelated</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>Highly related</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment</td>
<td>Risk management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessment</td>
<td>Perception</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessment</td>
<td>Probability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessment</td>
<td>Risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assessment</td>
<td>Threat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>when compared to</th>
<th>Unrelated</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>Highly related</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calculate</td>
<td>Communication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calculate</td>
<td>Consequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calculate</td>
<td>Culture</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calculate</td>
<td>Decision</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calculate</td>
<td>Evaluation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calculate</td>
<td>Loss</td>
<td>when compared to</td>
<td>Unrelated</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>-----------</td>
<td>------</td>
<td>-----------------</td>
<td>-----------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Calculate</td>
<td>Risk</td>
<td>management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calculate</td>
<td>Perception</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calculate</td>
<td>Probability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calculate</td>
<td>Risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Calculate</td>
<td>Threat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td>Consequence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td>Culture</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td>Decision</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td>Evaluation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td>Loss</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td>Risk</td>
<td>management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td>Perception</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td>Probability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td>Risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td>Threat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consequence</td>
<td>Culture</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consequence</td>
<td>Decision</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consequence</td>
<td>Evaluation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consequence</td>
<td>Loss</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consequence</td>
<td>Risk</td>
<td>management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consequence</td>
<td>Perception</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consequence</td>
<td>Probability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consequence</td>
<td>Risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consequence</td>
<td>Threat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Culture</td>
<td>Decision</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Culture</td>
<td>Evaluation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Culture</td>
<td>Loss</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Culture</td>
<td>Risk</td>
<td>management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Culture</td>
<td>Perception</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Culture</td>
<td>Probability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Culture</td>
<td>Risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Culture</td>
<td>Threat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decision</td>
<td>Evaluation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decision</td>
<td>Loss</td>
<td>Risk management</td>
<td>Perception</td>
<td>Probability</td>
<td>Risk</td>
<td>Threat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------</td>
<td>-----------------</td>
<td>------------</td>
<td>-------------</td>
<td>------</td>
<td>--------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluation</td>
<td>Loss</td>
<td>Risk management</td>
<td>Perception</td>
<td>Probability</td>
<td>Risk</td>
<td>Threat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluation</td>
<td>Risk</td>
<td>Risk management</td>
<td>Perception</td>
<td>Probability</td>
<td>Risk</td>
<td>Threat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluation</td>
<td>Perception</td>
<td>Perception</td>
<td>Perception</td>
<td>Probability</td>
<td>Risk</td>
<td>Threat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluation</td>
<td>Probability</td>
<td>Probability</td>
<td>Perception</td>
<td>Probability</td>
<td>Risk</td>
<td>Threat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluation</td>
<td>Risk</td>
<td>Risk</td>
<td>Perception</td>
<td>Probability</td>
<td>Risk</td>
<td>Threat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluation</td>
<td>Threat</td>
<td>Threat</td>
<td>Perception</td>
<td>Probability</td>
<td>Risk</td>
<td>Threat</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Thank you for your assistance
APPENDIX I
PHASE THREE: EXPERT INTERVIEW

INTRODUCTION
As an expert in security, your participation and time in this study is greatly appreciated.

Approximately one week ago you were given the following concept map of security risk management. The map shows how security risk management ideas may be linked and their possible relationships. [Explain the development of the map].

Today, I intend to ask you some questions regarding the concept map. These questions will begin with some general questions on the overall structure of the concept map, leading into more specific relationships between these ideas. Feel free to comment on what you consider are important issues at any time. We do not have to adhere to the order of the questions.

I intend to tape record our interview and once the tape is turned on, will request your permission. Data collected will remain confidential, you will not be identified and the only other people who will have access to the data will be my two academic supervisors.

INTERVIEW
[Tape ON] Can I request your verbal permission to tape record this interview?

Before we start, do you have any general questions regarding the study?

QUESTIONS
Q1. The concept map shows an overall structure for security risk management. Do you consider that this whole structure describes the ideas underlying risk?

Q2. On the concept map, do you consider if there are any inappropriately located ideas?

Q3. Do the think that the ideas represented in the security risk management concept map represents your thoughts on this topic?
Q4. From your knowledge of security risk management, are there any other *important* ideas that could be included?

Q5. Do you believe that this structure shows appropriate relationships in the ideas of security risk management?

Q6. On the concept map *threat* would appear to be a central theme, what are your comments regarding this?

Q7. Consider the ideas *risk, risk management, calculate/assessment, threat, loss and decision*. Do you think that this structure and/or links are justified? Why?

Q8. Consider the ideas *probability, consequence* and *analysis*. In your opinion, does this structure appear appropriate?

Q9. *Culture* and *perception* are clustered in close proximity to *threat*. What are your thoughts on this cluster?

Q10. Would you like to add or change any link (*explain link*)?
Q11. Would you like to add or change any linking label (*explain label*)?

Q12. Do you consider that this concept map provides a general consensual of security risk management ideas and their relationships?

Q13. Do you have any final comments?

END
Thank you for your time.
APPENDIX J

PHASE THREE: EXPERT INTERVIEW TRANSCRIPT

The following transcript was taken during the recorded interview of one of the six security experts, interviewed during Phase three of the primary study.

<table>
<thead>
<tr>
<th>Interview participant</th>
<th>Recorded comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interviewer</td>
<td>Start time: 1.45pm [19 July 2006] - Can I get your verbal permission to tape record this interview?</td>
</tr>
<tr>
<td>Expert 3</td>
<td>Yep</td>
</tr>
<tr>
<td>Interviewer</td>
<td>[Question 1] The map shows an overall structure for security risk management. Do you consider that this whole structure describes the ideas underlying security risk?</td>
</tr>
<tr>
<td>Expert 3</td>
<td>Yep</td>
</tr>
<tr>
<td>Interviewer</td>
<td>So all the concepts are covered within that map?</td>
</tr>
<tr>
<td>Expert 3</td>
<td>Yep</td>
</tr>
<tr>
<td>Interviewer</td>
<td>Yeh, to a certain extent, I think, for example, I guess if you look at why people would commit a crime in the first place, or if you’re looking at a threat say for example, break and entering, something like, then, you know, why are they doing that? Is there a reason behind it, do they have knowledge of an area where they’re going into? Do they have a knowledge of the systems that are in place, are they able to circumvent them. Do they have a desire to do it, to try, if it’s for cash or something like that, obviously there’s a desire there, they might need money. So I guess those types of principles which is probably delving down even a bit more into why people are committing those crimes, why they are doing those things. Is it for personal gain, is it for, very much to sustain a habit or something like that. So whilst I think it covers the main overlying principles of it, then there are other areas where you might be able to delve down even more.</td>
</tr>
<tr>
<td>Interviewer</td>
<td>[Question 2] On the map, do you consider if there are any inappropriately located ideas?</td>
</tr>
</tbody>
</table>
| Expert 3 | Em, just from quickly looking over it, I thought there should have been a link from assessment to your probability, consequence and analysis. So you’ve got a threat, you do your risk assessment and part of that assessment is looking at the probability and the consequence of those areas and then obviously analysing it to get a meaningful outcome to produce a treatment plan to try and mitigate those threats which you have. I thought there could be a link from assessment down to those areas there. Um, at the top threats are managed through risk management cause it’s got risk is managed through risk management. Em, and the only other real area was where your talking about loss I didn’t know if you meant whether there are any treatment options or treatment plans to mitigate that loss or where you just looking at, OK, this is what’s going to happen but not provide any further input as to how doing that from happening again. So where you’ve got your treatment plans, where you’ve got your options that a client may want to put in to mitigate those risks or transfer them or whatever they want, or just accept them. What we look at doing is basically writing down what the name threats are, looking at the level of risk associated with those and then providing a treatment plan of how they can lower or
reduce those, but obviously it’s the clients decision whether they want to accept those or not.

[Question 3] Do you think that the ideas represented in the security risk map represent your thoughts on this topic?

Expert 3

To a certain extent, yes. I said originally, though, I think, invariably you might be able to go down a bit further and look at, um, differing ideals or where perceptions come into play about what issues there are. If I went into a building I might look at things completely differently to the way you look at it. So it comes back to a lot of other things, like your background, knowledge of the area or knowledge of the operation of the building or operation of the facility. Um, to someone with a background in defence, going onto a defence sight may see completely different threats than someone without that background going on that sight. And then you look at their experience and knowledge that they have in that area as well can affect that, so although that covers it all, there’s all those, I guess, I don’t know whether you would call them a motive or just knowledge and experience of different areas. Everyone may come up with different ideas. So, from that point of view, unless you’re looking at using stats and things like that, it’s very subjective in that matter that it’s based upon your level of understanding or knowledge or information presents to you at that time.

[Question 4] From your knowledge of security risk, are there any other important ideas that could be included? In other words is there any significant idea missing from the overall map? i.e., any other concepts?

Expert 3

[Long pause] Apart from putting an option in there like your treatment plan and possibly looking at how your likelihood and consequences made up, so delving down into more depth why someone is committing that crime or why someone is committing that act. If it’s a threat against someone or something like that, so if someone is being verbally or physically abused by a person you know why they are doing that – is it the surroundings that they’re in, is it, going back it could probably be your principles, is it an inviting area or is it confronting to them are they becoming agitated, therefore is there level of risk being heightened because of that area and surrounding you’re in. Now I don’t know how you’d actually put that in to measure that for risk assessment.

[Question 5] Do you believe that this structure shows appropriate relationships in the ideas of security risk? I’ll skip question 5 and go straight on to question 6.

[Question 6] On the map threat would appear to be a central theme, what are your comments regarding this?

Expert 3

I agree. Em, every risk assessment is based on the threat so you do an assessment on the level of risk associated with that threat, so, whether that threat, I mean it could be anything from whether it’s a safety or security point of view, it could be an
armed hold up armed robbery or something like that, then obviously all the underlying principles around it are based on that, so although it’s not necessary for someone like Myers responsibility to do a threat assessment, we can do a threat identification and identify certain threats and then do a risk assessment based upon those threats, rather do an actual threat assessment itself and go on from there. So most definitely I think it is central point of all your risk assessments.

[Question 7] Consider the ideas risk, risk management, calculate/assessment, threat, loss and decision. Do you think that this (sequential) structure and/or links (are justified)?

[Long pause] If you looked at it from a flow point of view, like the top down flow approach, I’d have the threat at the top then you could look at your cultures and perceptions based on that threat and look at the assessment would be part of the risk management anyway really, so rather, I guess risk is managed through the risk management and the assessment goes into the threat, I’d probably look at the threat at the top then filter down into your risk management which would look at your assessment, calculating your likelihood and your consequence and all that kind of stuff down to a decision or before your decision that’s when I would look at my treatment plan and I guess ultimately it would be to help, if you look from a client’s perspective it would help the client make a decision. So all it is a decision-making tool so that they can make a decision what they are going to do to eliminate the likelihood of that threat occurring or the consequence or accept all the other areas there are, so I’ve got threat at the top rather than the risk, filter down, I guess go back to the other point is do you think threats the central theme of the whole thing. Does that make sense?

[Question 8] Consider the ideas probability, consequence and analysis cluster again. In your opinion, does this structure appear appropriate.

It says probability is measured with consequence, I don’t thing really that the probability can be measured by the consequence, you might have something which is a high consequence level but the probability may be low or very low or something like that, but I don’t think that you can really measure

Is that referring to is measured with, in other words, is that showing a direct relationship between the two or link

Yeh, I think there is a link between the two, I mean if you look at just the probability and not the consequence you might have but, a high probability is something from occurring but if there’s nil consequence there’s no real point. Where conversely if you’ve got something which is high consequence and low probability it may come out a medium level threat or medium level on your risk assessment and so there’s a direct relationship between the two and I think if you look at one without the other it would be a bit of a worry. You could look at something that might involve physical danger to a person, which is obviously a high consequence because you don’t want that to happen, but the probability may be very low, but if you don’t look at that then you can I guess get a carried away and say we’ve got all these problems and we need to do all these things when the likelihood of that probability of occurring may be very low which would reduce the level of risk anyway.

So you feel it’s quite appropriate that these two are clustered together.
Expert 3 Yes.

Interviewer [Question 9] Culture and perception are clustered in close proximity to threat. What are your thoughts on this cluster?

Expert 3 I think going back to what we were saying before, if you look at someone’s background and their perception that can have an influence on the threats that they may see. Say if you had a person from a culture where they may have, say for arguments sake look at someone from South Africa where there may be a lot of crime or danger on the streets when you’re driving around or even going to university where the guards have guns and things like that. If you come up in that culture then your perception of the threats would be different than someone from Australia. So someone from South Africa would come over to Australia and it’s like, there’s nothing wrong here, there’s no problems at all, compared to where there from, they’re looking at it from their culture so their perceptions would be based on their background, their knowledge, understanding all those type of things.

Interviewer [Question 10] Would you like to add or change any link, now link is primarily the lines between the concepts?

Expert 3 I think as I said before, I’d like to see a link between assessment which would, part of the assessment would include looking at your probability, your consequence and your analysis of that threat. Changing the top from risk to threat, threat is managed through risk management they require assessment and treatment plan at the loss that although that would indicate where the loss might occur then I think there might need to another one in there looking at any treatment plans to reduce them.

Interviewer [Question 11] Would you like to add or change any link in label? The label primarily being the word that gives the line some meaning.

Expert 3 [Long pause], No, I think they’re quite appropriate.

Interviewer [Question 12] Do you consider that this map provides a general consensual map of security risk management ideas and their relationships?

Expert 3 Yeh, I think it provides a general overview of the whole process. I guess it’s just the extent of how deep you want to go. Like if there is a general overview then do you want to break probability up, do you want to break communications up and culture. I suppose the levels that you could explode these entities you could call them too.

Interviewer [Question 13] Do you have any final comments?

Expert 3 The only thing I, this isn’t a criticism, the only thing I found it kind of jumbled, it didn’t seem to have I guess the logical flow, if that makes sense. Like if your looking at a decision tree or something like that where you have the yes or no and it branches out, they sort of have a logical flow, different type of assessment tool showing it, but it kind of seem to not flow if that makes sense

Interviewer Thanks very much XXXXX. Time ended 2.05 pm

END