Effective Information Assurance with Risk Management

By

Vassileios Andreas Dimopoulos

A thesis submitted to the University of Plymouth in partial fulfillment for the degree of

DOCTOR OF PHILOSOPHY

School of Computing, Communication & Electronics

January 2007

Effective Information Assurance with Risk Management

Vassileios Andreas Dimopoulos
BEng (Hons), MSc

Abstract

Today's businesses base their operation on their IT infrastructure, which consequently demands that it should be protected accordingly. Nevertheless, surveys tend to indicate that the number of IT security incidents is increasing, resulting in significant losses for the organisations concerned. Leading in poor security practices, and therefore frequent victims of related security incidents, are Small and Medium Enterprises (SMEs). Even though there are a number of solutions, ranging from baseline guidelines to a detailed Risk Assessment (which can be followed to guide organisations through systematically selecting appropriate controls and practices to properly secure their networked assets), evidence suggests that these are not being employed by SMEs. Constraints such as lack of budget, security personnel and awareness are amongst the factors that are deterring SMEs from adopting such solutions, and therefore contributing to their continued problem with security incidents.

This thesis specifically targets the problem of security risk assessment within SME environments. Following an examination of the aforementioned constraints, the investigation considers the existing solutions, establishing the reasons that they are not appropriate for SME users. The research identifies that SMEs are in need of a solution that represents a progression of current guidelines, but without being as complicated as existing forms of Risk Analysis. Therefore a new methodology is designed, known as PRAM (Profile-based Risk Analysis and Management), which enables SMEs to analyse and manage their risks in a way that is simple to use and understand, as well as providing economic considerations on threats, their likelihood, effect and the spending required to reduce them to an acceptable level.

The methodology is then implemented within a working prototype, which is evaluated using a series of test scenarios. These scenarios are also used as the basis for evaluating existing SME-oriented Risk Analysis solutions, and the findings determine that the PRAM approach is able to deliver a more comprehensive solution. In addition, an evaluation of the PRAM prototype by a series of end-users suggests that it also succeeds in providing a more user-friendly solution than the current alternatives.

Overall, this thesis presents a solution that can be adopted by SMEs lacking in-house security expertise. It can assist them in understanding the threats they are under, while at the same time presenting appropriate information to enable management to evaluate their organisation's current IT security situation and select appropriate countermeasures.

Acknowledgements

To enable me complete this research I acknowledge the financial contribution of the A.G. Leventis foundation that believed in me and offered me the scholarship which made it all possible.

I would like to thank my Director of Studies, Professor Steven Furnell whose motivation was the main contributor in me beginning this effort four years ago. Professor Furnell has shown great professionalism and has always been there for guidance and support throughout the duration of this research. I am also grateful to him for all the opportunities given to me in publishing papers, attending conferences, seminars and exhibitions that were relevant to my area of studies.

I also wish to thank my Supervisor, Dr Nathan Clarke for his effort in proof-reading and commenting upon my work as well as guiding me throughout this research no matter how busy his timetable might have been.

I also acknowledge the support of my parents and family, both moral as well as financial, and for always believing in me. More specifically I owe a great part of what I achieved over the past four years to my father Andreas, my mother Sofia, my uncle Alexander and grandmother Helen. I am grateful that these people had faith in me and my abilities and have always been by my side throughout my studies.

Great thanks go out to Fenia without whom none of this would have ever happened and my friends Marios, Andreas and Dimitris for their support and tolerance every time I visited the U.K. during the past two years.

Furthermore I would like to thank Artemis for her support over the past 1.5 year that I have been working on this project. Even though this has been the hardest period of the research she has shown notable understanding and was always there for me.

Finally I would like to dedicate all this work to my best friend Yiannis who I know was always proud of me for undertaking this PhD degree but did not live to see the end of it. Rest in peace my friend...

Authors Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award.

Relevant seminars and conferences were regularly attended at which work was often presented and several papers prepared for publication.

Signed V. Dimopoulos

Date 14-5-2007

Table of Contents

List of Figures

List of Tables

Glossary of Abbreviations

C-I-A:	Confidentiality, Integrity and Availability
COBiT:	Control Objectives for Information and related Technology
DTI:	Department of Trade and Industry
GUI:	Graphical User Interface
INFORM:	Information Assurance Risk Model
ISO:	International Standards Organisation
I.T.:	Information Technology
MRSAT:	Microsoft Security Risk Self-Assessment
NIST:	National Institute of Standards and Technology
OCTAVE:	Operationally Critical Threat, Asset, and Vulnerability Evaluation
PRAM:	Profile-based Risk Analysis and Management
RA:	Risk Assessment
RA2:	Art of Risk 2
SME:	Small and Medium Enterprise
VB:	Visual Basic

1 Introduction & Overview

This research presents a novel approach to Risk Assessment which can be implemented by Small and Medium Enterprises (SMEs) to assess the risks towards their assets and select appropriate controls to protect them, this way reducing the high levels of losses due to compromise of information security assets reported in surveys.

1.1 The problem of security risks for SMEs

"Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected" (ISO17799 2005).

Nowadays I.T. systems are essential and the vast majority of organisations have networks to facilitate their operations, transactions and business functions (Cisco 2006). This introduces a significant amount of information that exists within organisations in an electronic format (DTI 2005). Having based the operation on networked assets, what is even more challenging is maintaining the operational status of such a network, as any disruption of the flow of information or any occasion that one of the elements that constitute it becomes unavailable, may immediately mean loss of capital and reputation (Camp 2006).

Any part of an Information system (i.e. hardware, software, data) can be the target of an attack (Pfleeger 2006) and there are a large number of threats towards information assets that can lead to their compromise, but they can all be listed under five broad categories (DTI 2006). Those are:

- Malicious code, which includes Viruses, Trojans and Worms.
- Accidental damage, which among others can include hardware failure, faulty software, human errors and natural disasters.
- Staff misuse of Information Systems, which can be misuse of confidential information, web and email access.
- Unauthorised Outsider, such as attacks on internet or telecommunications traffic, attempts to break into and actual penetration into network.
- Theft of Fraud. For example, theft of computer systems or use of organisations systems to commit fraud.

It is common practice to every home not just within organisations to protect physical assets, such as currency or jewellery, from possible threats against them. People instinctively hide or protect such assets in safes and banks. Information is a very important asset (Buszta 2003) and should be secured like an organization would secure their physical assets since these two are nowadays almost completely interdependent (Hamilton 2002).

Information Security is commonly defined as being the protection of information within a business, and the systems and hardware used to store, process and transmit this information (Whitman 2003). This is achieved through the protection or preservation of three key aspects of information: availability, integrity and confidentiality (Shaurette 2003). According to Parker (1998): Protection of information availability means that information should be kept accessible and usable (for authorised parties) at any time. Preservation of integrity means that the unauthorised modification of information must always be prevented. Finally, safeguarding of confidentiality of information means that observation and disclosure of knowledge must be limited only to authorised individuals.

In the market there are a large number of solutions which, if implemented correctly, can eliminate the risk for all these threats (Lawlon 2003). However, organizations report major losses due to the compromise of security, meaning they are not assessing their security properly. Small and medium organisations generally experience common problems (Churchill 2006) and, as surveys point out, one of these is that they are leading in bad security practices while at the same time report a lot of the significant losses due to I.S. incidents (Jennex 2004).

A key step in securing is performing a Risk Assessment. In short, this means methodically identifying an organisations assets, the threats to those assets and selecting the best possible controls trying to be efficient in spending the budget (HKCERT 2005).

1.2 Aims and objectives of the research

This research investigates the need for and use of RA within SMEs, so as to establish why SMEs do not plan their security in a structured manner and are not adopting adequate security controls, and therefore, as a result continually face security incidents. This is achieved by investigating the available solutions to identify what elements make them unsuitable for SMEs and allow the design and implementation of a novel approach which addresses these identified issues.

To establish this, this research has been divided into the following five stages:

1. To establish the requirement for a method of structured asset-risk valuation and management (which is offered at its best by performing a Risk Assessment) for every organisation that wishes to effectively secure their I.T. assets.
2. Investigate whether such solutions are implemented within SMEs and analyse the characteristics of SMEs and their personnel which may be prohibiting their adoption.
3. Analyse and critique current solutions and evaluate them to discover what elements are prohibiting for the previously established distinctive SME environment.
4. Design a methodology based specifically on these identified needs of SMEs, making it free of all the prohibiting elements associated with existing solutions.
5. Implement this methodology into a prototype which will allow the testing of this novel framework so as to establish its effectiveness.

In order to achieve the first stage, a literature review is performed, providing an insight to the area of RA, its importance to organisations, how security is not thorough without having performed one, as well as proof that in real life it is not being adopted. This leads to the second stage where through the use of survey findings a set of requirements, which make RA solutions suitable, of SMEs from such solutions is established. In the third stage a detailed investigation of the available solutions, to SMEs wishing to plan their security in such a way, is performed. This investigation includes a rating of these solutions against the characteristics SMEs desire (as identified in the third stage) and from them establish the reasons that make them inappropriate. Having established what SMEs need and what makes current solutions inappropriate, allows the research to proceed to the next stage which is to design a novel methodology which surpasses the identified setbacks. Finally the novel methodology is used to produce a prototype which can be tested in SME scenarios and against the existing solutions to prove that the identified setbacks have been surpassed.

1.3 Thesis structure

Chapter 2 discusses the current problems faced in the I.S. sector and investigates what solutions are available for organisations wishing to overcome these problems. The discussion focuses upon Risk Assessment, which is widely recognised as the first step that organisations need perform towards a structured and systematic approach to I.S. After analysing the details of these solutions the focus is on survey data that points out they are not being implemented. The main industry sector that has the problem is shown to be Small and Medium Enterprises.

Having established there is an I.S. security problem and it concentrates on SMEs, the third chapter investigates the characteristics of SMEs that may prevent them from properly planning and organising their I.S. To achieve this, the deterring characteristics of SME security environments are identified through existing surveys and a survey conducted by the author establishes whether these initial assumptions stand. Identifying these characteristics enables this research to proceed and evaluate the existing solutions based on the requirements of SMEs and identify the reasons why they are not being adopted.

Chapter 4 includes the evaluation of the existing solutions available to SMEs, focusing upon selected RA tools that advertise themselves as being appropriate to SMEs. Then there is an investigation of the other solutions available to SMEs wishing to structure their security but cannot perform RA. This investigation establishes that none of these solutions is suitable for the characteristics of SMEs, which is why they are not being used, leading to poorly planned security and significant breaches and losses. This leads to the formulation of the requirements for a methodology that will match the requirements of SMEs therefore enable them to assess security properly.

The evaluation is based on three scenarios of SMEs (included in Appendix A), one of a home office, a small–sized business and one with a middle–sized organisation. For each one of these the business functions/characteristics and the security requirements were

devised and those characteristics of the tools that this research is concerned with (i.e. those that correspond to SMEs requirements) were rated.

Chapter 5 describes the methodology that has been considered and designed in order to address the identified requirements of SMEs from a RA framework that solves the existing problems in the area. In this chapter the elements that should be included by such a framework, such as the processes and the information inputs and outputs, are analysed.

Chapter 6 describes how the methodology was implemented into a working prototype. Profile–based Risk Analysis and Management (PRAM) uses background functionality and intelligence offered by spreadsheet, database and word processing software, all automated and handled by an easy to use profile-based interface programmed in Visual Basic, to produce a novel software tool which addresses all the identified requirements of SMEs.

Chapter 7 evaluates PRAM to assess whether it has achieved the desired goals for an SME RA tool. This is achieved by running the prototype with the three scenarios proposed in Chapter 4 and rating the performance on the same criteria as the other tools. This allows comparable results between PRAM and the existing solutions. The second approach selected to evaluate the prototype was to have 3rd party participants in a controlled environment evaluation compare and contrast the existing RA tools and this framework based on scenarios they devise.

Chapter 8 presents the conclusions, discusses certain limitations of the research, and presents future work that is required on the area of RA. The thesis concludes by considering the future outlook for Risk Analysis within SME environments.

2 SMEs and Security Planning Methodologies

This chapter identifies the existence and investigates the nature of the problem of SMEs having security issues and losses. The investigation considers the options available to organisations wishing to assess and minimize the information security incidents reported, and assesses whether these are being implemented, based on survey findings and a study of existing literature.

2.1 Introduction

Before starting to investigate the I.T. security problem this research will attempt to solve, some basic background information will be given on two topics that will be seen discussed largely throughout the thesis. This research focuses on SMEs and therefore it is worth beginning with giving a clear definition of which organisations are considered to fit within this category. In addition, a large segment of the discussion is based on survey findings and therefore some elementary information on the surveys mentioned in this thesis is provided at the start of this chapter.

2.2 What are SMEs

SME stands for Small and Medium Enterprises, and as explained in the introduction, this research focuses on SMEs as they face the same I.S. problems as all organisations but, as this chapter proves, usually lack the solutions. Different countries have a different perception of what an SME is. As an example, in Germany, organisations with under 500 employees were defined as medium (the same for the US) while in Belgium this category

only included organisations with under 100 employees (European Commission 2007). For the purposes of this research however the definition given by the European Union Commission as of the 1st of January 2005 (European Commission 2005) based on the criteria of the 'staff headcount' or on the annual turnover. According to this definition, SMEs are defined as those organisations that have less than 250 employees or have an annual turnover of less than 50 million Euros. In Europe, SMEs comprise approximately 99% of all firms and collectively employ around 65 million people (European Commission 2007).

Enterprise category	Headcount	Turnover	or	Balance sheet total
Medium-sized	< 250	≤ € 50 million		≤ € 43 million
Small	< 50	≤ € 10 million		≤ € 10 million

Table 1: Definition of SMEs by the EC

From now on when the term SME is referred to in this thesis, it will be consistent with the UK Department of Trade and Industry (DTI), which follows the EU description of SMEs portrayed above, and defines it as an organisation with fewer than 250 members of staff.

2.3 The surveys used in this thesis

Even though a number of documents are referenced throughout this thesis, what was chosen to be primarily the basis of the discussion were various I.S. surveys, this way illustrating results that are not assumptions but have statistical basis. An investigation

was made and appropriate surveys were chosen based on several criteria which are discussed in this section. These surveys results are discussed throughout the thesis therefore at this stage some information on those surveys is presented altogether, with some special focus on a survey that was conducted by the author focusing on SME I.S. issues more specifically for the purposes of this research.

- **The 2006 Information Security and Breaches Survey or ISBS** (DTI 2006). This survey is conducted by the Department of Trade and Industry every two years. ISBS 2006 is the latest of the series and its results are discussed widely in this thesis as it corresponds to the purposes of this research for several reasons: firstly it is a survey of the practices and problems of UK based organisations, and secondly it is the most appropriate of all the widely distributed surveys to represent SMEs (i.e. organisations with up to 250 employees) whilst having a quite credible number of samples (over 1000 organisations). The breakdown of respondent organisations is shown in Figure 1.

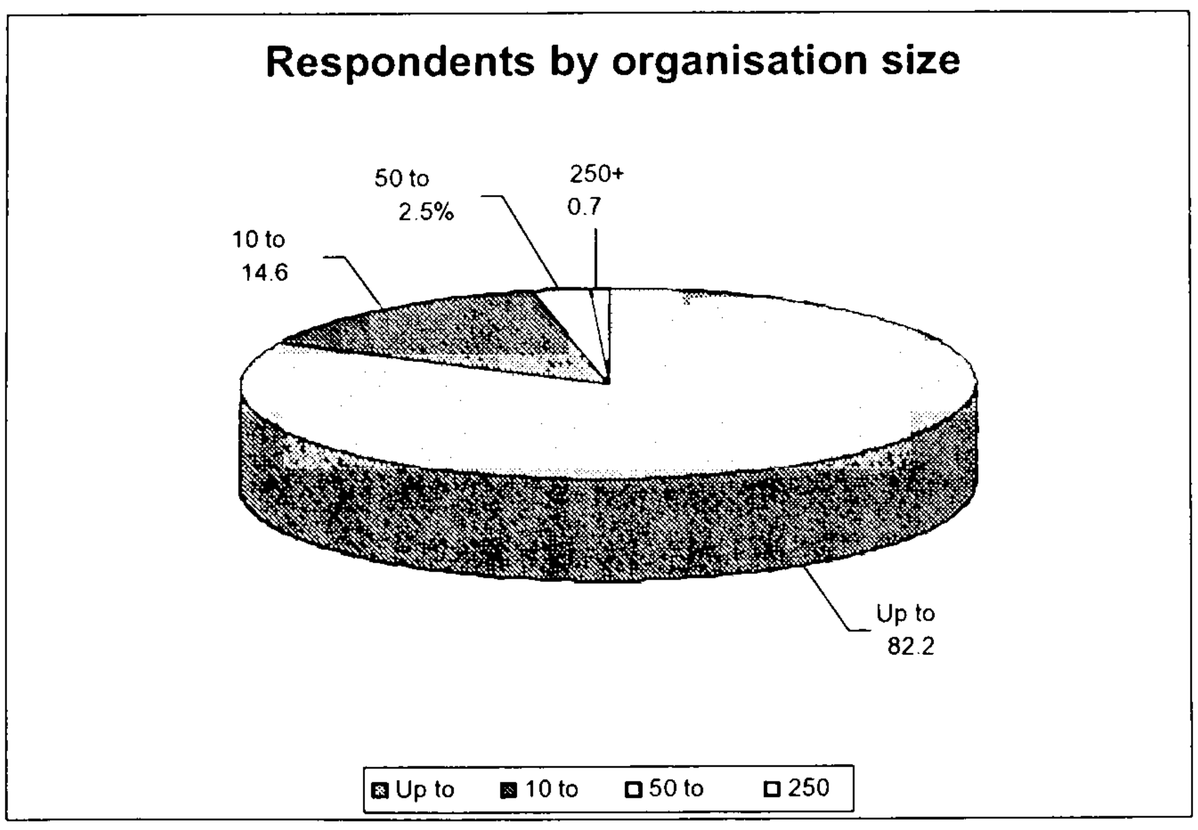


Figure 1: Respondents to the ISBS survey by size of organisation

- **The 2004 SME security survey** (Dimopoulos et al. 2004a)**.** The SME security survey was conducted in both Europe (mainly the UK) and the US, by the University of Plymouth and San Diego State University respectively, in order to compare organisations' attitude towards security. The US version (and the first section of the European survey) is concerned with security practices within SMEs, security expertise within, and the adoption of standards. This survey is described in more detail in Chapter 3. The findings of the two surveys were published in November 2004 and both survey questionnaires are included in Appendix B.

- **The 2006 Australian Computer Crime and Security Survey** (ACCSS 2006). An annual survey conducted with the large involvement of the Australian police, the AusCERT and the Australian government. It was chosen because it represents, As Figure 2 shows, a very wide spectrum of industry sectors and involves a credible number of samples (389 organisations). This survey does not focus specifically on SMEs but it does have a large sample from that business area, with 53% of the respondents employing less than 500 employees.

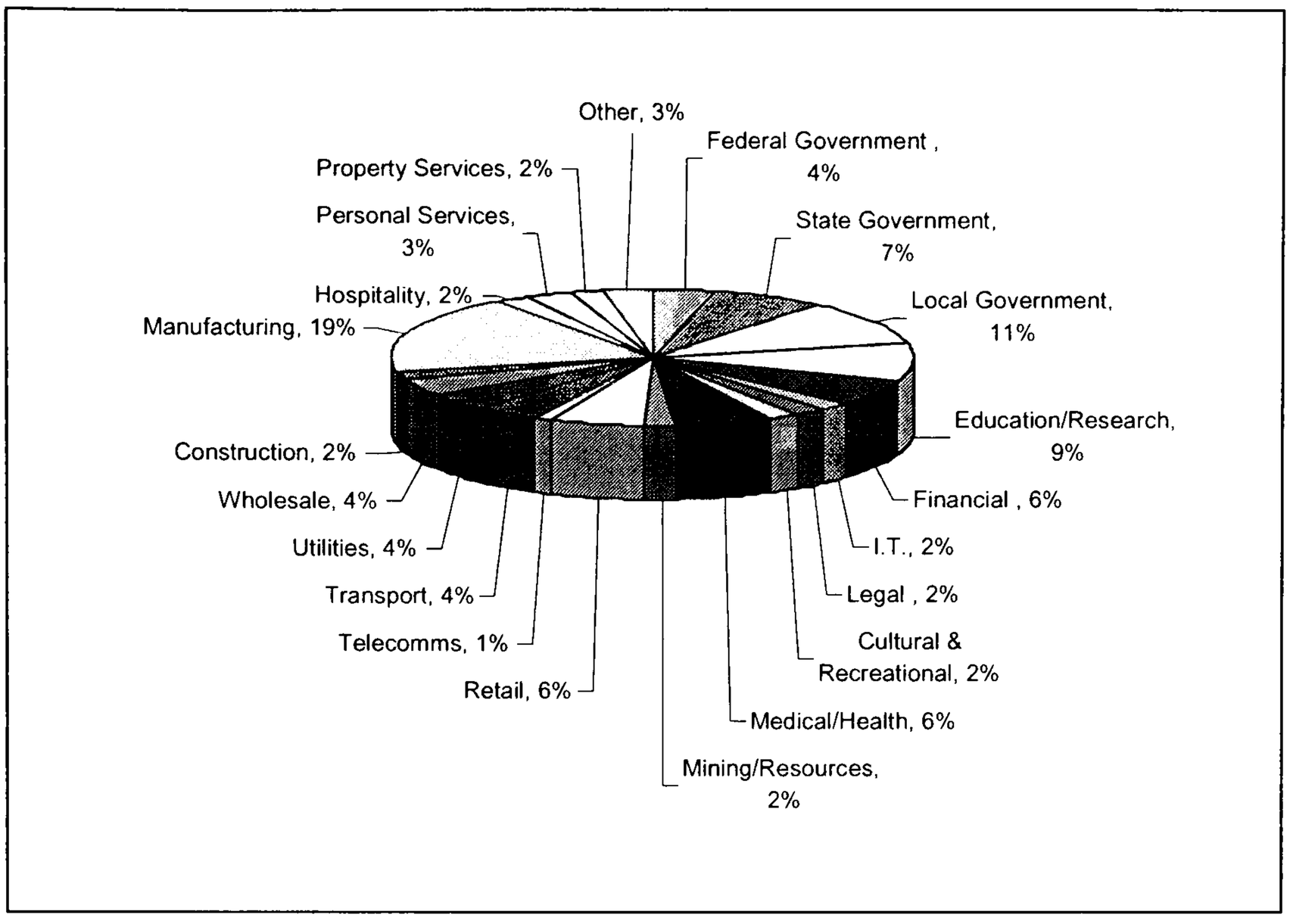


Figure 2: Respondents to the ACCSS survey by industry sector

- **The 2006 CSI/FBI Computer Crime and Security Survey** (Gordon et al. 2006)**.** This is the 11th version of one of the most widely known and referenced annual surveys on computer crime and security, which was the reason it was chosen for inclusion in this research. As the name implies, it is conducted in the USA by the Computer Security Institute with the participation of the Federal Bureau of Investigation's Computer Intrusion Squad. Like the previous survey the CSI/FBI survey includes a very wide sample in terms of the industry sectors it covers. Furthermore the size of the sample used for the findings of this survey is 615 respondents. As far as the size of the organisations involved is concerned, it generally aims more at large organisations (with 63% of the sample having over 500 personnel). However, this survey was included as it is used to discuss attack

trends and threats which are common towards all organisations and not security practices which may vary between SMEs and large organisations.

- **The 2005 Global Information Security Survey** (Ernst & Young 2005)**.** This survey is conducted by Ernst & Young and provides results from a global sample of organisations (1300 companies from 55 countries participated). Even though it does not address SMEs in particular, it does separate the results of organisations with an annual profit of over and under one billion dollars. When discussing results of this survey, the latter ones were used as being the nearest to SMEs. This survey was chosen as it discusses risk assessment and organisations requirements from it. The survey also discusses compliance with regulations and guidelines, which is interesting for the purposes of this research.

- **The Symantec Internet Security Threat report, volume VIII** (Symantec 2006)**.** This survey is issued annually by one of the leading vendors in I.T. security. It discusses the status of I.T. threats and attack trends. It was chosen as it is the most representative and accurate survey on the issue of threats the organisations face and industry sectors targeted, including a massive data sample. It bases findings on more than 24,000 sensors, monitoring network activity in over 180 countries, making it one of the most statistically reliable surveys.

- **The 2005 Global Security Survey** (Deloitte 2005)**.** Another global survey, conducted by Deloitte Touche Tohmatsu (or DTT), based on discussions with

representatives from the world's top firms. Even though this survey does not represent SMEs at all, it was chosen for some of the discussions in this thesis as it focuses on the business and financial aspect of I.T. risks and views I.S. from a managerial perspective, which is useful for when looking at what the management requires as the output of a risks assessment and looking at the financial aspects of RA and investments in security.

- **The 2005 Global State of Information Security Survey** (Berinato 2005)**.** This survey was performed by PricewaterhouseCoopers and the CIO magazine. It is interesting for the purposes of this research as it has a very large sample (8,200) of respondents from 63 countries that are all managers and directors in their organisations. It therefore illustrates the non-I.T. views on I.S. threats and practices, which constitutes a very significant element with RA.

2.4 The Information Security environment today

Every year more organisations become networked and depend on I.T. to conduct business, advertise, and interact with business partners and customers (GAO 2001). Nowadays most of the business can be performed online via organisations websites, from acquiring goods to paying bills, to filling in tax returns even voting (Labuschagne 2000). It is therefore surprising to find out that, according to the 2006 CSI/FBI report (Gordon et al. 2006), 95% of the organisations that responded (a total of 258 organisations) have experienced 'More than 10' website incidents.

However, it is not just the websites that are targeted and face security incidents, as the Department of Trade Industry reports in their latest security survey (DTI 2006), organisations are having security incidents in all areas of their I.T. infrastructure. To illustrate this, according to the aforementioned survey, in 2006 a rather large 62% of the overall organisations that responded reported they had a security incident of some sort.

Although one could argue that the large reported numbers of security incidents might be insignificant and unsuccessful incidents, the same report comes to add that: '*Overall, the cost of security breaches to UK plc is up by roughly 50% since two years ago, and is of the order of ten billion pounds per annum.*' while at the same time, in the US, CSI/FBI reports total losses within the previous year (2005) of 130 million dollars over 639 respondents with the greatest causes of loss being by far; malicious code ($43 million), unauthorised access ($31 million), and theft of proprietary information ($31 million). All three are quite severe threats (as one can judge from their effect) and more importantly cannot be characterised as accidental. Instead all three can be blamed upon negligence, poor selection of controls, lack of awareness and a variety of other avoidable reasons.

2.4.1 The lack of structured security

All these reported incidents and losses signify that there are gaps in the way organisations approach and assess their I.T. security. One would wonder however, if I.T. is so important to the organisations, and the nature of threats are more or less known, then why do incidents continue to occur? The answer is that organisations do not assess their I.T. in a correct and organised manner. There is no plan and they rarely assess assets and threats

properly (Upfold et al. 2005). Few are aware of guidelines and even fewer have formal documented policies and response plans without which *"an information system is likely to be a disjoint collection of countermeasures that address a variety of threats"* (Schneier 2000). The more one looks at survey data the more this view is strengthened:

- The author's SME security survey (described in full as part of Chapter 3) queried whether the respondents' organisations have a documented security plan or policy. In both continents the majority of the respondents stated they did not while, as Figure 3 illustrates, the smaller the organisation, the smaller the percentage that responded they have a plan.

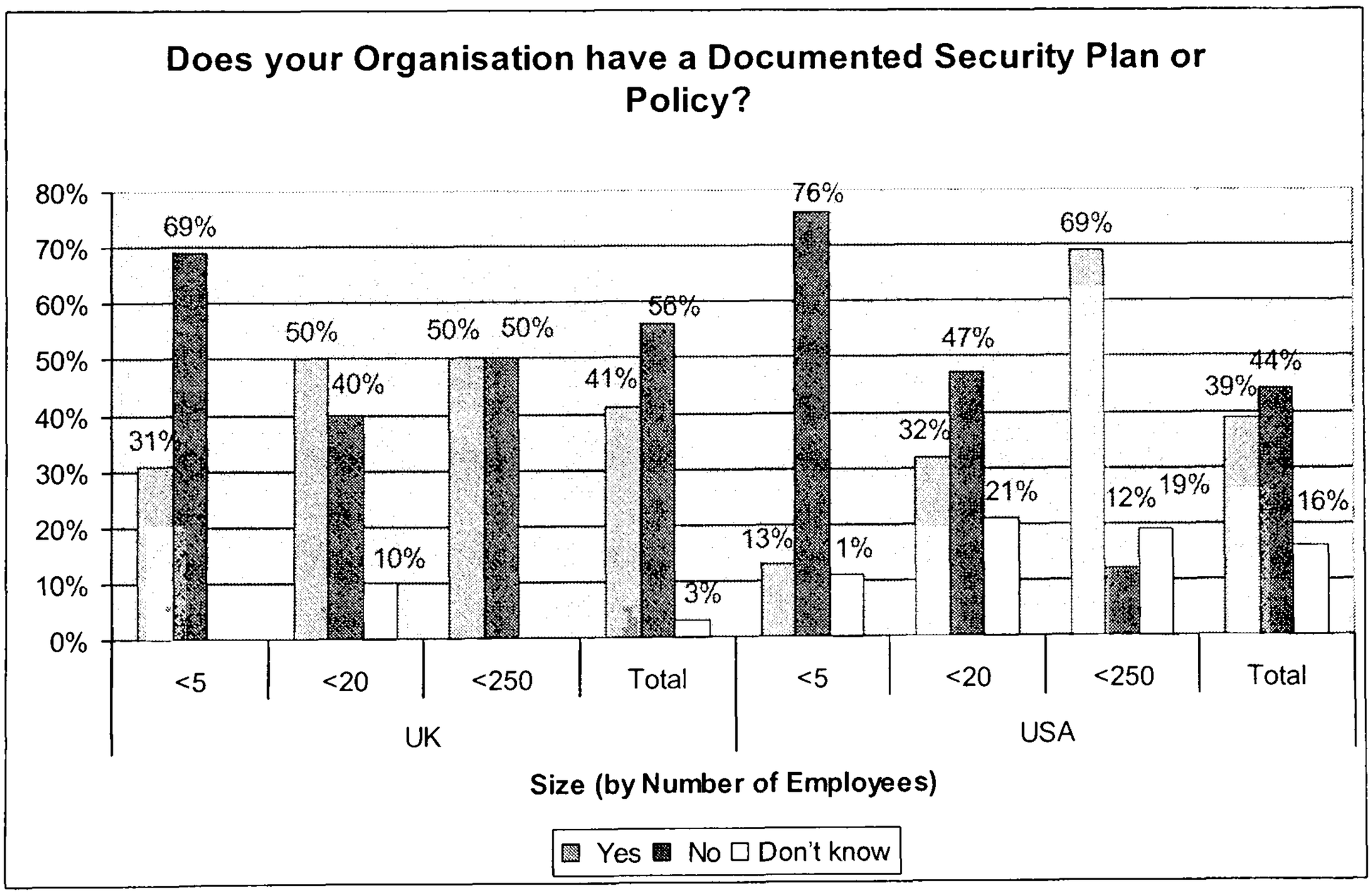


Figure 3: Findings of the SME security survey on the use of Plan and Policy

- The latest Australian Computer Crime and Security Survey queried whether respondents were guided by or followed any I.T. security standards, with only 47% responding positively.
- According to the DTI survey, the overall number of UK businesses that have a formally documented and defined information security policy is 40% which, when considering that the same number for large businesses is 73%, indicates that the vast majority of small and medium organisations do not take any action on this important issue.
- Numbers are equally low in the DTI survey when asking organisations about the methods they use to make staff aware of their I.S. responsibilities (introducing therefore even more risks such as social engineering, material for 'dumpster diving' and more (Granger 2001)). Apparently, one in eight organisations does nothing to educate their staff about their security responsibilities (e.g. only 38% use a staff handbook for this purpose).

However, as stated by Spinnelis et al (1999): *'One cannot reasonably develop security policies and procedures without clearly understanding the systems that must be protected and how valuable they are to the enterprise'.* This indicates that thorough security cannot be achieved by simply purchasing and implementing random controls and that a structured analysis of the system in need of protection is first required which will derive the essential controls.

Even when looking at the selected controls one can tell that there is something wrong in the way organisations plan their security. The DTI survey indicates that, in 2006 alone, 59% of the respondents have introduced wireless networks within their I.T. environment. Even though security is identified as the biggest liability of wireless networks (Briere 2003), one in five of these remain completely unprotected (it is again SMEs that significantly reduce the percentages, since 86% of large organizations stated they use encryption). CSI/FBI indicates that only 32% of organizations use 'specialised wireless security tools'. The same survey has found antivirus (97%) and firewalls (98%) are by far the most commonly used security technologies (and most other surveys agree to that). However when looking at the threats mentioned earlier, as those that have caused the biggest losses last year, they are exactly those that correspond to these controls (i.e. virus is the biggest and unauthorised access to information comes second).

2.4.2 Problem is focused on SMEs

One other thing that can be observed from all of these survey results is that the problem is concentrated among SMEs. According to the DTI survey findings, the total cost of security incidents in the overall sample (which mainly consists of SMEs) has increased in 2006 by as much as 50%. At the same time the survey reports that in large businesses the same figure has dropped by 50%. The same applies for the average cost per incident, which for the overall sample has risen by 20% since 2004. By contrast this has dropped 10% for large businesses, as illustrated in Table 2. Contrasting these figures it is clear that the I.S. problem is largely concentrated in SMEs.

	Overall	Large Businesses
Average number of incidents	+50%	-30%
Average cost per incident	+20%	-10%
Total Cost of incidents	+50%	-50%

Table 2: How the overall cost of security incidents to UK plc has changed since 2004

To complement the previous reference to survey data on the poor approach of SMEs towards security, the Symantec Threat Report VIII indicates that when talking about attack activity by industry (successful attacks), small businesses come first with 38%, while as far as 'targeted attacks by industry' is concerned, small business comes second behind education. The same survey states that *'Small businesses are less likely to have a well established security infrastructure, making them more vulnerable to attacks'* while at the same time small business personnel is known have an "It would not happen to me" mentality (Diamond 2004). This is why this research is going to concentrate on SMEs. SMEs are reported as successful attack targets the most, they have significant losses due to information security breaches (BBC 2004), the average reported loss from each incident according to DTI was £8,000 to £17,000 (with the percentage of large businesses that responded being 0.7% this amount mainly reflects SMEs), while due to their size SMEs are probably the ones that are harder to 'bounce-back' after a successful attack, and also they are the ones with the poorest approach towards information security according to all surveys. Finally, large organisations are more likely to have response plans and personnel that is particularly responsible for security making the recovery from a security incident faster and less costly. Therefore we are going to investigate whether

SMEs do have a poor security infrastructure and then investigate the reasons behind that and suggest a new solution that fits their needs.

2.4.3 Existing Solutions

Since the problem is identified to originate from the lack or incorrect planning of security, there are certain methods an organisation can use to create a well-thought plan and approach security in a structured manner. These will be described in the following parts of this chapter. What will be discussed first however is the most widely recognised option that organisations have and that is performing a Risk Assessment.

According to the International Standard Code of Practice for Information Security management (ISO17799 2005), the first source for an organisation to identify its security requirements is derived from '*assessing risks to the organization. Through risk assessment threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated'*

It is widely recognised that *"institutions should have a sound information security program that identifies, measures, monitors, and manages potential risk exposure. Fundamental to an effective information security program is ongoing risk assessment of threats and vulnerabilities surrounding networked and/or Internet systems."* (FDIC 1999). The process of Risk Assessment is strongly suggested by almost all government organisations, guidelines and standards as the first step for an organisation towards achieving thorough information security. In the US, *"The Office of Management and*

Budget (OMB), as part of Circular A-130, Appendix III, "Security of Federal Automated Information Resources," requires federal agencies to consider risk when deciding what security controls to implement. It states that a risk-based approach is required to determine adequate security, and it encourages agencies to consider major risk factors, such as the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards." (GAO 1999), Furthermore, in Australia, *"The government security policy requires departments to manage security risks"* (C.S.E. 1996).

The next section describes what risk assessment involves and how it can be approached. However, it will also demonstrate organisations have a poor approach to all the issues related to risk assessment.

2.5 Information Security Risk Assessment

A key step in establishing appropriate security for a system is to properly assess the risks to which it is exposed. Without having done this, an organisation cannot be sure to have an appropriate appreciation of the threats and vulnerabilities facing its assets (Noakes 2003). As such, questions could be raised over the suitability and sufficiency of security countermeasures that they may have introduced (e.g. are they actually providing the protection that the organization requires, and to an adequate level?). A way to accomplish this is by conducting a Risk Assessment. By definition, *'Risk assessment is systematic consideration of: a) The business harm likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of*

the information and other assets; b) The realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented.' (ISO17799 2005). The process of Risk assessment can be split into two distinct processes, as described bellow:

2.5.1 Risk Analysis

The process of Risk Analysis is defined as "the assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence" (ISO17799 2005), and involves steps such as the identification of assets that need to be protected and the identification of threats and vulnerabilities related to those assets (Network Working Group 1997). The process includes gathering information about the assets of the organization, including all company assets such as networks, data centres, computers, hardware, software, data/information; as well as human resources assets, such as the personnel who work for the organisation, the network users, and finally the physical assets like the physical facility and other physical organisational resources (HKCERT 2005). In addition, the risk assessment process includes finding sources for comprehensive threat data, which may be gathered from internal sources such as incident report data, intrusion detection software and/or threat data such as crime statistics, industry standards and benchmarking data, and historical data about what has happened in the organization previously.

2.5.2 Risk management

After the completion of risk analysis comes the process of risk management, which involves the identification, selection and implementation of countermeasures that are designed to reduce the identified levels of risk to acceptable levels, this way controlling, minimizing and potentially eliminating the acknowledged security risks, at an acceptable cost (ISO17799 2005). Risk management is therefore very much a matter of compromise between what is desirable, what is workable, and what is affordable. It involves both technical skill, a good knowledge of the business and its work-force, and good judgement (Intosai 1997).

2.5.3 How risk assessment works

Figure 4 summarizes the five main elements that need to be taken into account when performing Risk Assessment (Hamilton 2003; Pfleeger 2006). This section attempts to clarify what each of these involves.

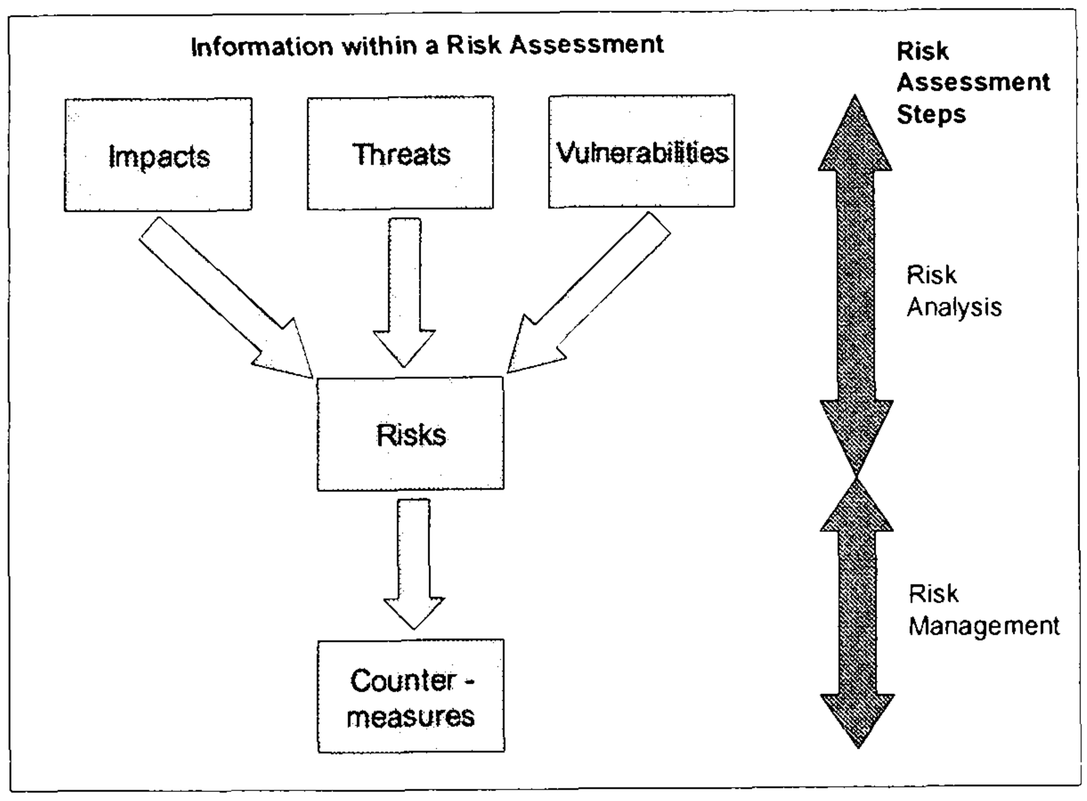


Figure 4: The Risk Assessment process

1. Identify **assets**. An asset is anything that is of value to an organisation. Thus it can be anything from physical assets to information assets, even specialised personnel can sometimes be considered as assets to the organisation. In this section a risk assessment methodology might require the user's input to rate the importance of the assets.

2. Identify and characterise **threats.** Generally speaking, threats are events that could occur and cause loss or damage to the assets that have been identified. Thus they should be completely eliminated, or the likelihood of their occurrence needs to be reduced, or finally their impact should be mitigated as even the most rigid security controls cannot eliminate every threat. Impact of threats to the organisation can be based on the importance of the assets that might be compromised because of the threat.

3. Identify **vulnerabilities.** Vulnerabilities are weaknesses that would create a condition allowing the threat to materialise and trigger a loss of assets. This stage of the Risk Assessment attempts to determine how vulnerable the systems are to the identified threats.

4. Analyze the **risks** for a certain asset-threat-vulnerability scenario to occur and determine the potential **losses** that would emerge if it does. Loss categories include direct loss, disclosure losses, loss of data integrity, losses due to data modification, losses due to delays and denials of service and more.

5. Identify and select **countermeasures** to reduce risks**.** Countermeasures are security controls which, when put in place, can eliminate, reduce or mitigate the impact of a threat occurrence.

The points just described are the five traditional steps when performing a risk assessment. To complete the process, organisations also need to:

6 Document the outputs of the assessment in order to create an organisational security policy.

7 Using information from an information system activity review, track results of controls, monitor changes in the environment, information systems, and security technology, update the risk analysis and implement any further controls that are identified as missing (Amatayakul 2003).

2.5.4 Collecting the Data

Based on the process just described, whatever the approach taken to risk management, there is always the common initial need for the person or team conducting the risk assessment to collect system-related information. Some examples of what this information may be are displayed in Table 3, listing an illustrative selection of assets as identified in N.I.S.T. SP-800-30 (Stoneburner et al 2002) and ISO 17799 (ISO17799 2005).

Asset Type	Examples/Description
Computer equipment	Processors, monitors, laptops, modems
Software Assets	Application software, system software, development tools and utilities
System interfaces	Internal and external connectivity
Data and information Assets	Databases and data files, system documentation, user manuals, training material, operational or support procedures, archived information;
Personnel who support and use the I.T. system	Can be employees or off-site contractors that require low-level access to the systems like security guards
System mission	The processes performed by the I.T. system
System and data criticality	The system's value or importance to an organization
Users of the system	Can either be system users who provide technical support to the I.T. system or application users who use the I.T. system to perform business functions
System security policies governing the I.T. system	Organizational policies, federal requirements, laws, industry practices
Current network topology	Network diagram
Flow of information pertaining to the I.T. system	System interfaces, system input and output flowchart
Technical controls used for the I.T. system	Security product that supports identification and authentication, discretionary or mandatory access control, audit, residual information protection, encryption methods
Operational controls used for the I.T. system	Personnel security, backup, contingency
Physical security environment of the I.T. system	Facility security, data center policies
Environmental security implemented for the I.T. system processing environment	Controls for humidity, water, power, pollution, temperature, and chemicals

Table 3: Examples of assets identified when performing a RA

Successfully collecting this data is one of the most important elements of Risk Analysis and a person that is not specialised in practising RA could easily overlook many of these elements or fail to identify their importance to the organisations operation. RA is a process intended to be performed by security analysts who have complete understanding of the I.T. system's operation and objectives (Gray 2005), thus being performed by an inexperienced user may lead to an inaccurate analysis of the organisations assets. This is also the reason why RA usually involves the input of not just one but several key personnel in different positions and with different knowledge of the organisation. There are several methods to perform the information gathering, but the most common as listed by the N.I.S.T. Risk Management Guide for I.T. Systems (Stoneburner et al 2002) is using a combination of the following:

- The use of **questionnaires.** This process requires applicable technical and management personnel to fill questionnaires created by the people performing the assessment and which mainly concerns the design and management of the I.T. system under assessment.
- Performing **on-site interviews.** Such interviews of I.T. and management personnel, conducted by the people performing the RA, should be performed to allow the RA team to gather information about how the I.T. system is operated. During these interviews the RA people can also make observations on the physical security environment related with the I.T. system.
- Conducting a **document review.** By reviewing all the security and policy related documents that exist within the organisation, the RA people can gather

information regarding system and data criticality and sensitivity as well as the security controls planned and used within the organisations I.T. infrastructure.

- Use of an **Automated Scanning Tool.** While no automated tool exists that can perform the RA without the need of human input, the people performing the RA can use automated tools like network mapping tools to obtain the related information more rapidly.

As one can infer from this list, not only is some certain expertise on the area of RA required but also a considerable amount of time in order to perform these operations.

2.5.5 Approaches to Risk Assessment

After the asset data has been collected, there is the need to measure their value, the likelihood of a risk occurring and other key elements. There are essentially two major approaches used to achieve this in modern risk analysis, the qualitative and the quantitative analysis. However certain papers mention a third approach, the ranking method. The quantitative and the qualitative approach that are best described by Wallhoff (2002), Intosai (1997), (Lawlor 2003) and Amatayakul (2003) with the latter also covering, the ranking approach.

2.5.5.1 The Qualitative Approach

This type of approach can be described as a walk-through different scenarios of risk possibilities followed by the rating of significance of the threats and the sensitivity of the

assets. This approach uses words or descriptive scales (e.g. low, medium, high) to describe the magnitude of potential consequences and the likelihood of these consequences occurring (Lawlor 2003). Qualitative methods are based upon scoring questionnaires that have been designed to assess the likely levels of a range of threats and their associated vulnerabilities. When performing this type of risk analysis, the common procedure is as follows (Wallhoff 2002):

- a team that performs the RA is required to write a scenario that addresses each major threat;
- these scenarios are then reviewed by business unit managers, whose responsibility is to weigh up how realistic they are;
- the team that performs the RA recommends and evaluates the various countermeasures that correspond to each threat;
- the team that performs the RA works through each finalized scenario using a threat, asset and countermeasure;
- Finally the team prepares their resulting report and submits it to the management.

In common with any questionnaire-driven approach, the relevance of some of the questions will vary according to circumstances, while the questionnaire itself may not be sufficiently comprehensive or relevant in unusual situations. This means that the reviewer may need to adjust the questionnaire's standards markings, and this could introduce a risk of distortion in the method (Intosai 1997).

2.5.5.2 The Quantitative Approach

This approach attempts to assign actual numbers to the amount of damage that can take place as well as the cost of countermeasures and when determining the likelihood of threats and risks it usually provides probability percentages (Lawlor 2003). Purely quantitative risk analysis is sometimes characterised as not possible as the method is attempting to quantify qualitative items (Wallhoff 2002).

A quantitative risk analysis attempts to assign monetary values to the potential losses that might occur as a result of a threat exploiting a certain vulnerability (i.e. requires that information assets be valued by some sort of common standard). There are typically three elements that determine the value of an information asset:

- Initial and ongoing cost of purchasing, licensing, developing, and supporting the information asset;
- Value of the information asset to the organization's operations, research, and business model viability;
- The value of the asset is established together with additional elements like the estimated value of intellectual property, such as trade secrets, patents, or copyrights (Amatayakul 2003).

Quantitative methods aim to balance the costs of implementing security against the possible cost of failing to implement it (which is a similar element to a Return on Investment metric, which will be discussed in Chapter 5). A problem with this approach

is that, to be effective, a comprehensive history of security incidents and their related impacts is required, but measuring impacts in financial terms may not necessarily always be realistic (Intosai 1997). If this does not exist, the calculations have to be based on the experience of similar organisations, but this may not always be representative or even available.

2.5.5.3 The Ranking Approach

The ranking approach may be more encouraging to budgeting than, for example, a qualitative approach alone. In a ranking approach, each vulnerability/threat pair can be rated as high-medium-low on a probability scale and a criticality scale. Together the ratings combine scores that can be used to prioritise the risks and therefore identify where the organisation's security needs to concentrate (Amatayakul 2003).

Figure 5 summarises the main points of each of the three available approaches that an organisation can make on risk assessment.

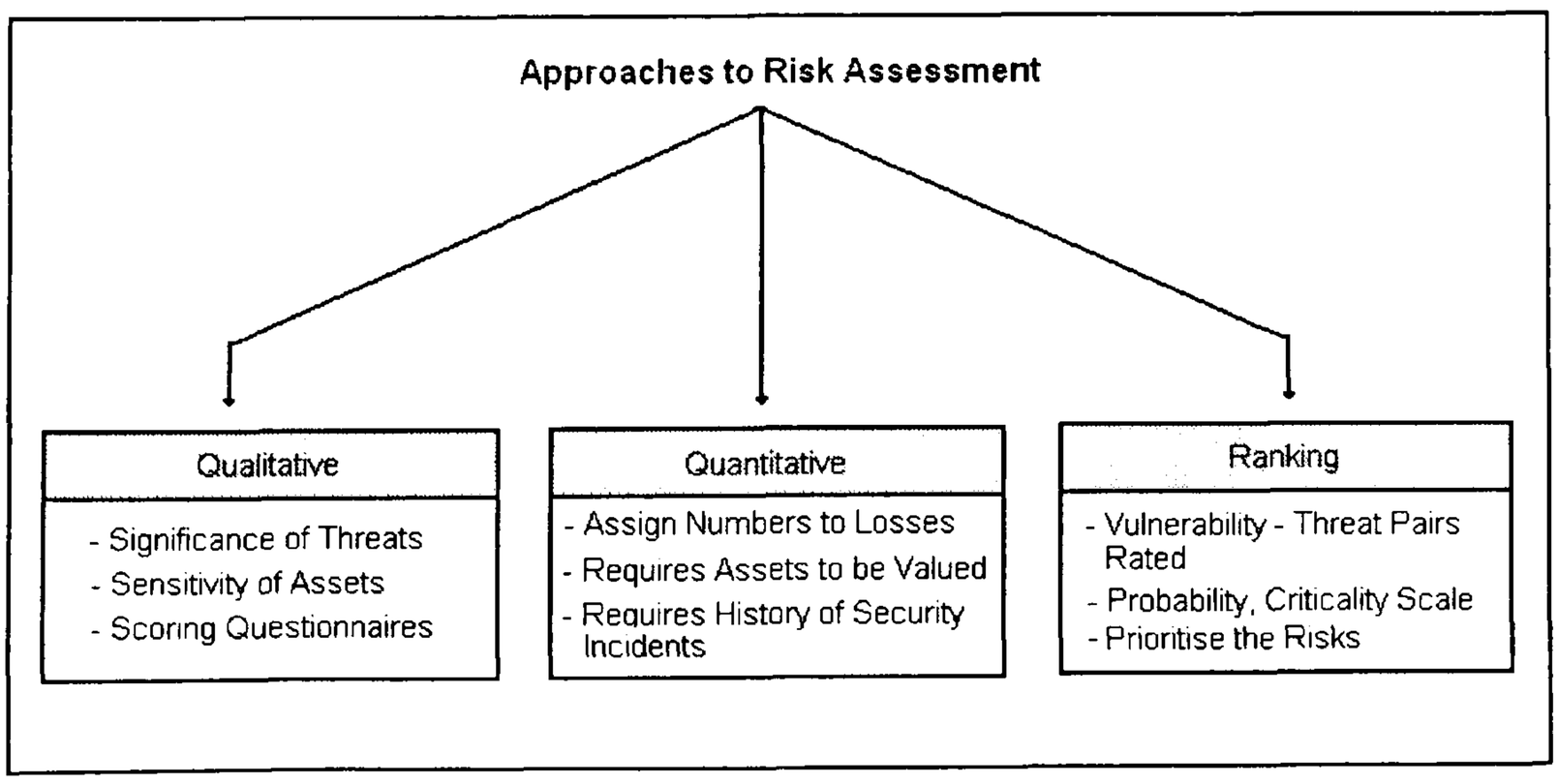


Figure 5: Approaches to Risk Assessment

2.5.6 Do Organisations perform RA?

Having identified the importance of performing a RA, looking at survey data we realise that many organisations do not perform it.

The DTI has queried respondents about whether they perform risk assessments, the report comments that: *"Many UK businesses are a long way from having a security-aware culture. Security expenditure is either low or not targeted at key risks. To justify expenditure and spend effectively, businesses need to carry out security risk assessments. However, only 44% of companies have done this in the last year."* It should be noted that this is 44% of the overall respondents. Thus, if this figure follows the trend of the other results previously examined then SMEs should fall well behind from this number. The author's SME security survey has specifically investigated whether SMEs perform RA, the results, illustrated in Figure 6, show that the larger proportion (60% of organisations asked) do not.

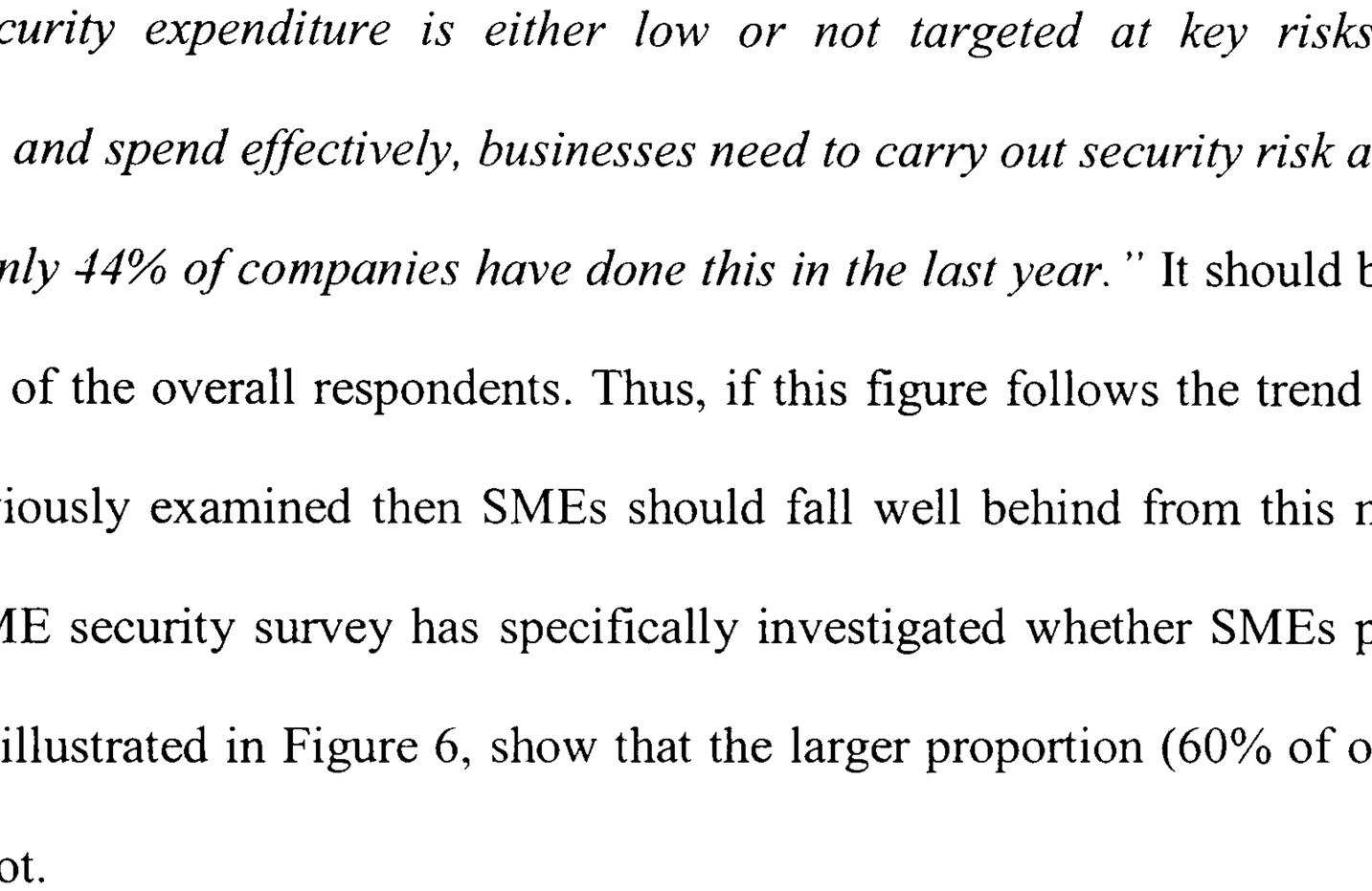


Figure 6: Do SMEs perform RA?

2.5.7 The characteristics of a typical RA tool

The common way to perform a RA is by the use of one of the commercially available specialised RA tools. The principle of how the RA is approached is usually the same as what has been described in section 2.5.5, however where they mainly differ is in the way the tools gather the information. This section will give some details on RA tools, focusing on the most widely recognised of all, CRAMM. CRAMM is a qualitative risk analysis and management tool that was initially developed in the United Kingdom by the Central Computer and Telecommunication Agency (CCTA) and is nowadays developed by Insight Consultancy owned by Siemens (CRAMM 2006). The most recent version is CRAMM 5.1.

The reason why CRAMM is going to be discussed as an illustrative example of RA tools here is because CRAMM is a software RA tool which has been extensively used since 1987, and is considered an effective and reliable method. CRAMM can also be regarded as a benchmark for RA to organizations because of the input of a number of government and private sector security experts to the tool (Yazar 2002). It is the mandatory security analysis method for UK governmental organisations (Spinnelis et al 1999), and is also used by large organisations that are in need of effective security such as IBM, Royal Air Force and the Swiss Bank Corporation (www.cramm.com). Performing RA with such a recognised tool is quite a lengthy process (full-reviews can sometimes take days or months according to the size and the geographic spread of the organisation (GSSL 1997)) which involves having to fill lengthy questionnaires, interview a number of users of the system and, for the person who performs the assessment, have specialist training in the

field. To use CRAMM one should undertake a training course which would cost £1200 in addition to the fee of purchasing the actual tool, which when quoted was approximately £1500 (www.cramm.com).

This is not only the case with CRAMM but with most of the RA tools on the market. Risk analysis is a very complex discipline that should be left to professional risk analysts. Few organisations can afford to have a dedicated, full-time risk analyst on their staff. A good risk analyst must have experience in many disciplines, for example information security, network architectures, hardware, software, and business strategies (Labuschagne 1999).

So even though such a tool offers a structured approach to risk assessment and a detailed countermeasures list, there are three major setbacks related with its use. (GSSL 1997, SANS 2002, Labuschagne 1999):

- The process is very lengthy and might take up to months;
- There is particular expertise and specialist training required by the person performing the analysis;
- The tool produces too much hard copy output;
- The high cost of such a solution;

CRAMM is further analysed in Chapter 4 where the existing solutions are discussed.

2.5.8 Other Solutions

Besides RA, the literature review identified certain other solutions that are often suggested for SMEs wishing to plan their security.

2.5.8.1 Baseline guidelines

According to ISO17799, after Risk Assessment, the second and the third sources for organisations to identify their security requirements are respectively *'the legal, statutory, regulatory and contractual requirements that an organisation, its trading partners, contractors and service providers have to satisfy'* and *'the particular set of principles, objectives and requirements for information processing that an organisation has developed to support its operations'* most commonly referred to as **baseline guidelines**.

Guidelines essentially *"provide best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining information security management systems"* (ISO 2006) and provide an alternative solution that can be followed in order to achieve security at a baseline level, but not as complete as the one accomplished after performing a risks assessment. A classic example of such documented security guidelines is ISO17799 itself, the International Standard Code of Practice for Information Security Management (ISO27001 2005). Unfortunately, only a small proportion of businesses are aware of the contents of such standards. As the DTI survey points out, only 38% of large organisations are aware of the contents of the standard, medium and small organisations once again fall significantly behind with 24% and 10% respectively.

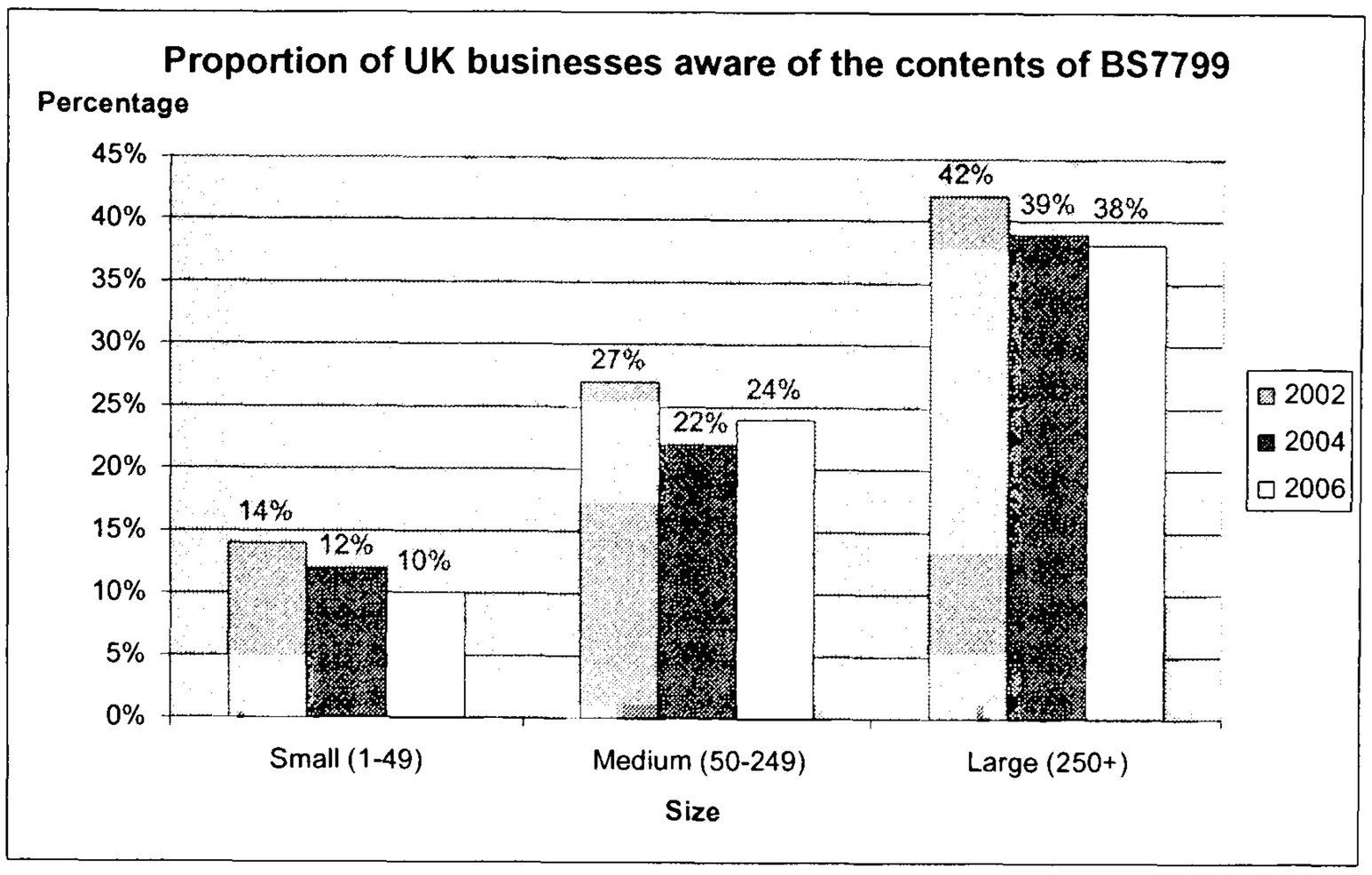


Figure 7: Awareness of the ISO 17799 Standard

As Figure 7 illustrates, there has actually been a fall in the number of organisations that adopt the standard compared to previous years (apart from medium enterprises where there has been a slight increase from the 2004 version of the survey, still lower than 2002, but nonetheless the numbers in all three categories are significantly low). Similar figures come from a survey performed by Ernst & Young (2005), which recognises that standards can provide a much needed framework for deploying effective I.S. practices, bringing out better alignment between I.S. and organisational objectives. However, according to this report, only 34% of large organisations and 18% of smaller have adopted the standard, while at the same time, looking at other similar guidelines, only 12% have become certified by the I.S. forum, 18% by CobIT, 23% by ITIL and 34% have adopted other standards. The statistics from this survey shown in Figure 8 are disappointing when looking at the percentages of organisations that have not adopted such a standard/certification.

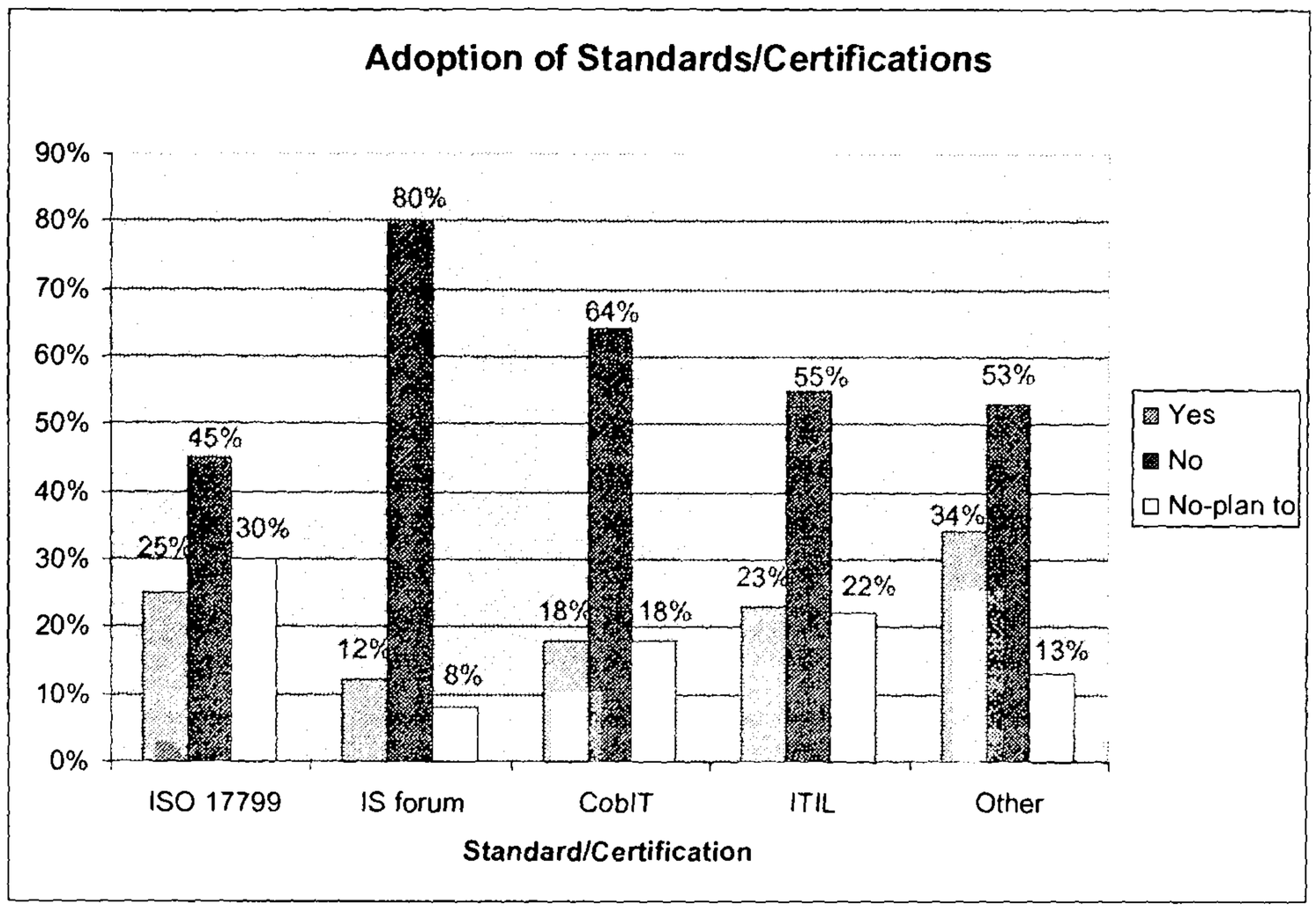


Figure 8: Organisations are not adopting I.S. standards/certifications

2.5.8.2 Outsourcing - third party security

Another alternative suggestion is for SMEs to implement third-party managed security services (Paraskevas and Buhalis 2002; Spinellis et al. 1999). This involves providing outside expertise and specialised support to organisations that do not employ security specialists. However as Figure 9 (including data from the DTI 2006 survey) illustrates, such solutions have not been significantly adopted either, even though they have more than doubled from the 2004 version of the survey.

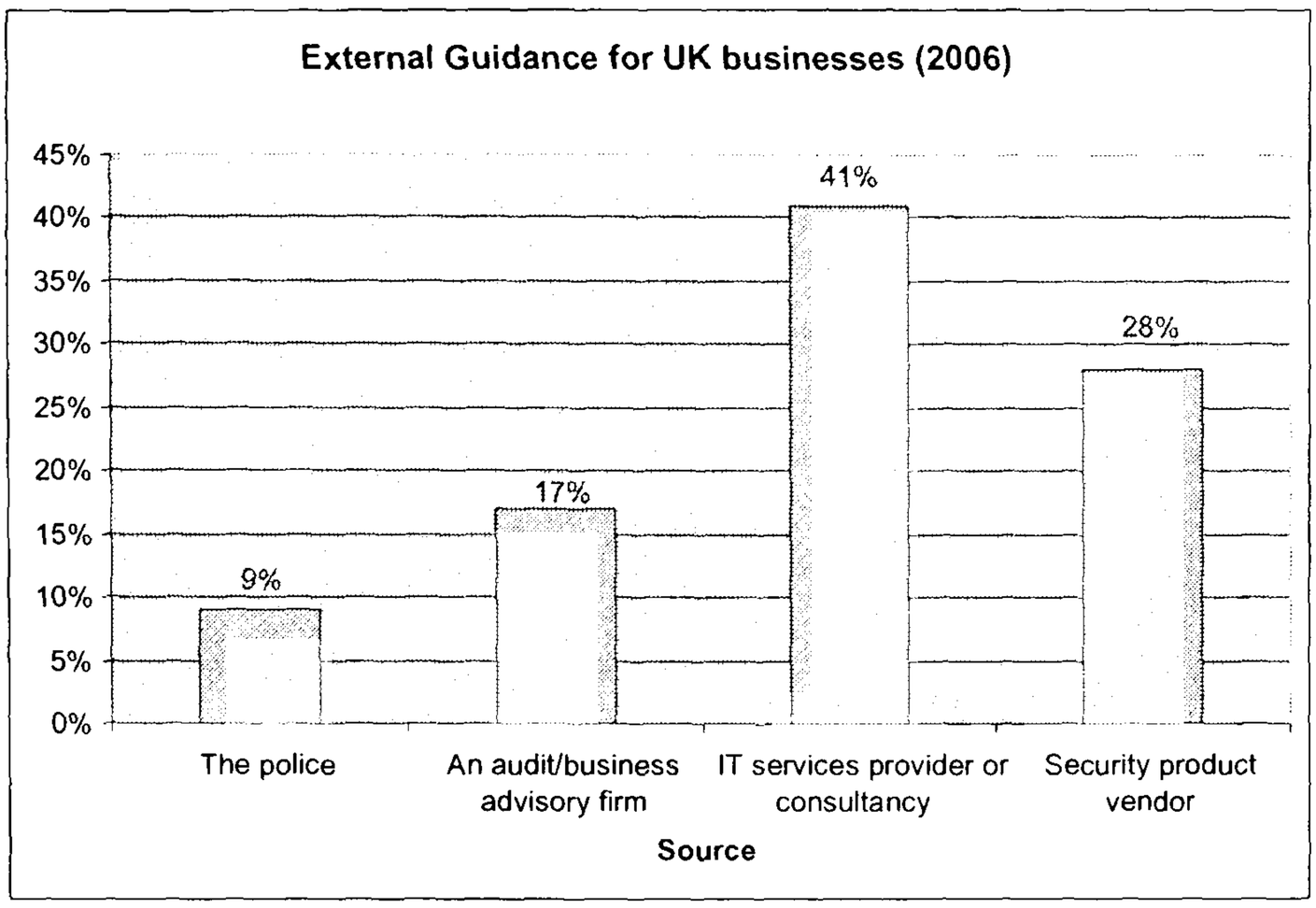


Figure 9: Adoption of external guidance

2.6 Conclusions

In this chapter we have established that although Risk Assessment is necessary, many organisations do not employ it. The required steps to be taken now in this research are:

- Identify the I.T. characteristics of SMEs. By doing so we can understand who has the problem, whom we are developing a solution for, and how the solution should be structured in order to cover their requirements.

- Use surveys and RA tool evaluation to determine what elements of RA and guidelines makes them unsuitable for SMEs, and also devise the requirements for a new tool that covers the needs of SMEs (i.e. what specific elements it needs to have).

RA is the number one practice when making a security strategy, but because of the characteristics of the SMEs described we need a mixture of the three solutions for an SME, a RA tool which can give assistance like guidelines but does not require a security expert to run or implement the selected controls, and which SME's budget can afford.

3. Security Requirements of SMEs

Based on survey findings, this chapter analyses the reasons why the existing solutions and particularly RA are not being implemented by SMEs. Having established that SMEs do not use RA, this section identifies those characteristics of SMEs that prevent its adoption.

3.1 Introduction

In the previous chapter we established the importance of approaching I.T. security in a planned and structured way, such as by consulting guidelines or performing a risk assessment, before acquiring and implementing any controls. What was also identified is that, even though a number of solutions exist, the large majority of organisations do not perform any of the operations that are recommended in order to achieve this approach to security, leading to large losses due to I.S. incidents. SMEs are the ones mainly facing both the security incidents and the non-adoption of the solutions. The purpose of this chapter is to investigate what the I.T. security characteristics of SMEs are, based on survey data. By identifying the characteristics of SME I.S. environments, the requirements of these organisations from an RA methodology can be established, leading this way to the investigation into the non-adoption of the existing RA solutions in the following chapter. More specifically, findings from the third-party surveys described in Chapter 2 will be used to identify the problem. Then the SME security survey conducted by the user will look to confirm these problems exist within SMEs and investigate their details. Having established the requirements of SMEs based on how the survey results are interpreted, this investigation will proceed to the identification and discussion of those

requirements that SMEs declare themselves they are in need of. Identifying the requirements of SMEs is the first step in identifying characteristics upon which existing solutions can be evaluated (in order to prove that it is these characteristics that existing solutions lack) and can also set the basis for the development of a novel methodology which shall cover these requirements.

3.2 Information Security Characteristics of SMEs

By looking at survey data on I.S. issues in the industry, certain aspects of SMEs can be identified that make the use of RA, as well as the other solutions, inappropriate for these organisations and deter the use of such methods.

3.2.1 Low budget for security

To commence this analysis, what is potentially the most prohibiting characteristic of SMEs will be discussed. All the SME problems start from here as all the other problems discussed later in this section are somewhat related to not having enough I.S. funding. Lack of information security funding not only affects the ability of an SME to purchase a RA tool, but also to train or hire someone to use it and even purchasing the appropriate controls for a risk that has been identified.

However, purchasing an RA tool alone only helps organisations plan their security. There is still the cost of acquiring the controls and SMEs devote a very low budget to do so. According to the findings of the ACCSS survey in Australia, 43% of the organisations

spend up to 5% of their I.T. budget on security and another 23% invest up to 10% of their budget for the same purpose while amazingly there are 4% that stated they do not spend any money on I.T. security (that is 16 organisations out of the 389 questioned that do not have any security at all). This leaves only a minor 30% that spend a somewhat significant proportion of their budget on I.T. security. According to data from the DTI survey (Figure 10), *'The average UK company now spends 4-5% of its I.T. budget on information security. Roughly two-fifths of businesses spend less than 1% of their I.T. budget on information security'* (DTI 2006). According to figures from the same report, out of the overall number of respondents (which are mainly SMEs), only 10% of the respondents spend more than 10% on security (Figure 10). It is somewhat surprising that a considerable 14% of the respondents have stated they do not invest any money on I.T. security while, another 26% invest less than 1% of their overall I.T. budget.

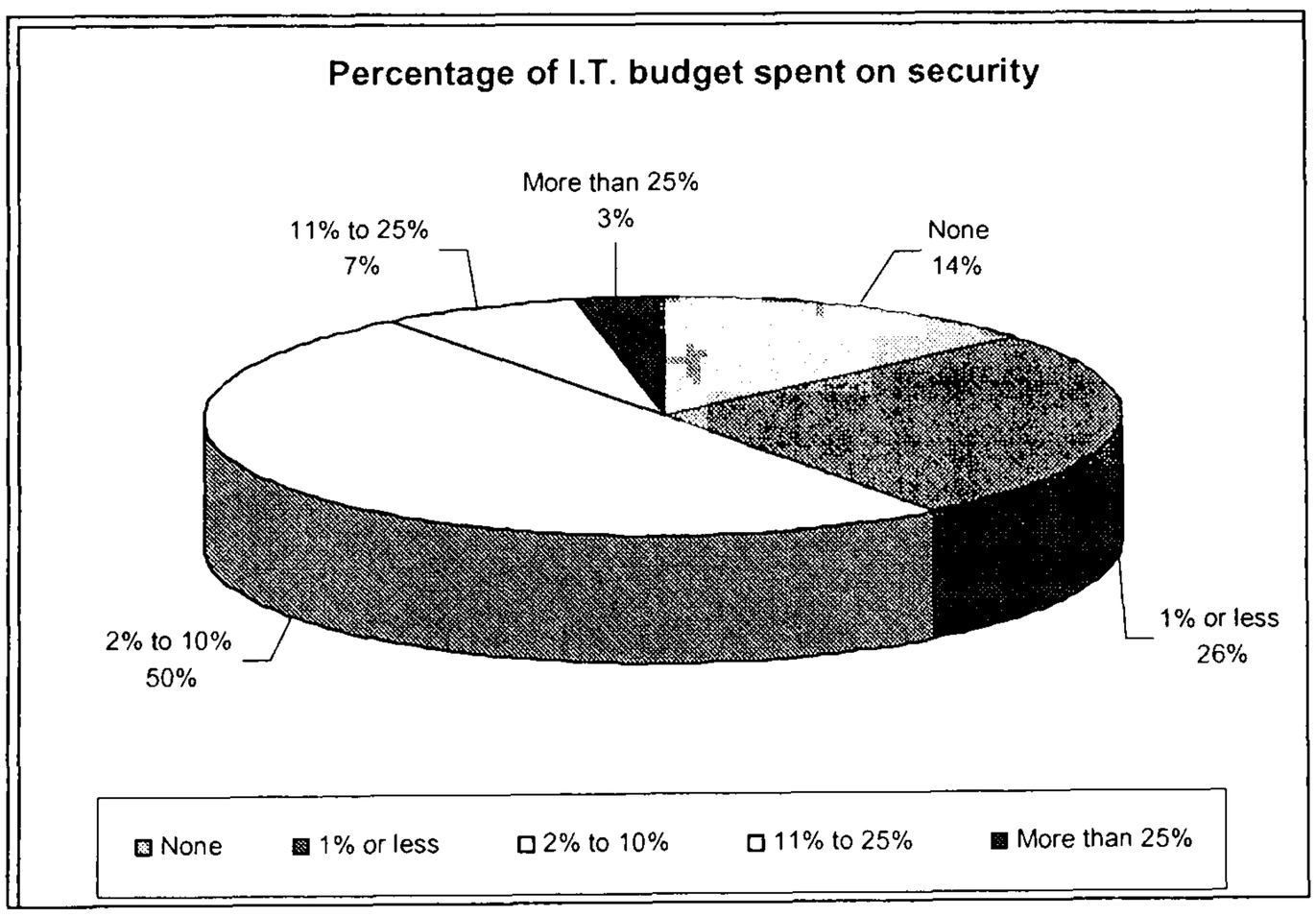


Figure 10: SMEs under-invest on security (source: DTI 2006)

A survey by Deloitte (2005) across a wider geographical sample, has found that the figures are similar throughout the world. Even though it does not address SMEs in particular, the figures are similar to the ones from the previous two surveys mentioned and therefore it cannot be very far off for the rest of the world. It is worth mentioning that the one that copes better here is USA with approximately 31% of organisations spending more than 10% of their I.T. budget while for the rest of the world the percentage of organisations that spend more than 10% are 23% for Europe, Middle-east and Africa, 12% for Canada, 11% for Asia Pacific (which includes Australia, Japan and China), and approximately 3% for Latin America and Caribbean,

Finally, an interesting statistic is provided by Department of Trade and Industry survey which indicates that *'Only 44% of companies have carried out any security risk assessment in the last year. Those that assess the risks tend to spend more on security, suggesting the others are under-investing.'*

Therefore a requirement of an SME from an RA methodology is to inform organisations of the benefits of spending for security, be comprehensive to the management that decides what is spent, at the same time provide cost effective controls to take full advantage of the available budget, and finally be at a low cost itself (which of course is irrelevant as far as this PhD research prototype is concerned, but says something when evaluating existing solutions later on in chapter 4)

3.2.2 Lack of expertise

Another key characteristic of SMEs from an I.T. perspective is that within these size organisations there rarely exists a full time security expert. Not having a person that is suitably qualified on the field and specialises in practicing I.T. security leaves great gaps in terms of planning and implementing security, and responding to incidents. As the DTI survey reports, *"There is still a shortage of security qualified staff; only one in eight companies has any"* (DTI 2006). Availability of qualified I.S. staff was one of the issues that considered by the SME security survey

More specifically, the DTI survey has also asked the question about whether the person responsible for security has formal I.T. security qualifications, from the whole range of respondents, only 2% said both the person responsible as well as others have qualifications, 3% stated that the person responsible has qualification and 7% responded that others in the team are formally qualified. This leaves 88% of the respondents with someone responsible for security who has no qualifications. Judging by these responses, an image is starting to build that I.T. security within SMEs is a task left to an employee who may either have some knowledge on the issue or even have more spare time than the rest of the staff, they do not however have any formal qualifications on the area which raises serious questions.

Therefore, as another requirement of SMEs, a methodology which aims to be used by this person and provide useful results will need to be easy to use and comprehensive enough to allow anyone within the organisation with some knowledge of the business or the I.T. functions to use it without however getting into very technical details as this person might

well be a manager with no technical knowledge. The results produced by the tool should also be comprehensive enough for the same purpose and, considering there is no I.T. security expert within the organisation, it should provide guidance on how to deploy the recommended countermeasures.

3.2.3 Poor selection of controls

What comes naturally after establishing that the majority of SMEs have a quite low dedicated security budget and very few have security staff employed, is wondering about the appropriateness of the controls they are implementing. Guiding an organisation towards selecting 'successful' and appropriate controls is one of the main purposes of a Risk Assessment tool.

Furthermore, purchasing and installing antivirus and a firewall (or any other control - these are simply mentioned because most organisations seem to have them) is not enough, correct configuration is also an issue (Chong 2003). The firewall needs to be configured to determine program and employee access privileges, and the antivirus needs to be configured to update and scan regularly. Having established that within SMEs I.T. security is not being handled by specially trained personnel it is logical to argue that correct configuration is not being performed. This can also be assumed for most of the controls and once again this is proved by the amount of incidents reported.

Data from the DTI survey supports the discussion about SMEs choosing controls poorly and, more importantly, implementing them incorrectly. More specifically, among the key findings of the DTI ISBS 2006 on this issue:

- A quarter of UK businesses are not protected against spyware.
- UK companies are poorly placed to deal with identity theft; only 1% have a comprehensive approach for identity management (authentication, access control and user provisioning). 84% say there is no business requirement to improve this.
- Three-fifths of companies that allow remote access do not encrypt their transmissions; businesses that allow remote access are more likely to have their networks penetrated.
- Three-fifths of companies do not block staff access to inappropriate web-sites and only one in six scans outgoing e-mail for inappropriate content.
- 30% of transactional web-sites do not encrypt the transactions that pass over the Internet.
- One in five wireless networks is completely unprotected, while a further one in five is not encrypted. Two-fifths of companies that allow staff to connect via public wireless hotspots do not encrypt the transmissions.
- 55% of firms have taken no steps to protect themselves against the threat posed by removable media devices (e.g. USB tokens).
- Two-fifths of companies that allow instant messaging have no controls in place over its use.

- Only half of the companies that have implemented Voice over IP telephony evaluated the security risks before doing so.

These are only some of the findings on the issue but they are sufficient to confirm that there is a clear need for providing explanations on what the controls are, how they can be implemented correctly, how they correspond to threats, and what savings they can help achieve, so the user can select the appropriate ones even with no security expertise. They should also provide feedback to ensure any neglecting of appropriate (based on statistical data and not a precise figure) controls that the users select can be corrected as soon as threats start occurring.

3.2.4 Awareness

Even if controls were selected carefully, organisations fail to follow a holistic approach to security which will combine technology with awareness (Munley 2004). Ignorance of even the basics of security is a very big threat itself (Sustaita 2001), so it is even worst if this lack of awareness on security issues is encountered on an organisations management. This lack of managerial awareness on I.T. security issues is seen in the CIO survey where executives of organisations that have reported they have been attacked were asked to identify how they were attacked, where from and by whom. As Figure 11 illustrates, a quarter of the respondents, was not aware of any of the details that caused losses and potentially damaged reputation and disruption of operations to the organisation. At the same time 47% of the executives that responded stated they were not aware of what damages were caused by the security incidents they had. These figures shown in this

survey mainly correspond to large organisations. As the trend of all the survey findings normally show, it would be expected SME executives to fare even worse in this area.

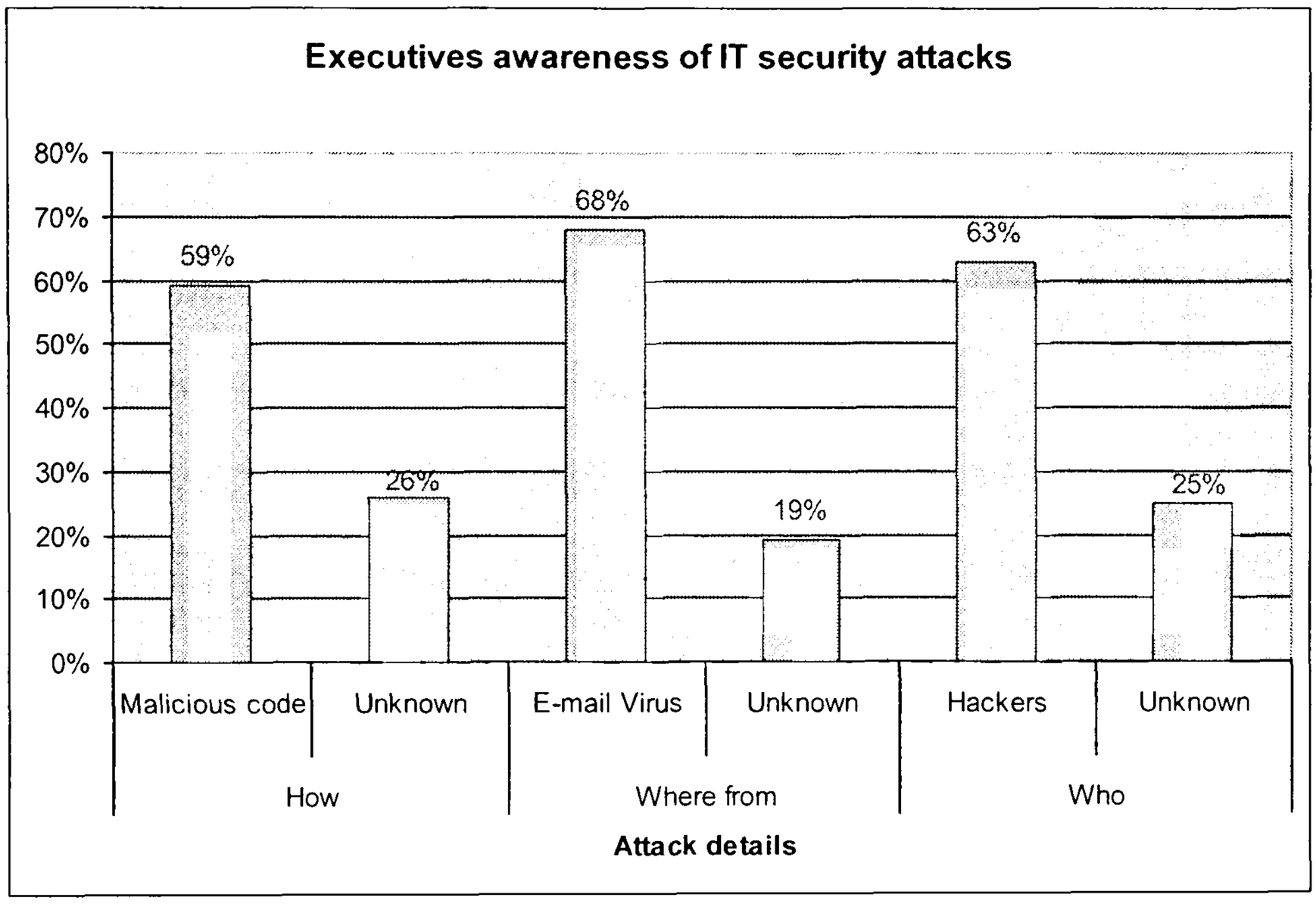


Figure 11: Executive's awareness of attack details (Berinato 2005)

In the findings of the survey published by DTT, respondents from the managerial level of organisations where asked their view of I.S. A massive 82% responded that it is 'somewhat appreciated', while only 18% stated it is highly appreciated. This again illustrates the lack of managerial awareness on the importance of properly securing their I.T. infrastructure and what losses a security incident may cause their organisations.

This lack of managerial awareness also justifies the lack of funding towards I.T. security, meaning that it is the management that funds these operations and it must therefore be informed enough on the threats and possible losses to proceed to spending the appropriate

amount of funds towards purchasing and implementing controls. As the previous part found, SMEs spend 5% of their budget on securing (incompletely as survey data on annual losses indicates) critical information assets that cost thousands. This illustrates they most likely do not build a formal business case to estimate Annual Loss Expectancy (ALE) because of risks and the Return on Investment (ROI) offered when spending on security controls to eliminate these risks. Therefore one of the primary purposes of an RA methodology aiming at SMEs should be to offer ROI considerations by quantifying what assets need protecting, what their cost is and how likely they will be subject to a threat, what this threat occurring may cost them (Hoo 2000) and contrast that to the cost of securing each asset with the appropriate number of controls (Cisco 2001). The absence of an accepted industry-wide measurement system that would enable managers to judge the importance and the effects of the threats (Robins 2001) (i.e. a well-understood economic model exists for evaluating the benefits of reducing the risks versus the investment in security technology and management) makes the output of RA's hard to be understood by the management. Therefore it would be preferable for the case of SMEs if this data was, at the end of the RA, presented to the management in the form of a comprehensive report that attempts to raise awareness by contrasting both the effect of controls to the threats the organisation faces together with the cost of the controls against a threat versus the cost of a breach because of that threat. This way the management would be aware on all three issues of the I.T. assets of the organisation, the threats the organisation faces and the benefits offered by the controls.

3.2.5 Disruption of operations

By definition, SMEs have a relatively small number of employees, making it more likely that conducting RA would disrupt staff that may have other significant responsibilities to attend to. Consequently assigning a member of personnel with the task of performing a Risk Assessment would be likely to involve the time consuming tasks of identifying the assets, the details for these assets, rating their importance or value, selecting and implementing the controls. Such a task would require significant reading and background education on these subjects and even more if the person is performing the assessment using one of the automated tools available. A lot of these tools require background training for the person using it and normally involves needing the person to undergo seminars on how to use the tool as is the case discussed earlier with CRAMM. Moreover if the process of the RA involves needing several members of personnel within the organisation to undergo interviews or complete questionnaires, such a task would firstly cause more disruption and secondly could possibly span over a few days (if people are unavailable). This disruption becomes a more significant problem if the analysis points out deficiencies that need to be assessed (Federal Aviation Association 2001).

3.3 The SME security survey

Having established, through existing survey data, that there are certain setbacks associated with the security characteristics of SMEs which may be deterring the wide adoption of RA, a further survey was conducted by the author more specific into the issue of RA within SMEs. The aim was to confirm the assumptions discussed from the previous survey findings and investigate the I.T. and I.S. characteristics of SMEs,

examine the adoption of RA and reasons deterring it from being embraced by these type organisations.

3.3.1 Methodology

As introduced in Chapter 2, this survey was initially conducted in the US and subsequently in Europe. The reason for considering both geographical areas individually is because different security and data protection legislation apply in each continent as May (2004) and Burke (2003) describe for the US and Baker and McKenzie (2004) for the EU. The purpose was to investigate to what extent and how these influence organisations approaches to security. For the purposes of the survey, organisations with up to 250 employees were classed as SMEs mainly to allow for the results to be comparable with those in the DTI survey which also mainly assesses SMEs. Figure 12 illustrates the exact distribution of sizes that responded in the survey.

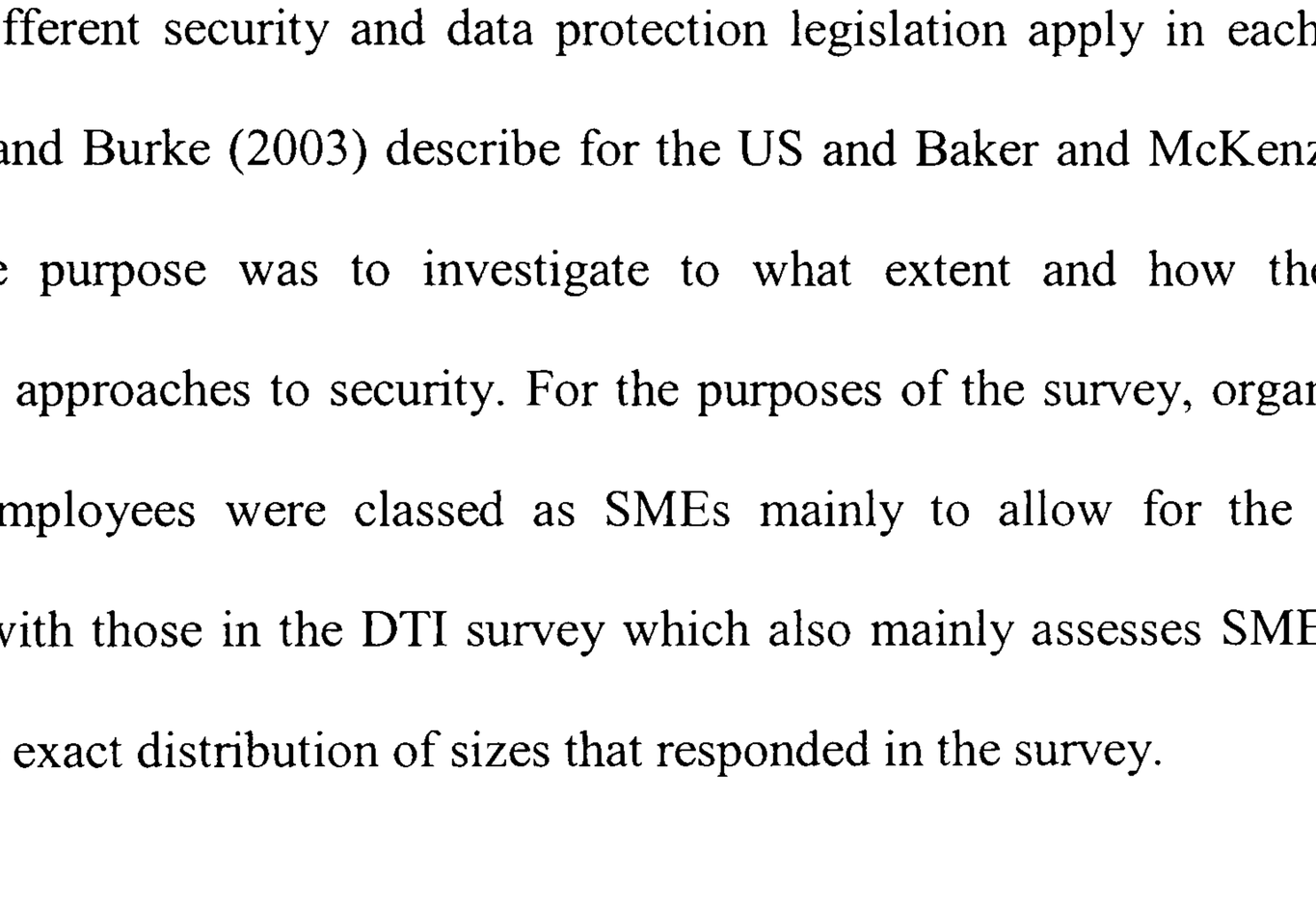


Figure 12: Size of the organisations that participated in the survey (US and Europe)

As Figure 13 Illustrates, the survey gathered responses from 40 organisations within Europe and 79 within the US.

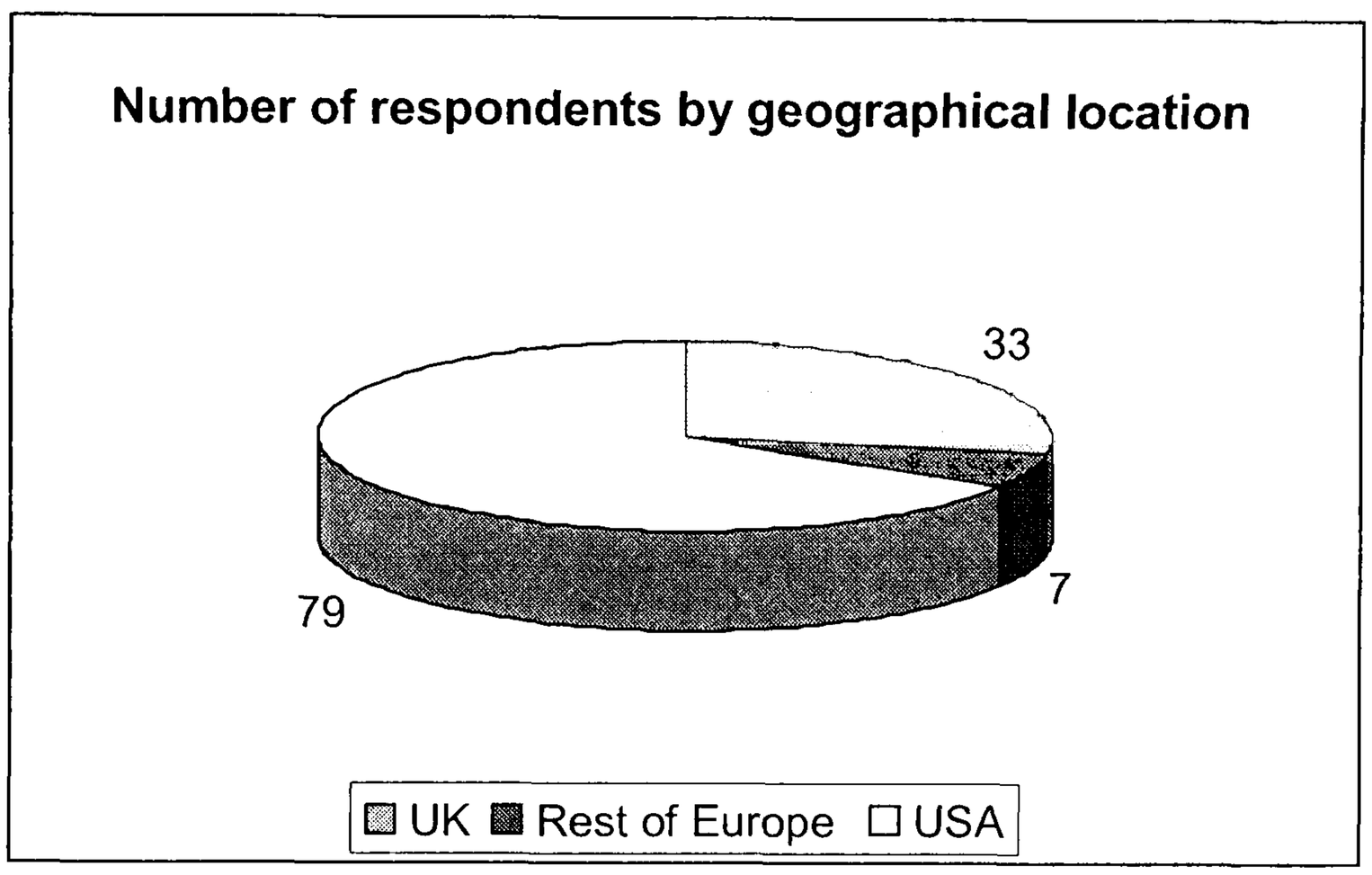


Figure 13: Where the responding organisations originated from

In the US, the survey was conducted by San Diego University in early 2004 and was distributed by hand to personnel related to the Managerial, I.T. and security operation within organisations of various sizes. After a discussion with the creators of this survey in April 2004, it was decided to create a European version which would allow the sharing of results and establish attitudes towards security in both continents. The European survey was conducted subsequent to the US version (took place between the period of 11th of June until the 15th of August 2004) as an email-based survey. The questionnaire was distributed to 500 SMEs and overall 119 responded. Initially, a number of trial questionnaires were sent out in order to identify potential problems regarding the structure and expression of the questions. The responses resulted in the correction of a

few minor points. The next stage was the distribution of the corrected questionnaire to selected companies. It was sent out as an email attachment in the form of a Microsoft Word document (as shown in Appendix B) accompanied with a cover letter stating the purpose of the survey.

In contrast to the criteria upon which organisations were selected by in the US version (primarily distributed by hand to local SME personnel), the SMEs that participated in the European version of the SME security survey are selected primarily from related directories on the Internet such as *www.smedirectory.net* and *www.ukontheweb.net*. Certain criteria were considered in order to filter the potential candidates:

- Their relative dependence on the IT infrastructure (i.e. assuming that organisations under categories such as "Builders" are not that dependant on their I.T.).
- Their size does not exceed 250 employees to be according to the SME definition given earlier in this thesis.
- Avoiding industries that are large by nature such as those belonging to the government sector.

Figure 14 illustrates the spread of the industry sectors the respondents of the SME security survey (in both continents) originated from.

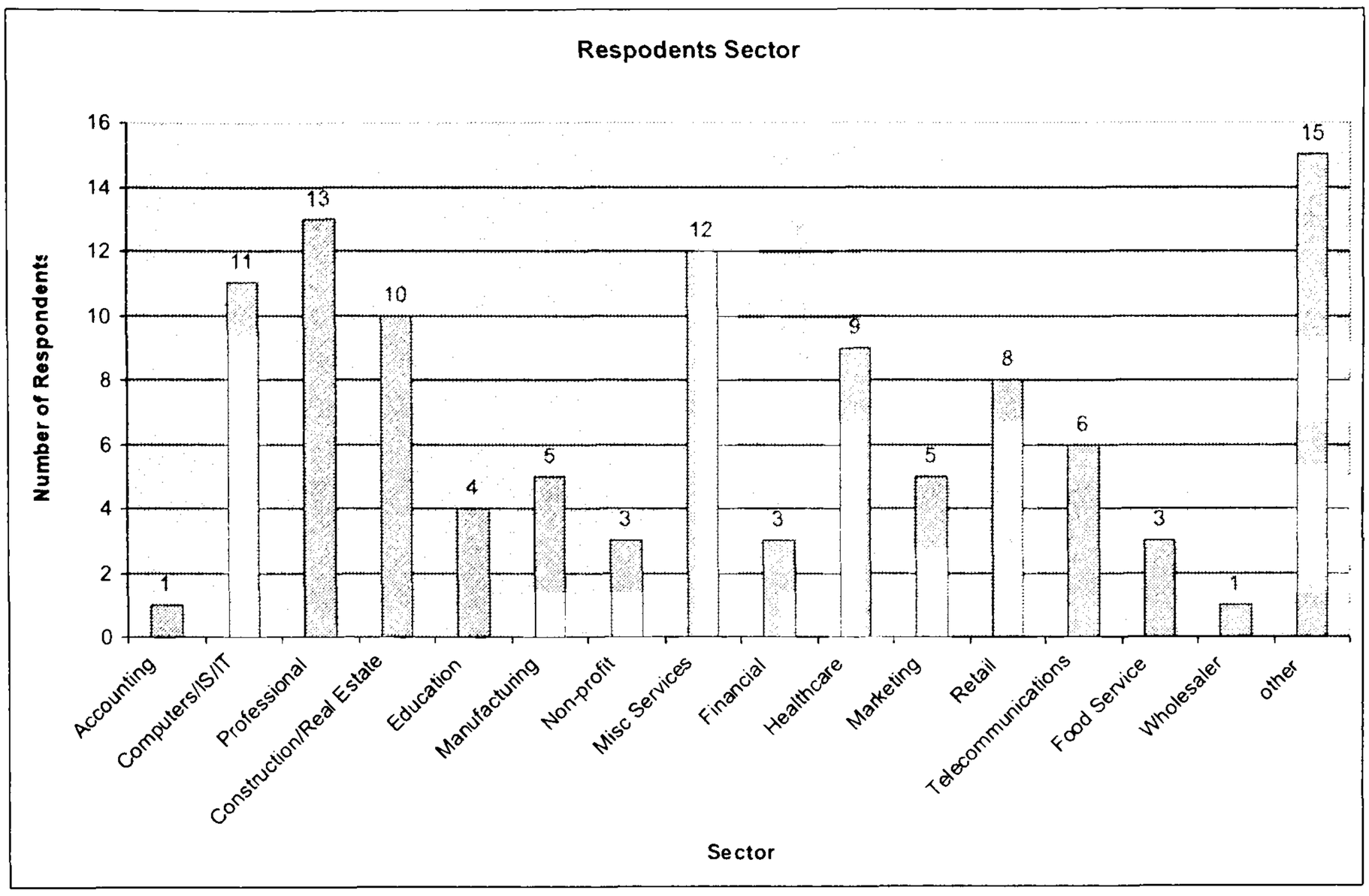


Figure 14: Industry sector the respondents originated from

The European version was created based on the US questionnaire but with the addition of certain questions on issues this research was specifically interested in addressing. More specifically, the US version of the survey included three main sections:

- The first section profiled the respondent as well as the organisation in order to provide statistical data on the sectors, sizes etc that were investigated.
- The second section concerned security management issues such as security planning, policies and employee training. The aim was to establish information on what the current security education and awareness levels within SMEs.
- Finally the third part focused on the actual security practices organisations have in place so as to determine whether organisations that do not generally analyse and manage their risks (survey data in Chapter 2 already established RA is not being used by SMEs) manage to deploy efficient countermeasures.

In the European version, the same three sections were investigated so as to provide comparable results. However, a further section was included which investigated:

- Issues related with Risk Analysis such as its adoption, organisations view of RA, investment in RA and reasons that may deter it. This additional investigation aims to provide with further insight into what organisations wish from an RA solution therefore lead to the design of a novel methodology (after establishing in the following chapters whether or not existing tools fulfil these requirements).

3.3.2 Survey Findings

The findings of the SME security survey confirm the issues identified in section 3.2 about the characteristics of SMEs. The following sections will describe these findings on the same issues.

3.3.2.1 Lack of Funding

As Figure 15 illustrates, the SME security survey queried the respondents to what extend they would be willing to invest on purchasing an RA tool if they were convinced it would solve all their problems. The majority responded that they are not willing to spend more than £1000, with a considerable percentage declaring they would not even spend more than £100. Just to illustrate, CRAMM would cost an organisation approximately £1500 plus another £1200 for training alone each person who will be using the tool.

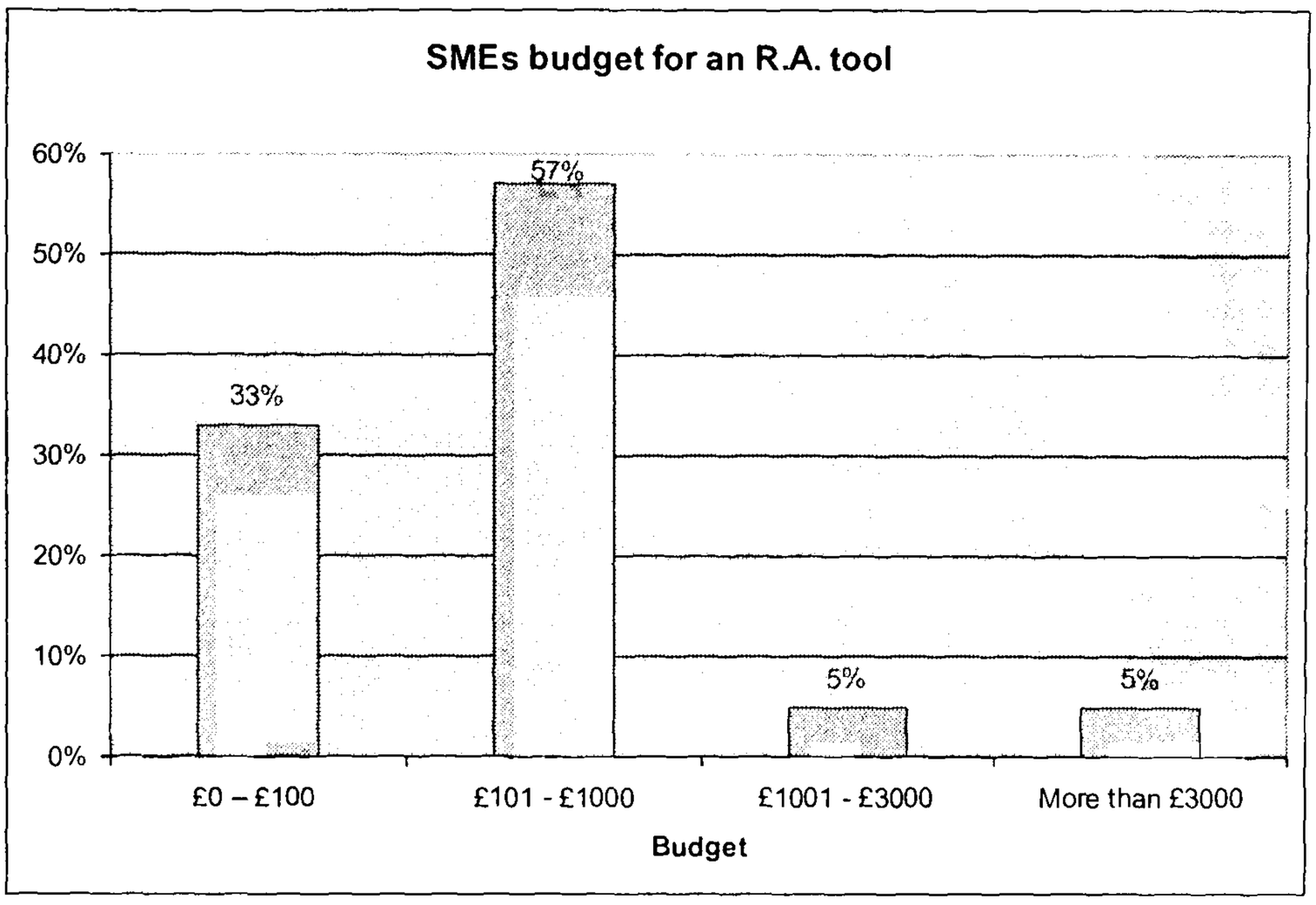


Figure 15: What are organisations willing to spend for an RA tool

3.3.2.2 Lack of Expertise

What raised questions between the designers of the survey was that the American version of the survey found that, as illustrated in Figure 16, quite a lot of organisations stated they do have a person who is responsible for security. Of course, more than half the organisations having an I.S. specialist is still not a re-assuring figure but it still seems higher than what one would expect judging by the amount of incidents and the losses reported.

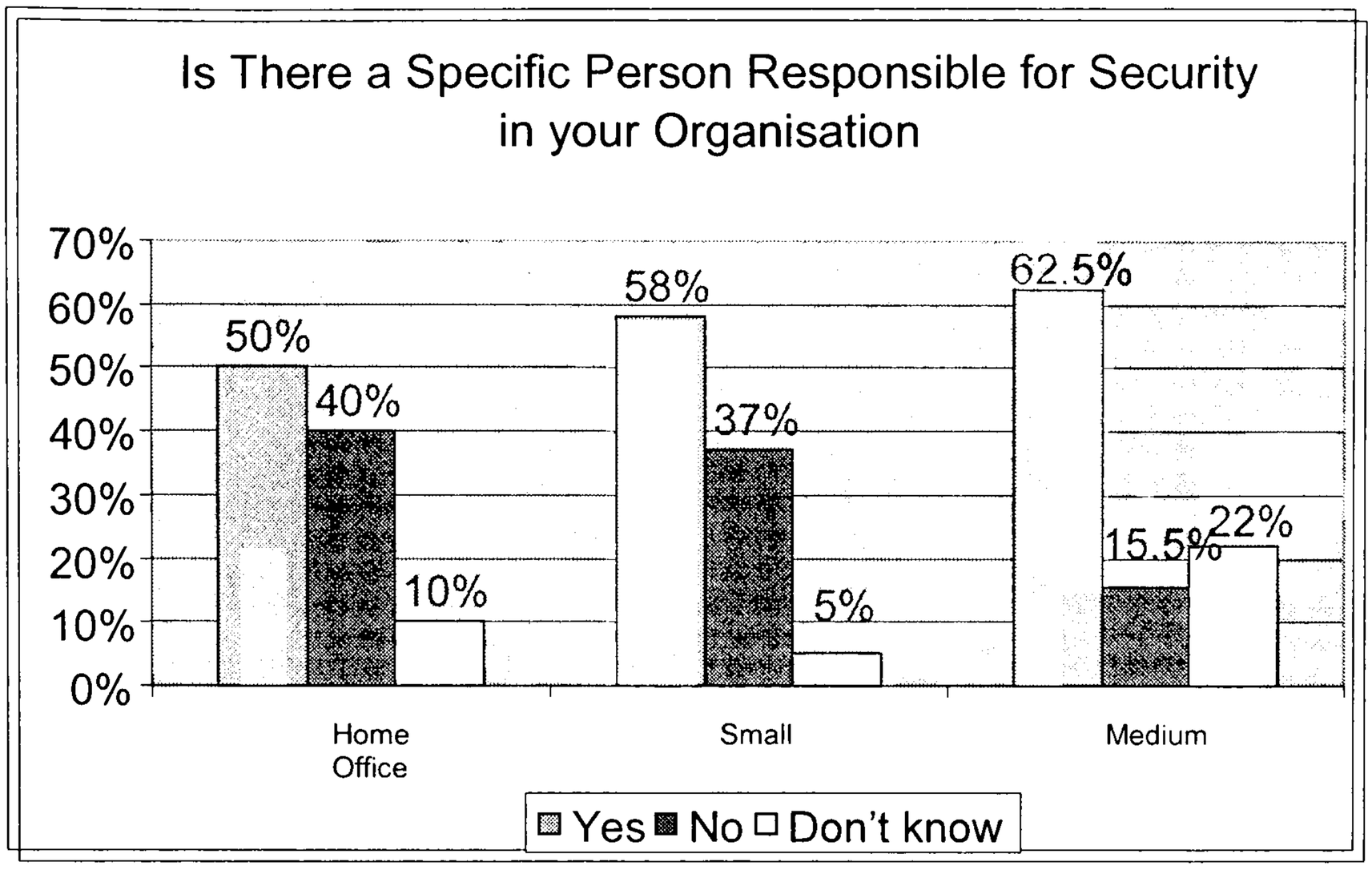


Figure 16: Is there a person responsible for I.T. security? (USA)

Therefore, in the European version of the survey, the same question also queried the respondents who the person responsible for security actually is. The responses, which can be seen in Figure 17, illustrate that SMEs just do not employee dedicated I.T. security officers. Half the organisations responded that it is the I.T. administrator that handles security and the remaining indicated either a manager, or a director or the owner (all possibly with no training on I.T., but with access to funds however) has responsibility. It is worth noting that, probably as expected, none of the organisations that employee less than 20 employees had a security officer.

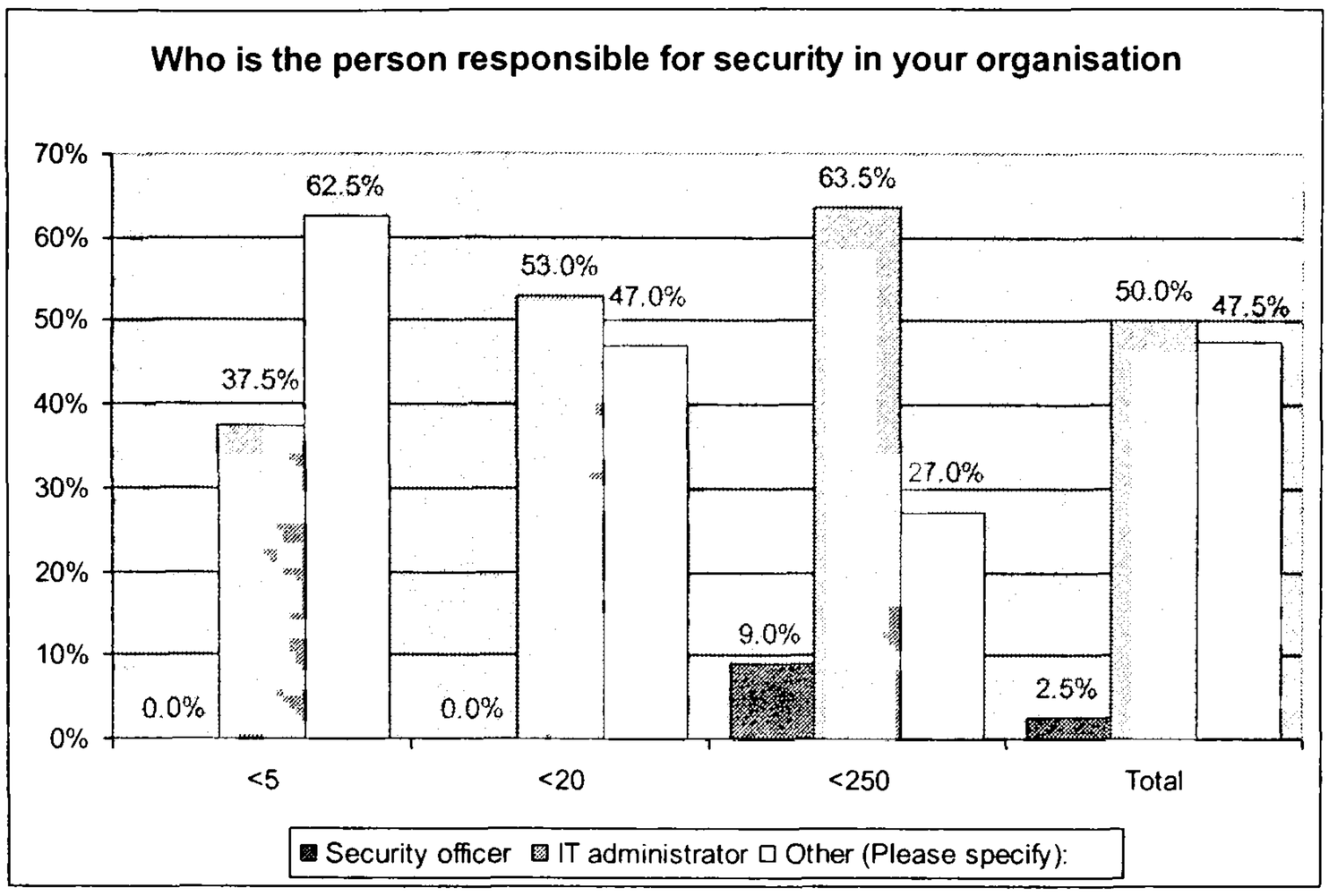


Figure 17: Who is responsible for security (Europe)

To look further into this issue, the European version of the survey asked whether the person responsible for I.T. security had any I.T. security qualifications. The response, as Figure 18 illustrates, was a staggering 75% out of the total number of respondents that said 'No'.

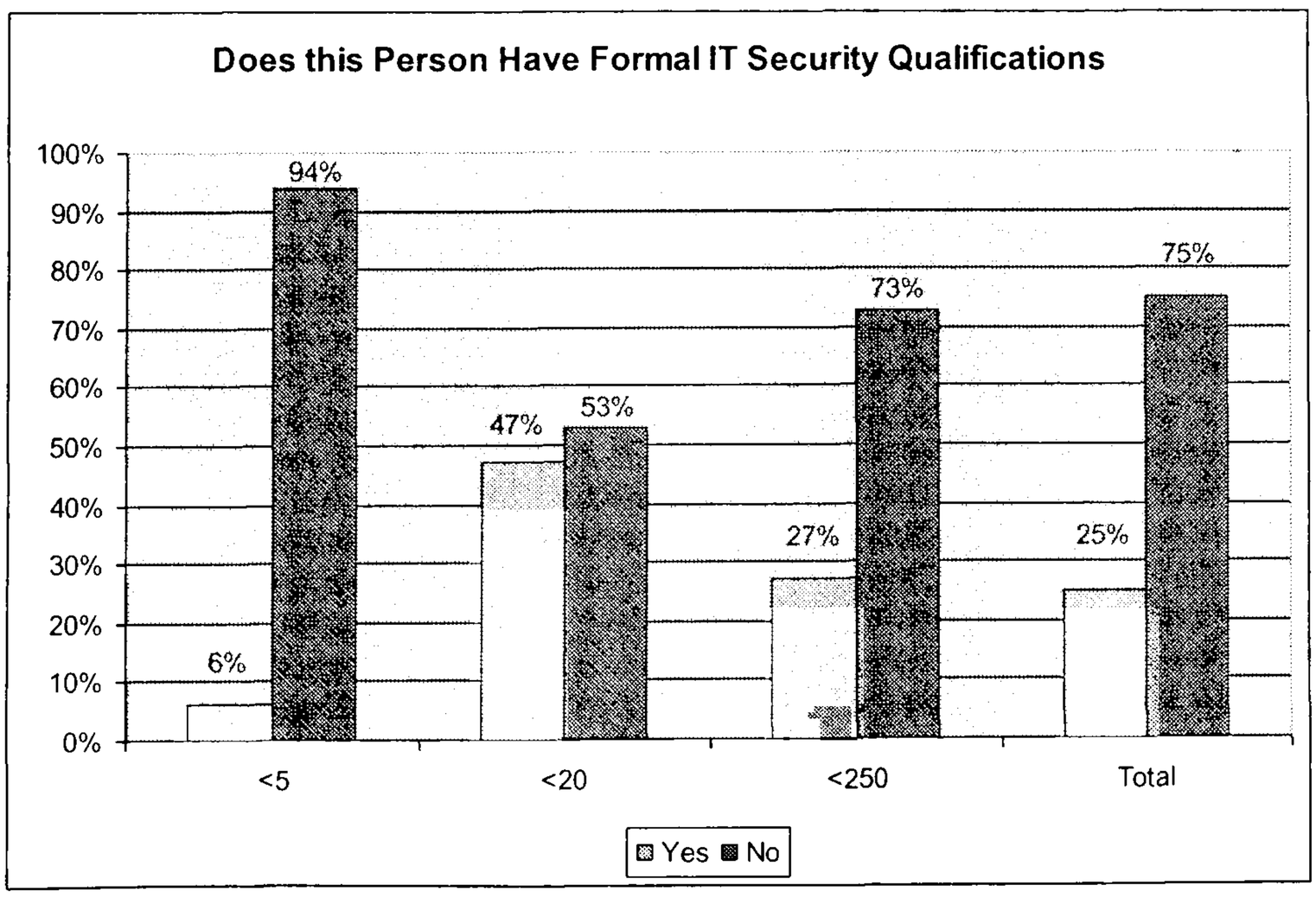


Figure 18: Formal qualifications of the person responsible

This leads into two conclusions as far as the characteristics of SMEs is concerned. Firstly half of the organisations do not employee anyone responsible for security and secondly from the other half that do, three quarters do not have any qualifications. Even though our test sample was relatively small, data from other surveys comes to confirm our findings

3.3.2.3 Poor selection of controls

The survey looked into SMEs selections of controls both in the US as well as in Europe. An investigation into these selections reveals their quality. Figure 19 and Figure 20 indicate that, despite the different legislation and requirements, respondents in both continents have a similar attitude towards I.T. security, and although there are some noticeable differences in some aspects (e.g. organisations in Europe appear to be better at applying operating system patches, while those in the US are better with implementing password policies), the general picture suggests some significant areas of weakness in SME security. Even amongst the high-scoring categories (e.g. antivirus and firewalls), the results suggest that a fair proportion of organisations have not attended to these issues at all.

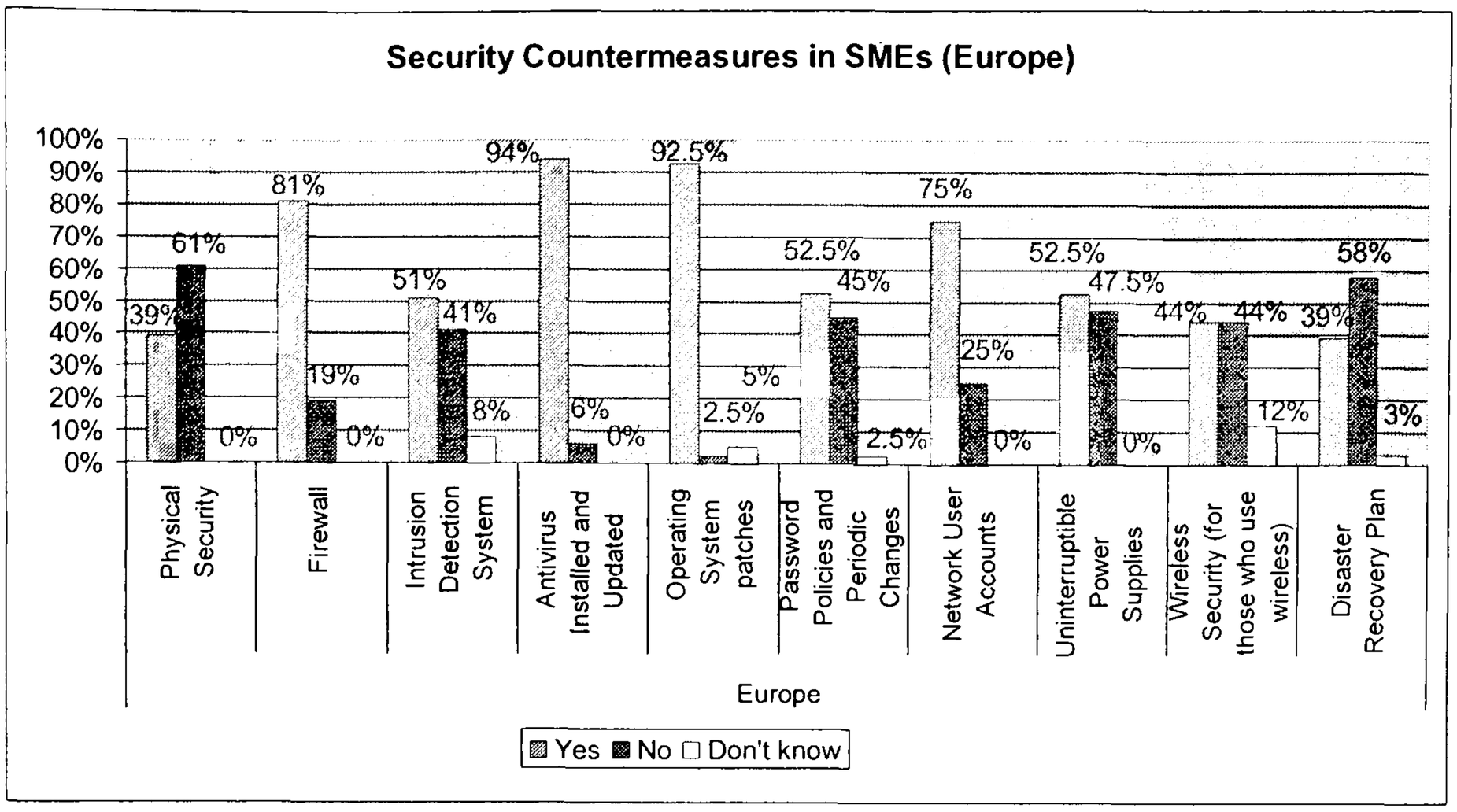


Figure 19: Security Countermeasures in Europe

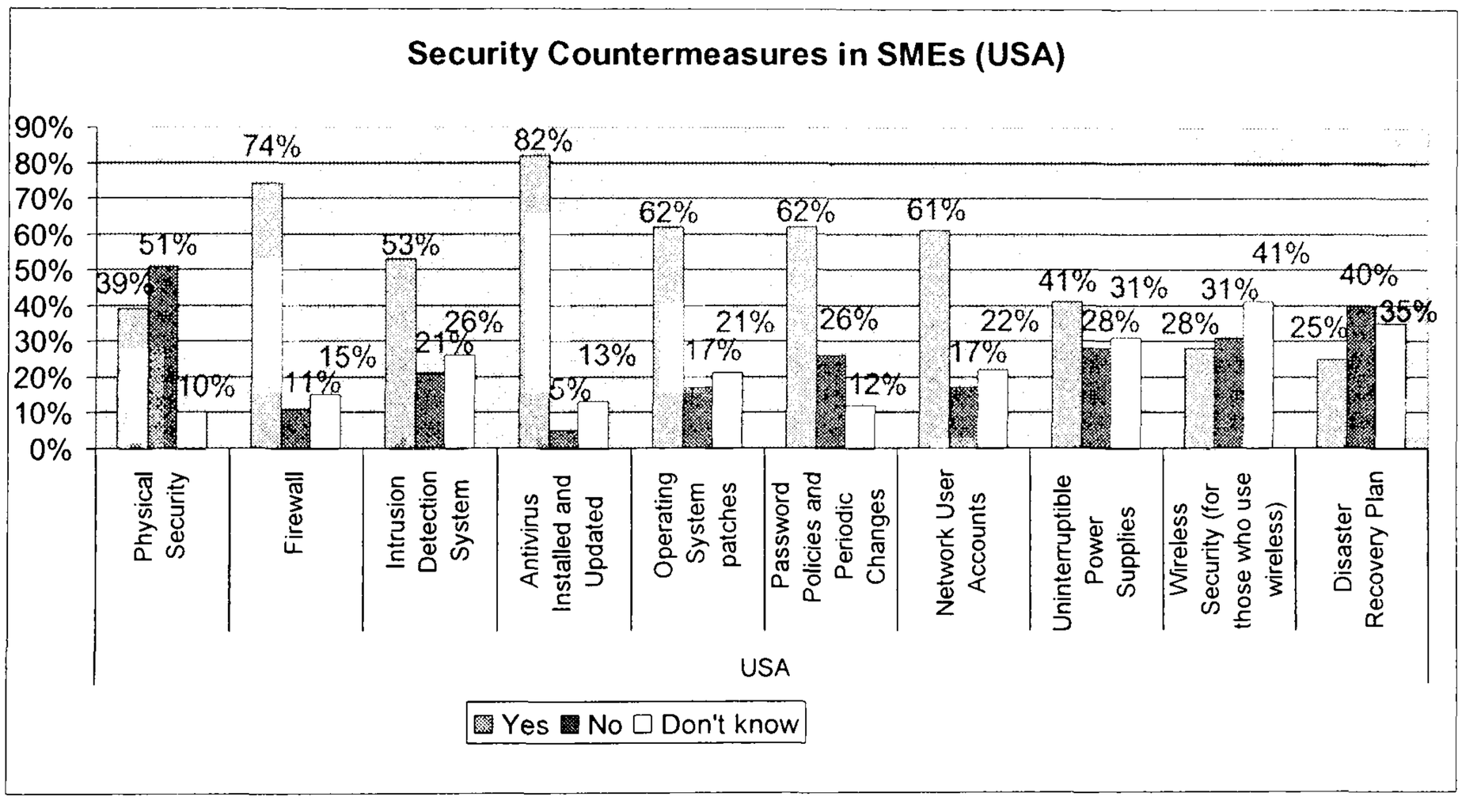


Figure 20: Security Countermeasures in the USA

Besides antivirus and firewalls, the results of the survey illustrate that a very large percentage of SMEs do not take any precautions as far as physical security is concerned. Logical IDS systems as well as logical access (i.e. passwords) also fare very badly with

approximately half the organisations not implementing any. Out of those organisations that reported they use wireless only a very low percentage (28% in the US and 44% in Europe) stated they have wireless security in place. All these leave the I.T. systems largely exposed, primarily to abuse by insiders and outsiders but to other threats as well. One of the most critical controls against accidental disruption of I.T. activities, UPS, is also being used by approximately half the organisations while the percentage of the organisations that have a well-thought and documented plan of recovering from a security incident is a lot less than half in both continents. Not having such a plan will only increase the man-hours required to respond to a security incident and therefore, in most cases, increase the financial burden.

A key point is that these results are particular to the SME environment, and posing the same questions in larger organisations reveals substantially different findings. Indeed, in the US version of the study, where the questionnaire was also distributed to over 100 organisations with 500+ employees, the 'yes' responses were an average of 21% higher across these ten categories (although in some cases, such as attention to wireless security, even the large organisations still faired badly, with only 34% responding positively).

3.3.2.4 Lack of awareness

Having established that SMEs do not select the appropriate controls, a question that is raised is whether the management is aware of these bad security practices or are the managers and owners sitting confident that security is adequate? The lack of security awareness within SMEs and their management is obvious when looking at the

contradicting statistics that were established from the SME security survey. More specifically, even though all the respondents stated they are somewhat or totally dependent on their I.T. infrastructure, as Figure 21 shows.

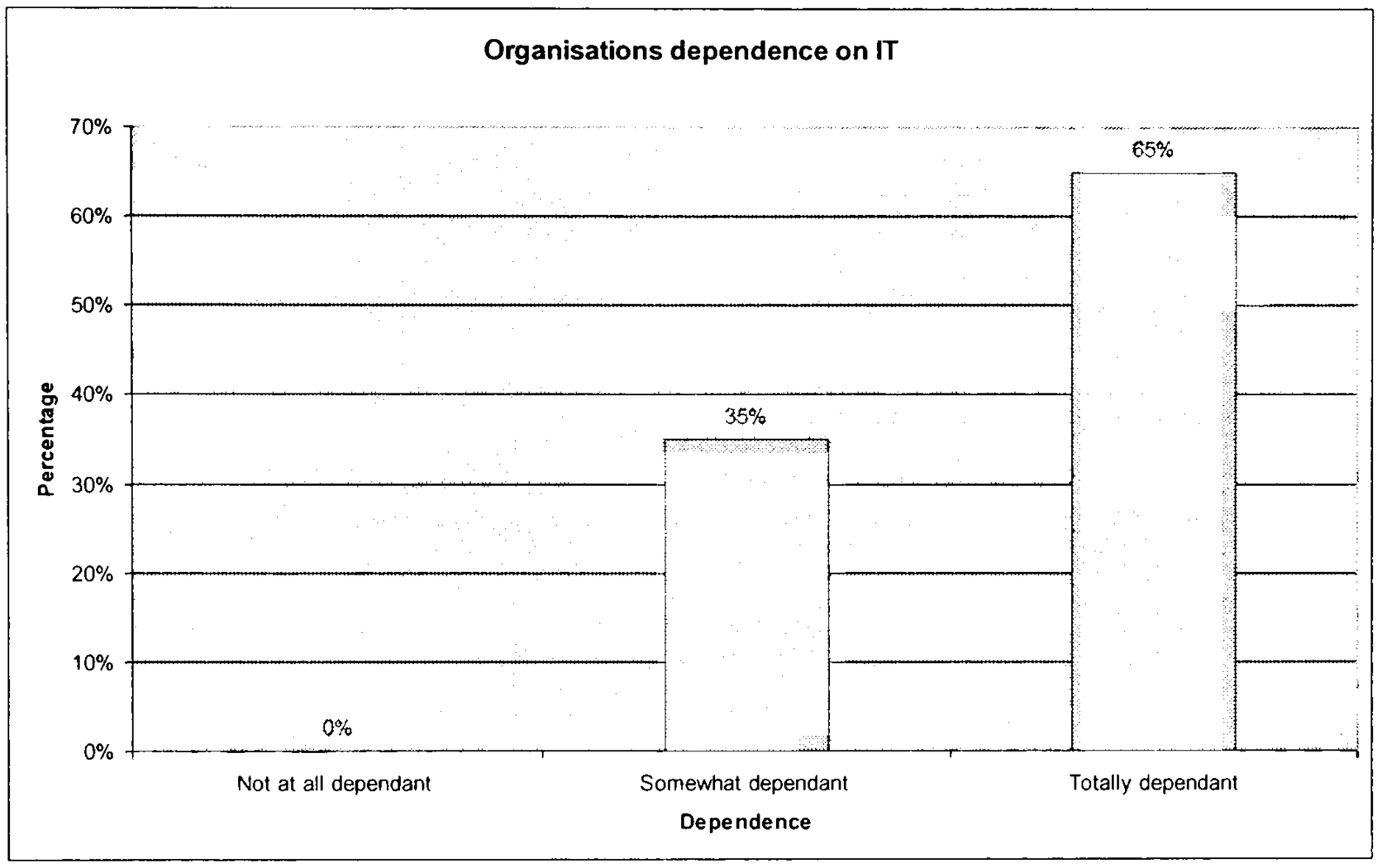


Figure 21: Organisations dependence on I.T. (Europe)

The previously discussed (both here as well as in Chapter 2) findings have established that:

- The same SMEs do not employee any security experts
- They do not adopt standards and guidelines like ISO17799, or have documented security policies
- They do not identify analyse and manage risks and vulnerabilities by performing an RA.
- They have deployed insufficient security practices, proved both by their survey responses as well as from the surveys which illustrate rise of incidents and losses particularly SMEs.

However, the lack of awareness on I.S. issues is evident when the majority of the respondents (62.5%) state they are confident of their security as Figure 22 illustrates.

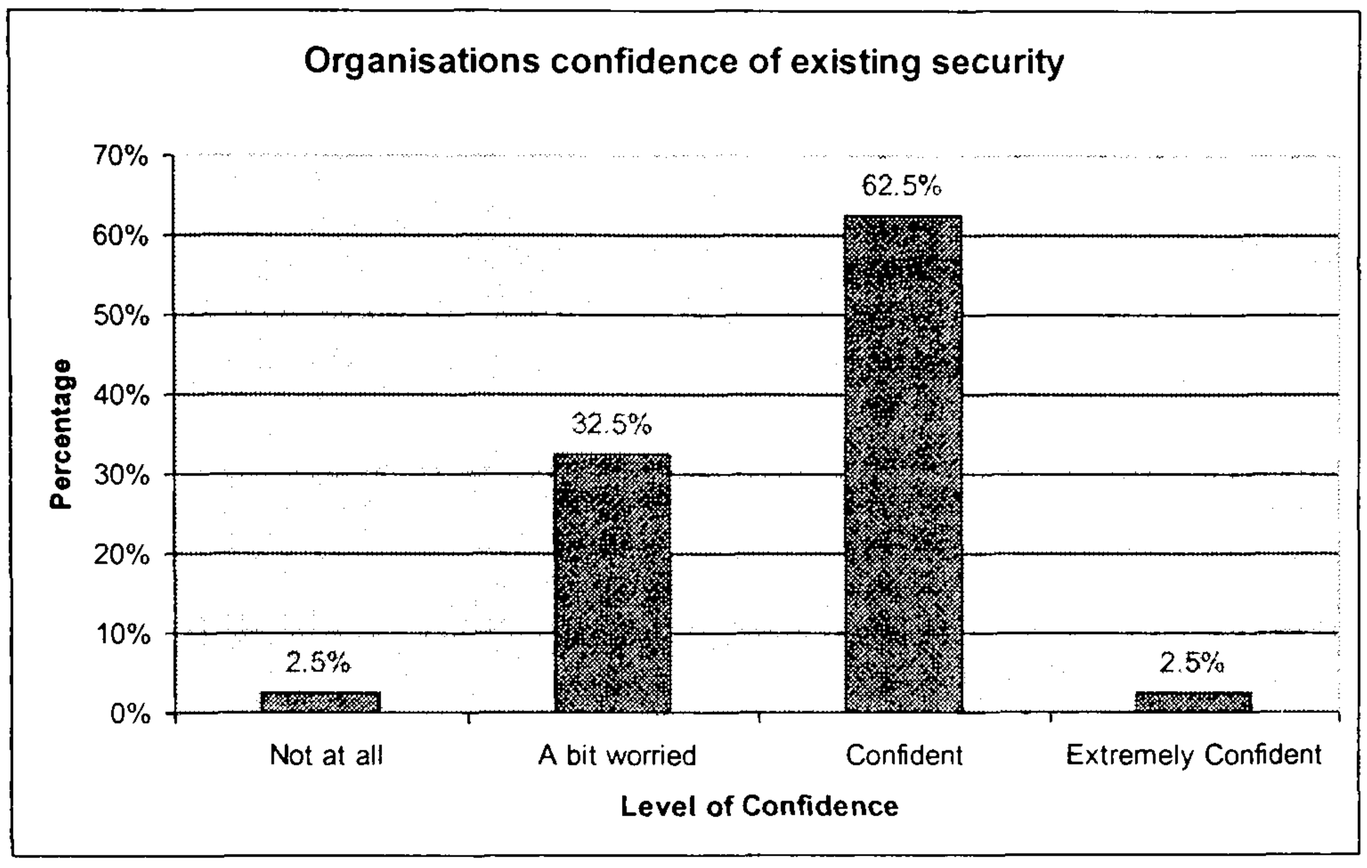


Figure 22: Respondents confidence in existing security (Europe & US)

Furthermore, if one considers the data Figure 23 illustrates on the position of respondents within the SME, the lack of managerial awareness is evident.

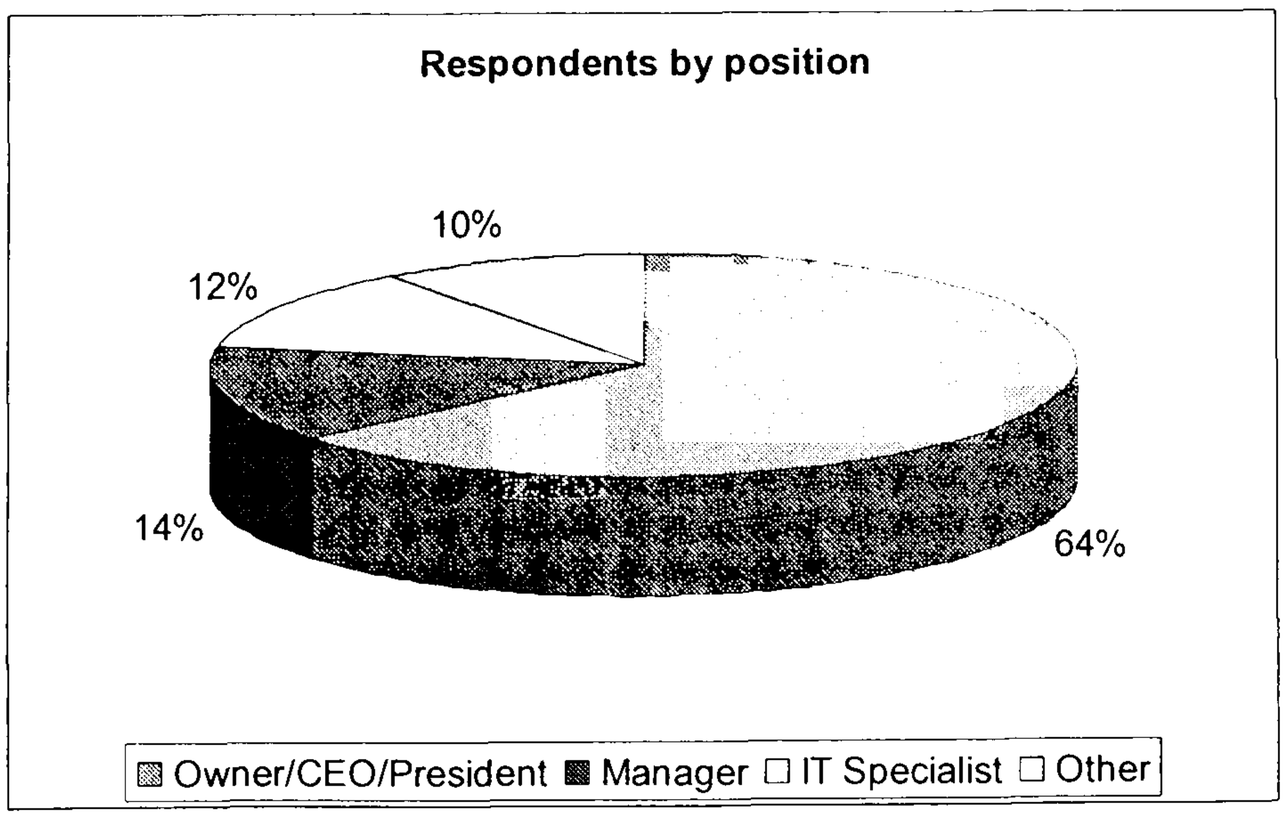


Figure 23: Respondents function within the organisation

Establishing that the lack of security awareness is on the SMEs management (and not simply between employees) is a significant concern. With the management being confident of the existing security which is in fact inappropriate, it is unlikely they will be willing to invest more on security evaluation, design or controls, leaving this way the organisation exposed to the large number of threats out there. This makes the need for an SME RA tool to include some method of raising the managements awareness, (i.e. illustrate that threats do exist, the level of threat the organisation is under and the potential losses due to these, all in simple terms since it is the management it needs to address) an essential addition.

3.4 SME risk analysis methodology requirements

This section will discuss the requirements of SMEs from a risk assessment methodology as they were identified firstly from within surveys findings and then as SMEs have stated for themselves.

3.4.1 Requirements identified from surveys

Looking at the characteristics of SMEs, they require a RA methodology which will take the place of a full time security expert they lack and assist in raising awareness and manage risks. Based on these SME characteristics, the requirements of SMEs from this RA methodology have been established. More specifically:

- Lack of Funds. This characteristic of SMEs not only necessitates for the RA methodology not to be costly, but it should also consider the cost of the controls to be implemented and offer the best possible choices that the SME budget can afford, reducing risks as much as possible.

- Lack of Expertise. With SMEs lacking a full-time security expert, such a solution is required to be simple to use, and provide as much assistance as possible to the user facilitating both in the selections as well as in the implementation and configuration issues. Furthermore it is required to provide the SME with the potential to re-address the situation after the initial RA, should threats have not been addressed properly or new assets introduced, therefore assist not only in the selection of controls but also in their further management.

- Poor Selection of Controls. The RA methodology aimed at SMEs should either automatically suggest or provide sufficient information to enable users to select the best controls possible based on their organisations security requirements and assets.

- Lack of Awareness. By providing the appropriate information, particularly in the output report, the RA methodology should assist in raising managerial awareness on threats and why considerations and funds should be devoted to manage them. The better IS issues are communicated to the management, the more likely it is that management will respond positively (Hall 2003).

- Disruption of operations. Because SMEs cannot afford the disruption of operations from a lengthy RA, this process aiming at SMEs should be as short as possible, requiring the input of a sole user who is informed on the organisations business functions and operation.

3.4.2 SMEs self-identified requirements

Having identified certain requirements for a new risk assessment tool which addresses the characteristics of SMEs, the next step is to use survey findings to establish what organisations themselves declare they require and see if it matches the requirements already identified. The SME security survey investigated specifically into this topic asking what is missing from RA. In this section, findings from other surveys are also discussed which are relevant to the issue and can be used to identify what organisations want to achieve better security and see which of these requirements can be included in an RA methodology. To start from the basic requirements, as the authors SME security survey found when queried the users 'how much they would be willing to spend for purchasing an RA tool if they were completely convinced it would solve their security problems' (Figure 24).

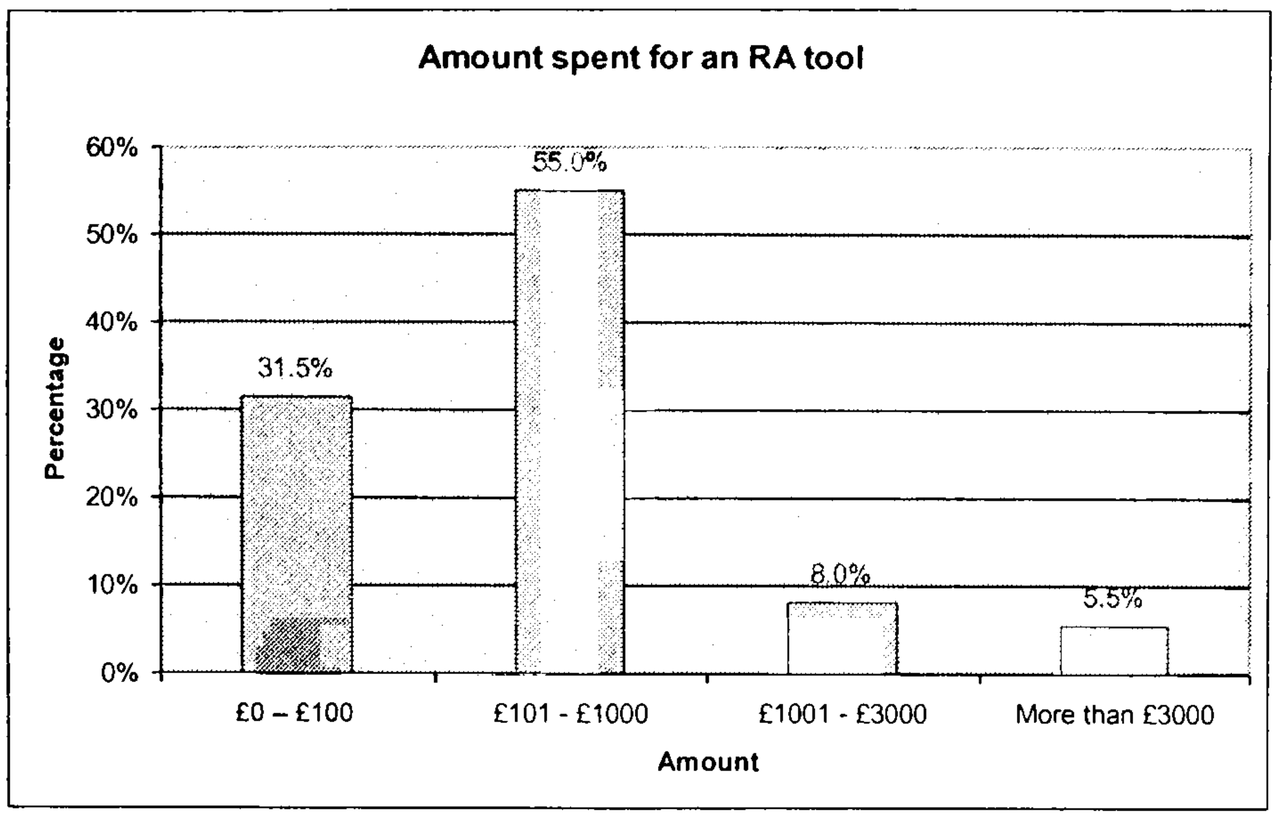


Figure 24: Amount organisations are willing to spend for an RA tool

This data illustrates a massive (86.5%) first requirement of SMEs for an RA tool to cost less than £1000. Even though this is not relevant for the development of the methodology by this research, it needs to be considered when evaluating the reasons for the non-adoption of the existing commercially available RA tools in the following chapter.

Figure 25 illustrates what organisations from Europe identified, as the elements of current RA that makes it prohibiting for SMEs.

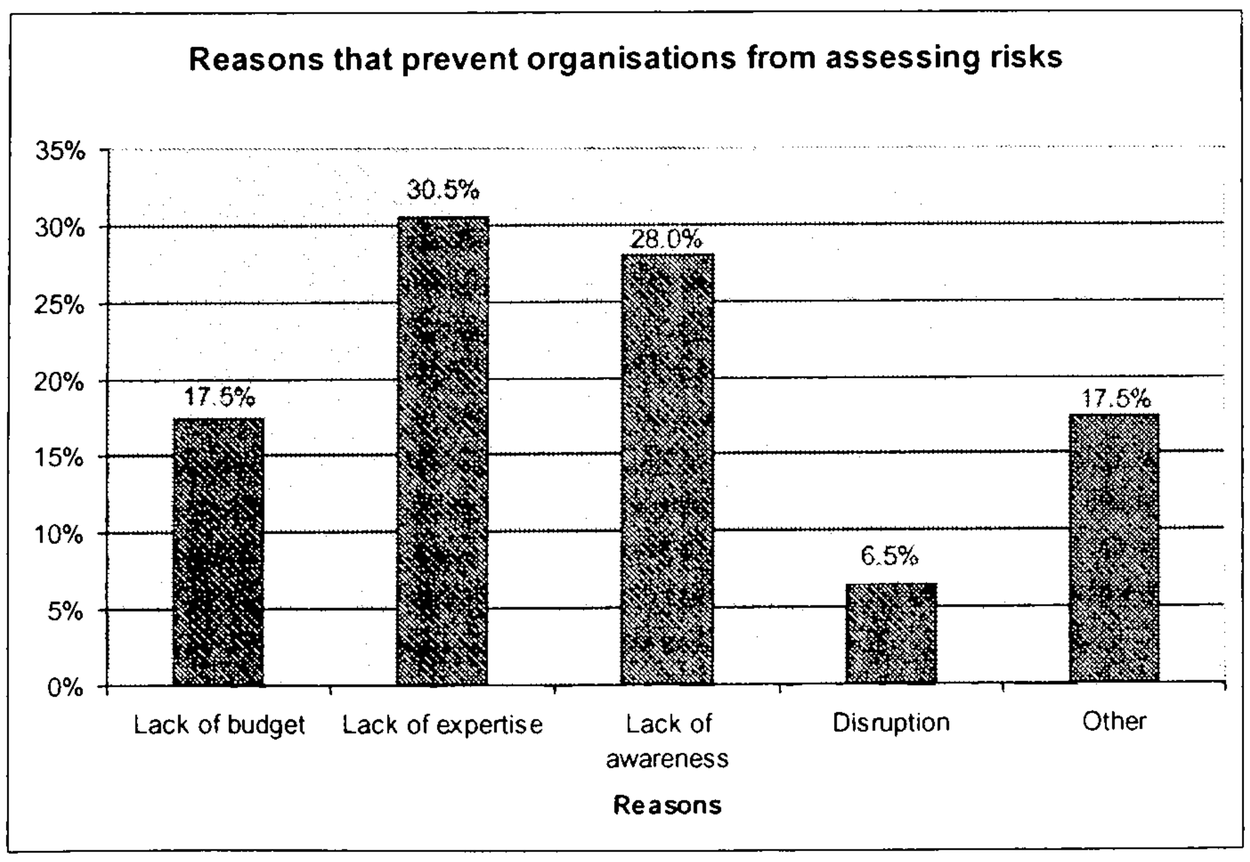


Figure 25: What stops SMEs from performing RA

The biggest concern of the organisations (30%) was the lack of expertise, an issue which as discussed earlier causes a lot of the other problems as well. Then there was the lack of awareness, suggesting that SMEs are not aware of the importance and assistance that a RA can provide them with securing their organisation efficiently and avoiding unwanted incidents. Lack of budget came third on the list with 17.5% of the respondents having chosen it. Finally 6.5% (interestingly all out of the 'less than 20 employees' sample) declared that performing an RA is a disruption to their activities. It is worth noting that none of the organisations occupying between 20 to 250 employees said disruption therefore confirms that the larger the organisation gets, the most likely it has the ability to assign this task to one person for a couple of days. Finally, from the organisations that selected 'other' we required that they state what they meant in an attempt to identify other reasons that were overlooked until now. However the responses strengthened the belief that there is a large lack of I.T. security education and awareness within the SMEs. To illustrate what is meant here, a typical example - response was "only a few computers connect to the internet so there is no risk".

The findings from the ACCSS are quite illustrative on the requirements of organisations as far as I.S. security is concerned. According to the survey, the most significant concern of organisations as far as information security management is concerned is changing personnel/users attitude and behaviour regarding information security. There is not much that this particular research can do on this, but RA is not completely irrelevant to this task. In order to achieve better personnel attitudes towards security, a number of things

need to be done such as policy, training, awareness initiatives, disciplinary processes etc. An RA tool cannot create all these, but can however inform the user and the management of the need to do them. The second biggest concern however is configuration management, which is one of the elements previously identified as missing from an RA methodology which aims at SMEs. Then there are the concerns about keeping up to date with threats and solutions, issues which from an RA perspective have to do with efficient support and feedback. Major concerns to organisations are 'getting more support from the management in addressing I.S. issues' and 'Lack of management understanding in I.S. issues' both discussed when proposing that an RA tool for SMEs should produce comprehensive results to the management including financial elements which justify spending, so as to ensure that the management is encouraged to invest effort and funds towards security.

A percentage of the respondents do state that they find 'applying risk management principles' a problematic area, this is inherently linked with the requirement of SMEs for a tool which is easy to use and gives comprehensive results. Furthermore, the DTI survey, investigated a similar issue asking their respondents what would help businesses manage their risks. A large number of the respondents (second biggest issue after 'more education for the general public about I.S. risks' which is not related with RA) stated they required the provision of more information security advice or information, once again leading us to the issue that organisations would require from an RA tool to present them with a useful, comprehensive output which will also provide them with information on the issues. The rest of the issues that organisations stated they want are related to more

standards and industry initiatives, which again do not correspond to what an RA tool can do for an organisation (it can however inform them of the standards they are meant to be implementing, according to their industry sector, in case they are not aware). Finally from the same survey there was a question on how businesses decide what to spend on security. The two issues that came first, with an equal 45% of the respondents, were 'Formal business case' and 'Quantify the benefits'. Both these issues are in line with the discussion made previously about a risk assessment tool for SMEs needing to present users with financial elements such as the ROI (ROI being the third and last source organisations stated they rely upon to decide spending on security) offered by selected controls, and ALE by threats, and generally not making the process too technical for the management that decides what funds are invested.

3.5 Conclusions

By looking into the characteristics of SMEs, the following were identified as the requirements that any solution which attempts to address their security needs should address:

- Because of the lack of security expertise within SMEs, such a solution should be easy to use, therefore avoiding as much as possible the need for the user who performs the RA to have technical knowledge
- The process of performing a basic assessment of a SMEs' security should not be lengthy, certainly not span over a period of a day.

- Such a tool should allow a single user with some knowledge of the organisations operation, to be able to perform an assessment (i.e. not require a group input).
- The assessment should yield financial data, comprehensive to the management (including ROI and ALE) to justify spending and help choosing controls efficiently (Hamilton 2002).
- SMEs require as much possible assistance in the selection of the appropriate controls especially because the person performing the assessment is likely not to be security educated.
- For the same reason, SMEs would require certain assistance in the setting up and configuration of the selected controls.
- Because of the lack of internal expertise to constantly monitor efficiency of countermeasures and alter the controls, it would be useful to SMEs for such a tool to provide with feedback on the effectiveness of the selected controls and update features. In order not to constitute a disruption to the users activities this functionality should allow users to report incidents and update the assets list without needing to perform the entire RA process from the beginning. When discussing the "effectiveness" of controls, the metric is statistical data (such as the frequency by which a security event keeps occurring even though a control has been implemented to address it) and not precise figures.

Having identified the elements that a solution should have for the requirements of SMEs, the next step is to proceed into investigating the existing solutions, using these requirements as the criteria to discover the reasons why these solutions have not been

adopted by SMEs. After evaluating the existing solutions, therefore establishing in practice why SMEs do not use them, the requirements for a new methodology that overcomes the setbacks can be formulated.

4 Evaluation of Existing Solutions for SMEs

Having established that RA is not being used by SMEs and what the requirements of SMEs from an RA tool would be, this chapter presents a practical evaluation of the existing solutions, focusing on RA tools for SMEs to establish whether the hypothesis that the existing solutions do not address the requirements of SMEs (therefore for this reason they are not being adopted) is correct. A preliminary version of the evaluation of existing RA tools, including two of the three SME RA tools evaluated here, has been published by the author in 2004 (Dimopoulos et al., 2004b).

4.1 Purpose of this chapter

Chapter 2 established that performing a proper RA is the primary practice that organisations should follow when planning their security. Chapter 3 then identified those characteristics that SMEs require from a solution designed to assist them with this task. In both these chapters the finding was that SMEs in general neither employ RA nor any of the other existing solutions. This section starts by giving a brief analysis of each of the other solutions available and will establish whether they are appropriate, leading to a proper evaluation of RA tools. The purpose of this chapter is to investigate, not the '**if**' but the '**why**' these solutions are not being used. In this chapter, all existing solutions shall be evaluated using as criteria the characteristics identified as required for a solution that addresses SMEs in chapter 3. Therefore there are three goals to this evaluation:

- Establish how existing solutions cope with the requirements of SMEs therefore if this is the reason they are not being adopted.

- Gain Practical knowledge of the existing solutions and particularly of automated RA solutions.
- Identify certain characteristics of existing RA solutions that are positive and not related with the setbacks and which should be included in a future methodology.

4.2 Evaluation of the existing solutions

There are two basic paths SMEs can follow to achieve security if they do not perform an RA, the first is outsourcing security and the second is following documented procedures like standards, guidelines and checklists. While there is essentially only one approach to the first (i.e. an organisation hires external expertise to set up and support everything and ideally they rarely have to worry about I.S. issues again) the latter can take many forms which are described in this section.

4.2.1 Outsourcing

A number of I.S. elements can be outsourced, from personnel training, to policy development and the actual practical securing of a network (Corby 2003). However, this solution is not preferable for SMEs because of the associated cost. However, since it is an option, it will briefly be discussed in this section.

- Description

  As described in the second chapter, this solution involves hiring expertise from outside the organisation to organise and manage security.

- Advantages and disadvantages

  The advantage of such an approach is that if the organisation selects well-trained and professional outsiders to handle security they can provide excellent I.S. and support. However, the setbacks are the cost involved with hiring outside expertise and the fact that there is still no permanent I.T. security person within the organisation.

- Reasons for lack of adoption

  Outsourcing security is not being implemented by SMEs for the principal reason of their cost. This solution is also not appropriate for SMEs as they do not employ any full-time security-trained staff therefore an SME would be left with a I.S. system that no-one within the organisation can maintain or troubleshoot. The outside experts would need to be called upon each time a malfunction has occurred or some modification to the protected assets, introducing delays (that get more costly the more serious the problem is) and more costs. Outside experts can even be hired to create policies and recovery plans but they would not be there to keep track and monitor whether users are conforming to these. From these perspectives it would be better if SMEs could design and handle their I.S. themselves. The available options for SMEs wishing to do this are discussed in this chapter

4.3 Self – Assessment Solutions

The first set of options that are available for SMEs wishing to assess their security issues **themselves** has the form of documents that aim to provide guidance on security issues on a generic baseline level

4.3.1 Documented Procedures and their progressions

As the simplest form of this solution, there are a number of standards and guidelines available for SMEs wishing to assess security themselves. As Tanenbaum (1988) says: *"The nice thing about standards is that there are so many to choose from"*. This is the case for information security standards as well. This section will attempt to outline all these security solutions that can be listed under the 'standards' category, that are essentially documented procedures or instructions that guide organisations at a baseline level on how to 'orchestrate' and maintain security. The evaluation and comments are made after reading the standards and comparing them with the requirements of SMEs

The evaluation categories used in this section to analyse the characteristics and suitability of these solutions are: "Solution Content" which gives a brief description of what they include, then there is a portrayal of how these solutions can be used, followed by the "Advantages and Disadvantages" of each solution and finally the discussion of why they are not suitable for SMEs. The fact they are not being used has been established already in Chapter 2, now we are looking at why. Most importantly even if the solutions are ultimately deemed inappropriate for the case of SMEs, at the end of each evaluation certain good characteristics are identified as worth using in a new methodology.

4.3.2 Guidelines and Standards:

The solutions discussed here have the form of documents, essentially baseline security guidelines that are international standards or issued by local governments. Such solutions are ISO17799, ISO27001, N.I.S.T. SP800-12 and SP800-30

4.3.2.1 Solution Content

ISO 17799 (initially published in 2000, updated in 2002 and currently on version 2005) is the international standard for I.S. management (ISO17799 2005); it is 130 pages long and includes brief instructions for securing all areas of an I.T. infrastructure such as physical security, access control, communications management, personnel security and more. ISO27001 (ISO27001 2005) before becoming an international standard was initially published in 2002 as the second part of BS7799, the British Standard for IS management (BSI 2002). This standard is 44 pages long and focuses on the fact that organisations should create an information security management strategy and lists a comprehensive inventory of available I.S. controls and practices. However there is not much detail on how to perform the first or how to deploy the latter.

N.I.S.T SP800-12, also called "The N.I.S.T handbook" (N.I.S.T 1995) is the American equivalent of the international standard. N.I.S.T's contents are generally fairly similar to ISO's but it is structured differently and presents some more detail to the user on certain aspects since this standard is 290 pages long. Among its contents it explains what the threats to an I.T. system are, it gives some recommendations on some procedural issues (e.g. how to design I.T. security, write policies, promote awareness and security education) and also dedicates 20 pages on how to perform an RA. Finally the N.I.S.T.

handbook presents its own list of controls for I.T. systems, very similar to I.S.O and quite exhaustive on this issue. In 2002, N.I.S.T. released another publication which is also relevant to the issues investigated in this chapter. That was SP800-30, also known as "Risk Management Guide for Information Technology Systems" (Stoneburner et al., 2002). This local standard is 41 pages long and is essentially a more detailed version of chapter on RA found within the N.I.S.T. handbook. Both these publications focus on identifying assets, vulnerabilities and their likelihood of occurrence before proceeding to recommendations on how to mitigate risks.

4.3.2.2 Practical Implementation of Solution

Like any standard, both these are "Published specifications that establish a common language, and contain a technical specification or other precise criteria and are designed to be used consistently, as a rule, a guideline, or a definition" (ISO Standards Bookshop 2002). As such users can refer to them for guidance when designing security, however they will never adapt to the specific requirements of one organisation or help in selecting and setting up, configuring or maintaining any controls. I.S.O also comes with a quite costly ($995) 'toolkit' which essentially is a set of checklists that users can print and check what practices they have in place for some major security issues like virus protection and backup.

4.3.2.3 Advantages and disadvantages

- **Advantages:** N.I.S.T. publications are free which is preferable for SMEs, however the international standard is more detailed in the way it presents the controls (thus one could say that the N.I.S.T. standard is more 'introductory'). Both solutions are very methodical in the material they present. Being standards means that all possible I.S. objectives and controls are included within, therefore they are excellent for guidance, i.e. to ensure that organisations do not overlook certain issues,
- **Disadvantages:** They do require an expert to use them, not in the sense of the contents being complicated but because they only provide recommendations and best-practices which someone needs to adapt to the organisations' requirements, and also implement, configure and maintain the controls without any guidance provided.

4.3.2.5 Why they are not appropriate

This makes such standards very useful to security experts, as they may be used as a thorough reference when designing an I.T. system to make sure some controls have not been overlooked. However, they will not provide any assistance to someone with no I.T. security expertise as the recommendations for controls they provide will be meaningless without having a way to identify the specific assets the organisation should protect, and indicate what controls match to these and implement these selected controls.

4.3.2.6 Positive characteristics identified in solution

Because of the comprehensiveness of the security issues and practices within such guidelines, they can be used as reference to the methodology's databases to ensure issues are not neglected.

4.3.3 Progressions of guidelines and standards

Solutions like these could be described as a slight progression of the guidelines discussed above. They are produced by organisations involved in I.S. and they resemble self-assessments of security. Therefore they require user input to produce some result which makes them adopt more to the organisation than vague standards. Well known examples of such solutions are CobIT (ISACA 2000) and Octave (Alberts et al. 2001).

4.3.3.1 Solution Content

OCTAVE stands for Operationally Critical Threat, Asset, and Vulnerability Evaluation and proclaims to "define an approach to information security risk evaluations that is comprehensive, systematic, context driven, and self directed." CobIT stands for Control Objectives for Information and related Technology and is advertised to "provide good practices for the management of I.T. processes in a manageable and logical structure"

4.3.3.2 Practical Implementation of Solution

What OCTAVE essentially does is guide a team of business and I.T. people through a process of identifying and rating risks. The methodology provides with diagrams like the

one in Figure 26 which the team that performs the analysis can complete themselves this way identifying what risks relate to what assets

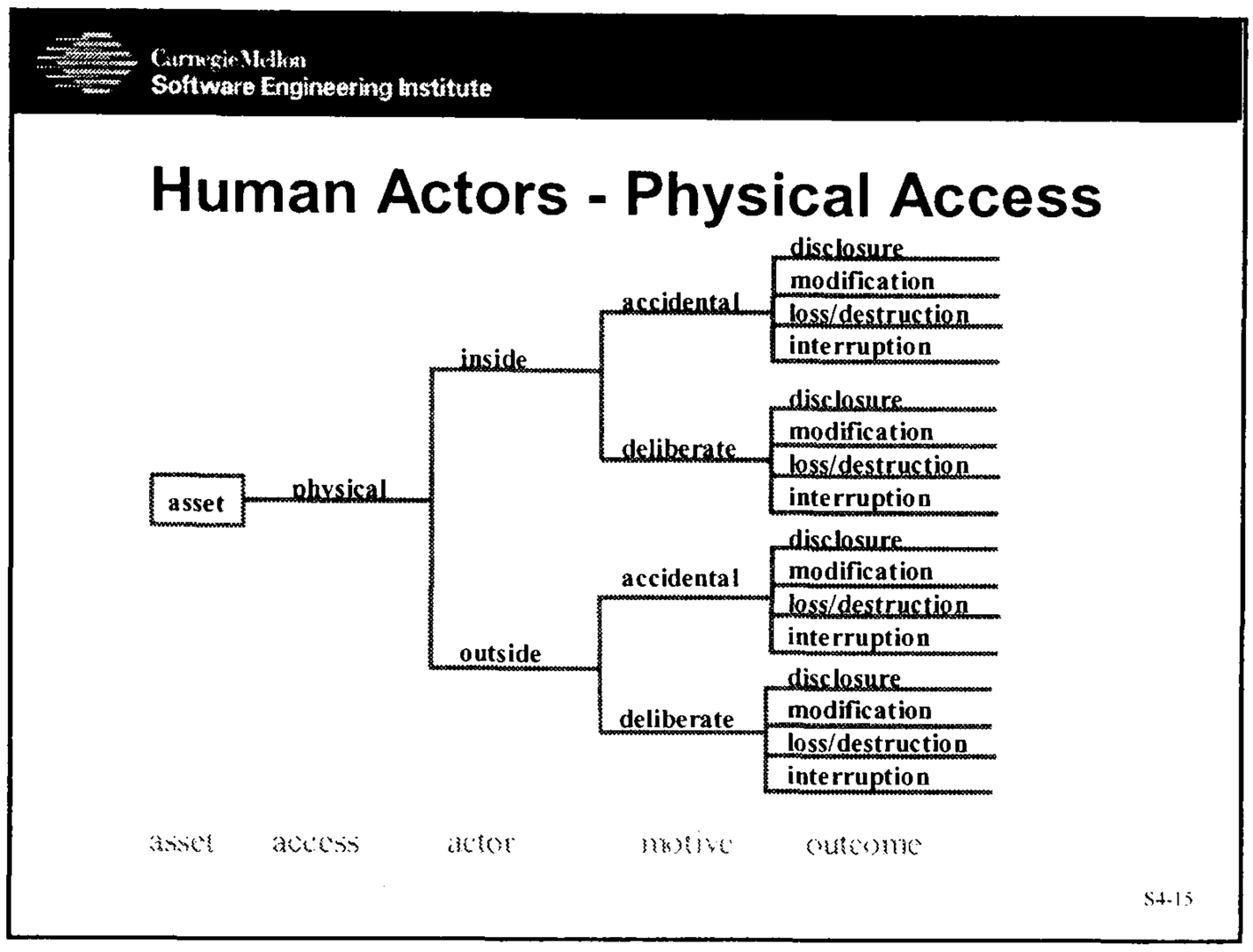


Figure 26: The OCTAVE risk self-assessment approach

Then the team is required to rate the impact of the risks that have been identified in a qualitative way i.e. as low, medium and high. Finally, they are given a list of security practices such as physical security, personnel security and I.T. security practices out of which the team needs to distinguish the ones they require and implement them.

The general idea behind CobIT's operation is very similar to that of OCTAVE, it uses a different way of identifying assets to the organization (which in this case are in the form of the organisations business functions) as illustrated in Figure 27.

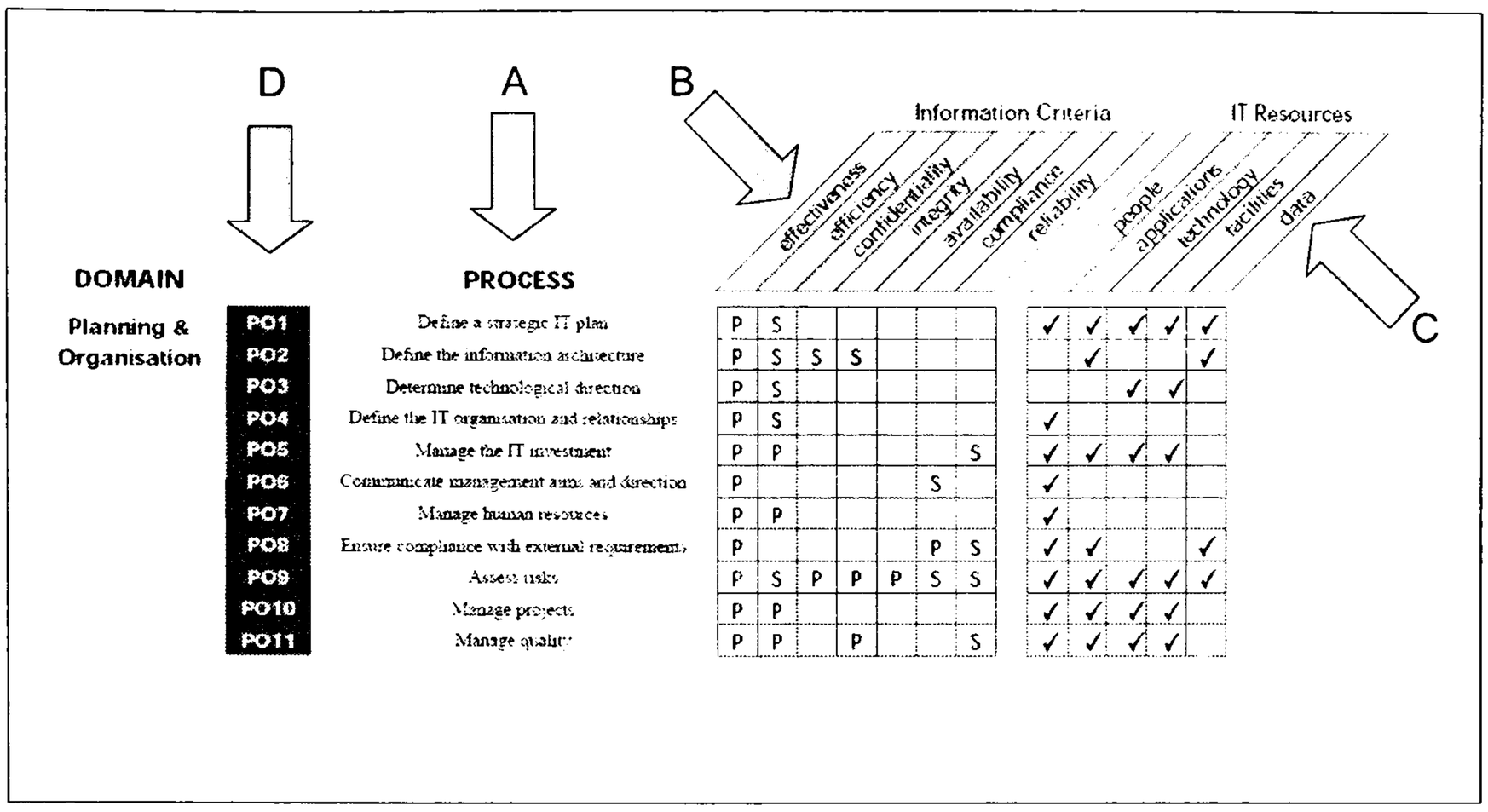


Figure 27: The operation of CobIT

More specifically, it presents the user or team of users with a list of business processes commonly found within organizations (A), then links each of these functions with certain criteria that define how significant this process is (B), and indicates what resources might be linked with this business function (C). Finally once the user has identified all the applicable functions, they can refer to another section indicated by the code (D) next to each function which lists all the controls that are relevant to this function.

4.3.3.2 Advantages and disadvantages

- **Advantages:** These are very well thought methods for identifying assets, their importance and risks towards them; however they require time and I.S. expertise. They are definitely a step forward from guidelines since the organisations can select from them assets and functions that correspond to them and therefore make the assessment more specific to the organisation than with guidelines.

- **Disadvantages:** OCTAVE requires a team of I.T. and business personnel to perform the task, the users still need to judge which controls are appropriate themselves from large lists, unless they apply all controls which would not be cost-effective, there are still no recommendations on how to select and implement countermeasures.

4.3.3.3 Why they are not appropriate

Not only do they require the same level of expertise as standards, but even greater as they need someone with good knowledge of the organisations' I.T. operations - making it very easy to overlook an area at risk if the user does not recognise it formulates an asset. At least standards are exhaustive.

4.3.3.4 Positive characteristics of solution

Compared to standards that are simply listings, these solutions point the way to identifying assets and linking them with relevant controls. In the case of SMEs they would however benefit from being automated to make the process shorter and to ensure that the assets are identified correctly and linked to the appropriate controls, as well as provide some assistance to the user on how this can be achieved. This exists in the form of the solutions described in the next part.

4.3.4 Automated guideline tools

A progression of the methodologies just described, these are websites that a user, informed on the organisations' operation, can provide with certain details and this way obtain recommendations on security practices that should be followed. A lot of providers might have similar approaches to this issue but here we will look at how three major organisations approach the issue. The three major solutions discussed in this part are: the Microsoft Security Guidance Centre (Microsoft 2006), the Symantec Information Assurance Risk Model (INFORM 2005) and the McAfee Security Planner (McAfee 2006).

4.3.4.1 Solution Content

Microsoft Security Guidance is a website offering certain online functions, tool downloads and support documents all related with identifying vulnerabilities, planning and implementing I.S.

McAfee Security planner for small and medium businesses is another web-based tool, which uses a graphical environment which claims to help organisations 'Identify their security risks and create a protection plan'

Symantec offers a solution with the same aims. However, INFORM does not advertise itself as being targeted at SMEs and actually requires a Symantec consultant to be hired by the organisation in need of the assessment in order to drive the tool.

4.3.4.2 Practical Implementation of Solution

The Microsoft solution aims at improving SME I.S. and involves a website which performs five basic operations. The first is that users can watch a video, illustrating seven steps small businesses need to do in order to achieve a secure environment. Secondly it provides online details on these seven steps and how to perform them. Essentially it provides generic baseline information of the type 'You should install an antivirus' and 'You should keep automatic updates on' together with some instructions on how to, also suggesting certain products and giving the links to other resources one can read on the issues, on seven major issues of I.S. security: protecting desktops and laptops, keeping data safe, using the internet safely, protecting the network, protecting servers, handling PCs from servers and securing applications. The third thing this website does to improve security is to provide a free download of the computer security guide for small businesses, a relatively short guide (62 pages) to I.S. which gives some recommendations on how to implement certain solutions (e.g. how to set-up a firewall) without however becoming too detailed or technical. The fourth function this website provides with is a tool called Microsoft Baseline Security Analyzer, which can be downloaded and installed to scan any number of computers within a network to detect a number of known vulnerabilities and misconfigurations related with windows systems, like administrative, SQL, II.S. vulnerabilities, weak passwords etc and report them to the user as illustrated in Figure 28.

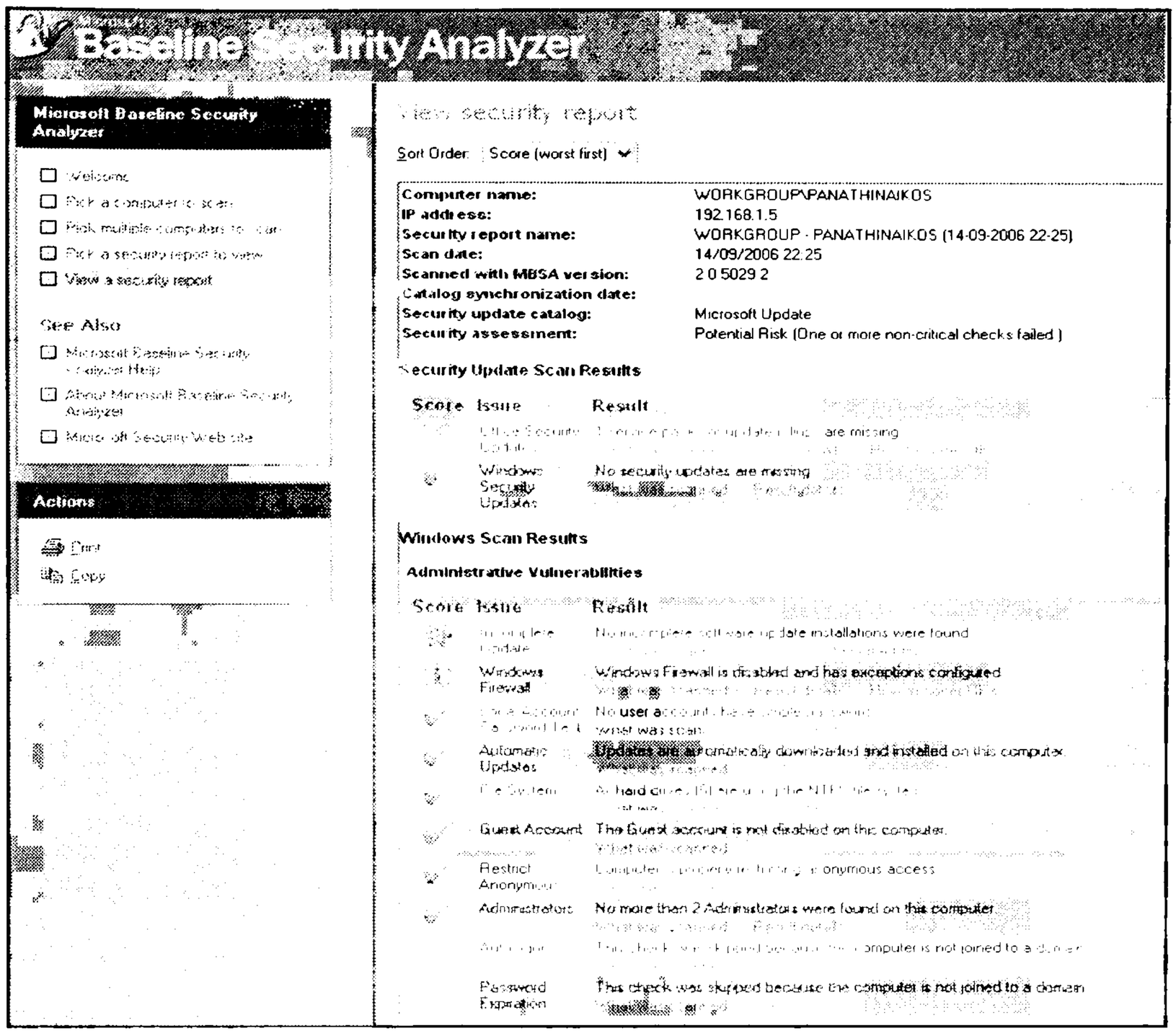


Figure 28: The vulnerability scanner included in the Microsoft solution

Finally the last function of this solution is that it provides a questionnaire which tests the users knowledge on some classic I.S. issues, such as password selection, and then for those that the user has responded to incorrectly the system redirects the user to the appropriate chapter in the 'seven steps checklist' mentioned previously.

The tool offered by McAfee requires the user to provide with some basic information on the organisation, mainly the number of employees, and whether certain specific types of servers exist (Email, File and Web). It basically creates a network plan based on the existence of desktop PCs, the three types of servers, the Internet and remote access, as illustrated in Figure 29.

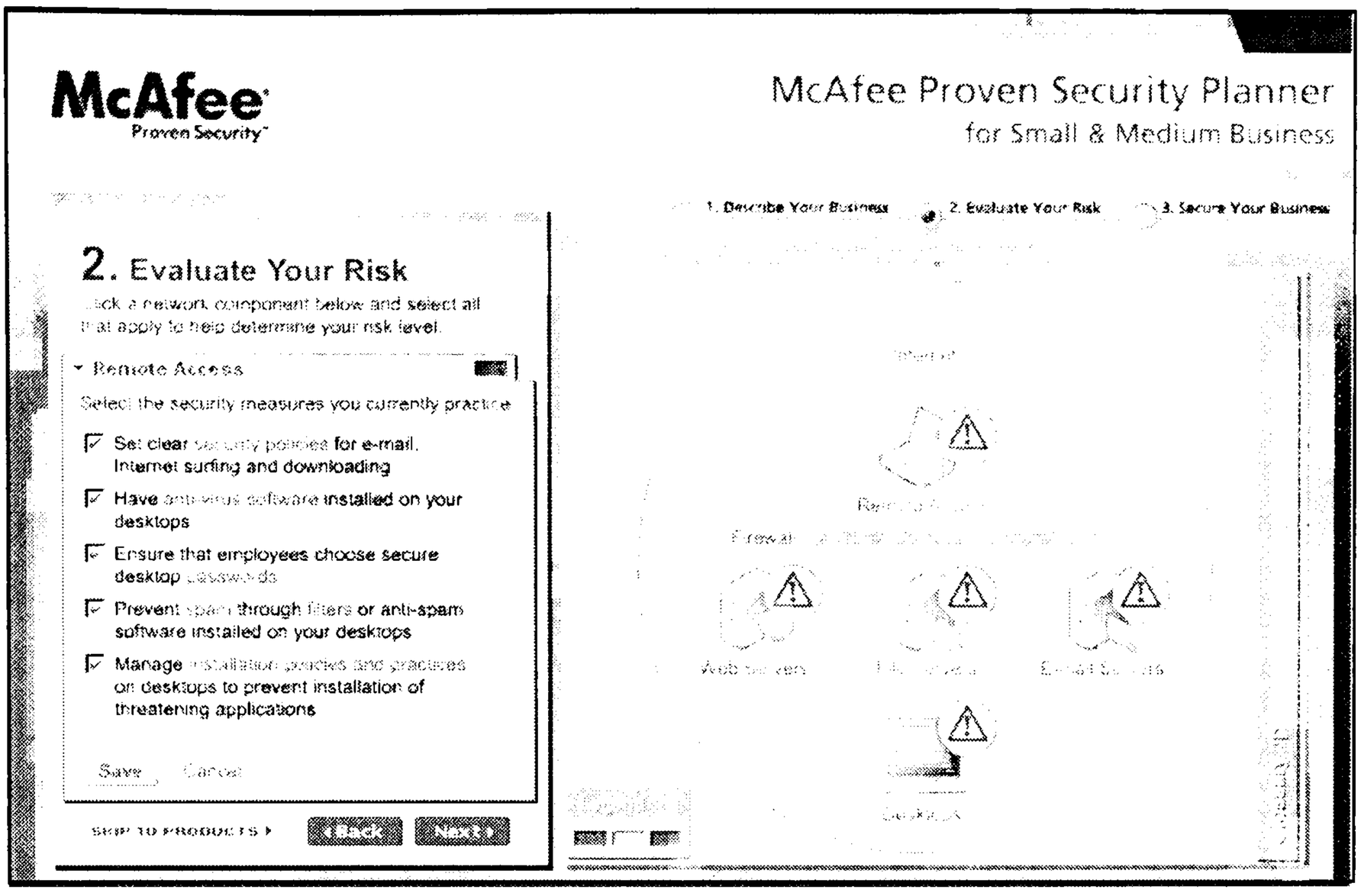


Figure 29: Assessing risks to servers with the McAfee security planner

The user is then required to select from a short list of security solutions that are in place for these assets. At the final stage the tool illustrates the risk that the network is exposed to, according to the selections of available controls, and recommends certain security solutions that are missing.

The Symantec INFORM solution is mainly concerned with the economics of I.T. security, therefore estimates risks according to the users input of estimated losses if a threat is realised against the identified business functions and information within the organisation. It then gives a comprehensive report from a business perspective (Figure 30). However, this has no use in terms of I.T. security countermeasure selection or implementation.

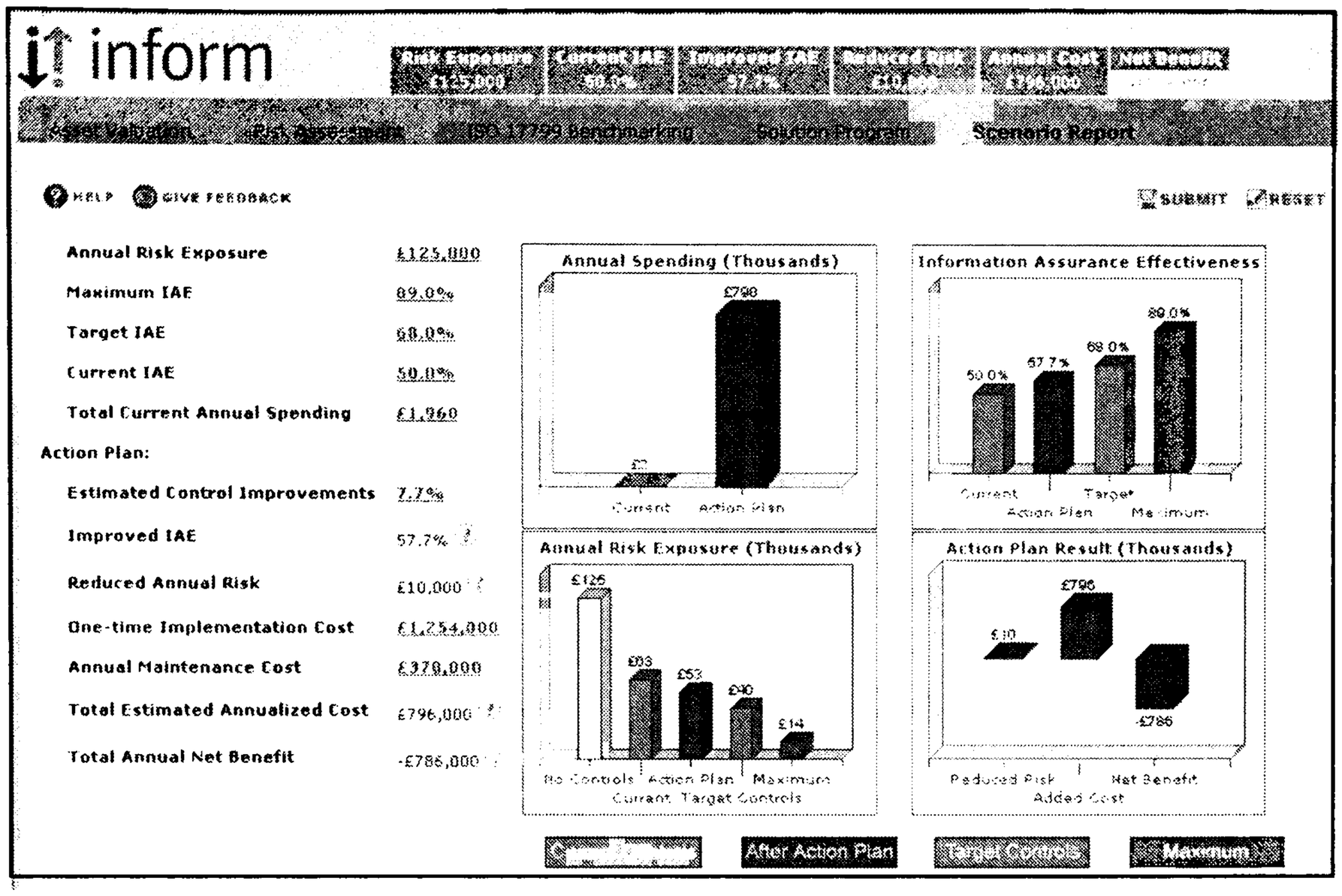


Figure 30: The output of INFORM

4.3.4.3 Advantages and Disadvantages

- **Advantages:** All these solutions address at I.S. from a business/business functions perspective, and all three processes are short. The Microsoft tool certainly would not do any harm as long as the user is a little bit security aware to know that they are far from safe just by following this 7 step checklist. They all do not require I.T. experts but mainly business people. With all of these tools, if run by a person with knowledge of the organisations business and I.T. functions, the process last less than a couple of hours.

- **Disadvantages:** They are all not detailed in how they profile the organisation and the selection of controls, especially McAfee mainly promotes their products. McAfee only assesses logical security of desktop PCs and three specific server

types. Microsoft only addresses Windows and makes it sound that if you have the Windows Firewall on you are safe. All three solutions aim to promote their own products and services. Microsoft promotes its O.S. and security features in it, McAfee promotes their security solution and Symantec hire their expertise and services to organisations needing such a solution.

4.3.4.4 Why they are not suitable for SMEs

Because they only provide guidance, not suitable for SMEs that do not employee security specialists, that would not be able to identify assets, risks and appropriate controls, even if they did choose some controls there is no guidance on how to implement them. Also, in all of these there is no consideration at all about the budget of the organization and what are the most cost effective control or solutions should the organization not be able to acquire them all. Also there is no help on how to implement and configure the solutions

4.3.4.5 Positive characteristics of solution

Even though these solutions are judged to be inappropriate to the distinctive environment of an SME, there has been a large effort on them by the parties that created them, therefore some elements they include should be good and worth identifying, keeping and adding to the requirements for a new methodology

4.4 Risk Analysis tools

One of the biggest concerns in I.S. is the need to assist the management and improve security decision making (Garrett 2004). Considering however the characteristics of the solutions in the previous section that make them inappropriate for SMEs, combined with the lack of expertise and security awareness within, SMEs need something to guide and assist them with making decisions when implementing security. Therefore what appears to be the best solution is an RA tool that is automated and should assist in the decisions process. Having identified why RA is often referred to as the first thing organisations should do to secure their I.T. systems, this section attempts to discuss the characteristics of existing RA tools that make them inappropriate to and not-adopted by SMEs.

4.4.1 Major RA tools

Certain RA tools, like CRAMM, are not meant to be for SMEs. However, since they are all commercial products (therefore there is nothing prohibiting an SME from using them) it is worth briefly mentioning the characteristics that limit its use to this type of organisations for this evaluation.

4.4.1.1 CRAMM

As discussed earlier CRAMM is the most well known RA solution and some times even obligatory to be used (e.g. for UK government organisations). Thus this section will discuss CRAMM as an indicative example of major RA solutions.

To start at the basic factor potentially prohibiting CRAMMs' use by SMEs, the cost of the tool plus the costs of the training seminars required by a selected person from the organisation is against the requirement of SMEs for a low-budget solution. The high cost of CRAMM is the main reason why it could not be purchased and evaluated for the purposes of this research. Instead a brief evaluation will be discussed here, based upon evidence from other publications but also on how CRAMM appears to operate and the results it provides based on a flash demo of the tool. Furthermore considering this person needs to leave their regular duties to undertake this training and perform the lengthy assessment (which includes meetings, interviews and structured questionnaires for data collection (Yazak 2002)) creates the deterring characteristic of disruption to the organisations (and this persons') normal operations.

By looking at CRAMM's analysis of threats (Figure 31), it does appear to be very detailed but at the same time it is evident that the information on the screen do require training to understand, particularly by the SME user. The analysis also appears to be quite lengthy since the screenshot only illustrates the risk analysis for a single threat and the list of selections required to be made by the user seems rather long.

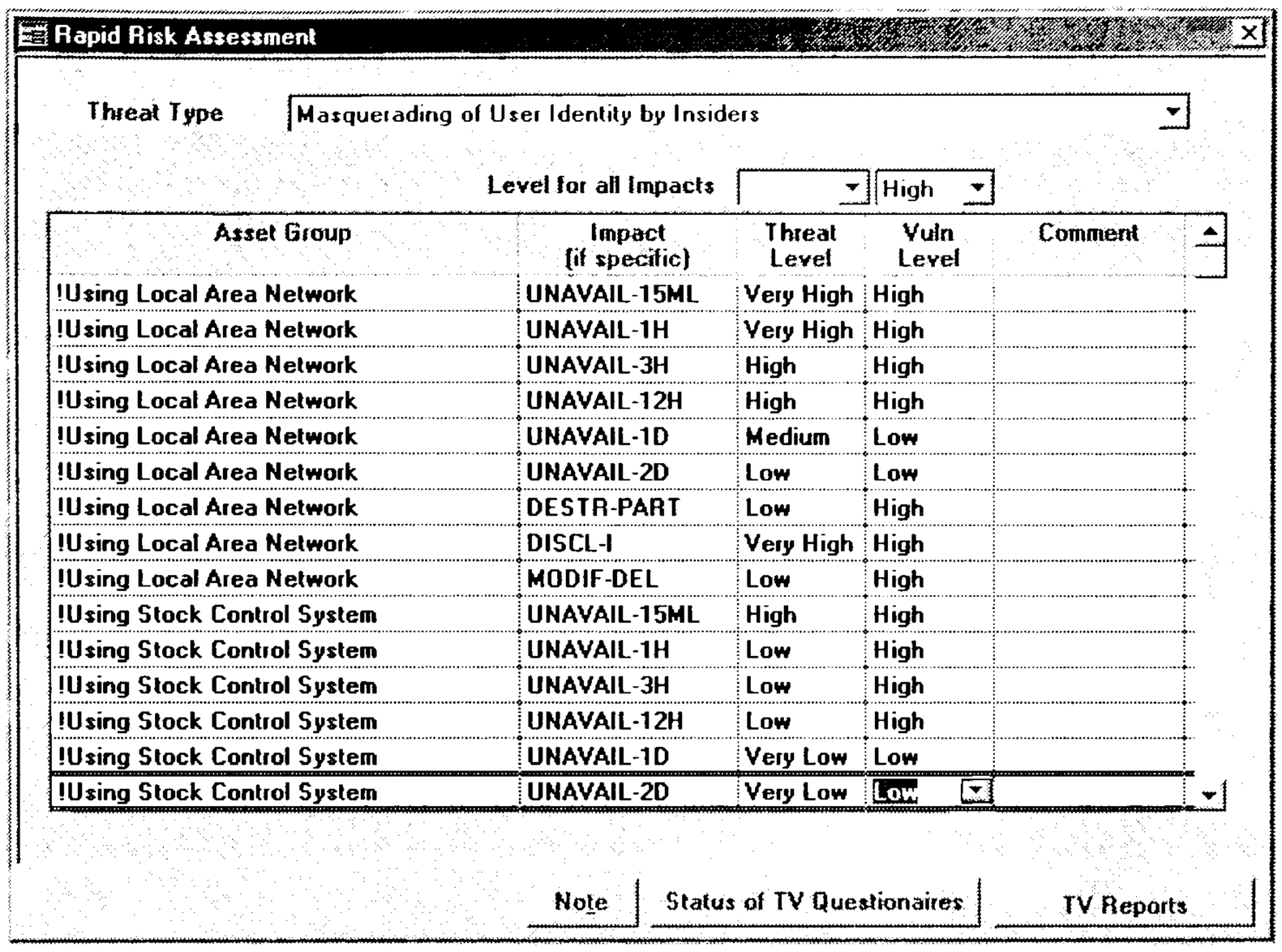


Figure 31: CRAMM analysis of threats

This confirms the reports that CRAMM is a lengthy process (GSSL 1997) and cannot be performed without the user having particular expertise and training (SANS 2002).

By looking at Figure 32 it is evident that the output of CRAMM is also not suitable for the SME user. Even though it, again, looks very exhaustive, there does not appear to be any details on what the controls actually are (to facilitate the users selections), or any assistance on how they can be acquired, deployed and maintained. The impression this output of CRAMM leaves is that only a trained user can interpret it, while an I.S. expert is required to obtain, implement and manage the solutions. This type of output would also not be of any use to the SME management who would not be able to interpret it in order to understand risks and justify security expenditure.

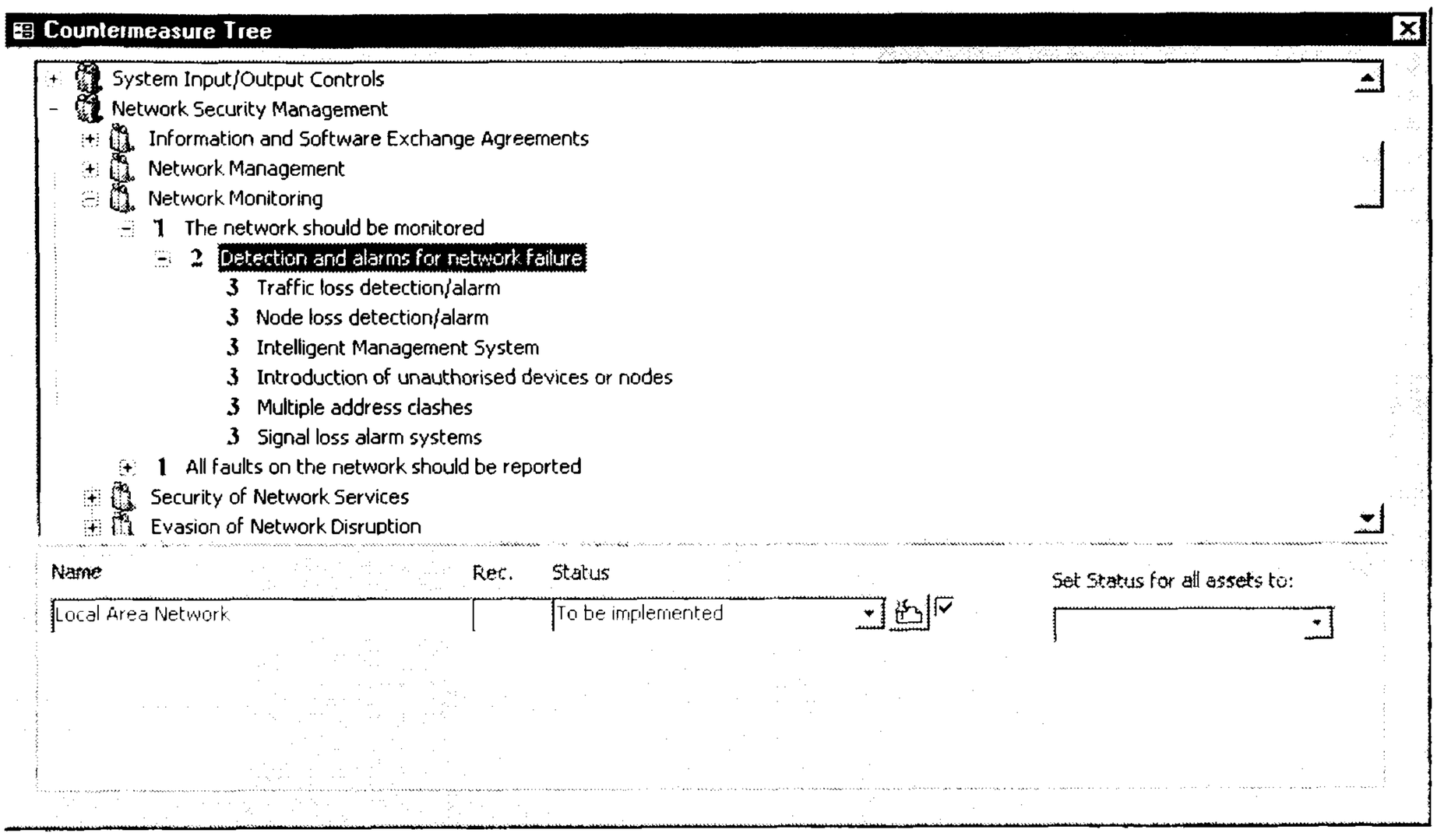


Figure 32: CRAMM recommended countermeasures

This strengthens the view that CRAMM requires particular expertise on the area of I.S. and risk analysis, as well as training on the specific tool in order to use it (Yazak 2002). Furthermore it coincides with other research findings that state the output of CRAMM is unnecessarily and prohibitingly lengthy (Labuschagne 1999).

Overall CRAMM appears to be inappropriate for SMEs as it does not match a number of their identified requirements. Since however it is unquestionably not designed (nor advertised) for use by SMEs, the next section will look at the appropriateness of RA solutions that are.

4.4.1.2 RA2 Art of Risk

Another major RA tool (at least in the sense that it is developed by BSI, the initial authors of ISO17799 and ISO27001 and offers compliance with these standards), which however again does not advertise to be designed for SMEs is RA2 Art of Risk (BSI 2006). A demo version of this software was acquired for the purposes of this research; its details will be discussed here as this tool too does not apply to SMEs. To begin with, a first factor that makes this tool inappropriate for SMEs is its cost which being £1300 is prohibiting for SMEs as discussed in Chapter 3. Overall RA2, is very systematic and analytical in the way it approaches the analysis of risks and selection of controls. At the start of the assessment, users are required to select the scales upon which they wish the asset and threat to be valuated on (users have the choice between a 3, 4 and 5 point scale) and can then proceed to the identification of assets and evaluation of assets. The user can select from a list of example assets and then values them in terms of Confidentiality, Integrity and Availability. Where the process itself starts being deterring for SMEs is when the threat identification takes place (Figure 33).

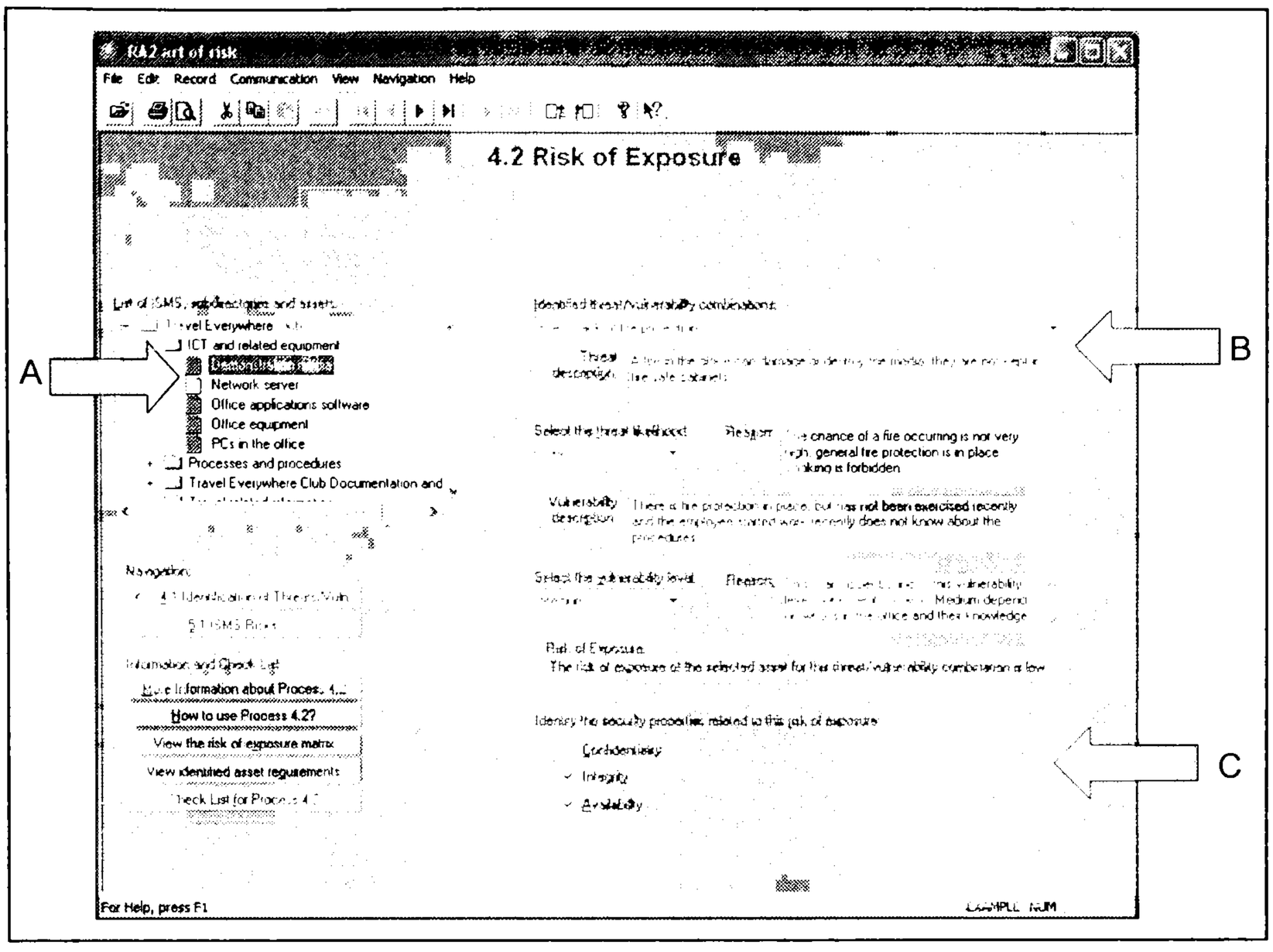


Figure 33: Calculation of Risk within RA2

More specifically, the users have to identify threats that apply to their assets themselves (Figure 33A) and they are also required to estimate the level and likelihood of the threat (Figure 33B). Finally, the users are required to know and select for themselves whether each threat has an effect upon the C-I-A of assets (Figure 33C). The next step in RA2 is the selection of controls (Figure 34), in this stage the user is presented with a thorough list of ISO27001 controls that are relevant to each existing threat and they need to select which ones they wish to implement.

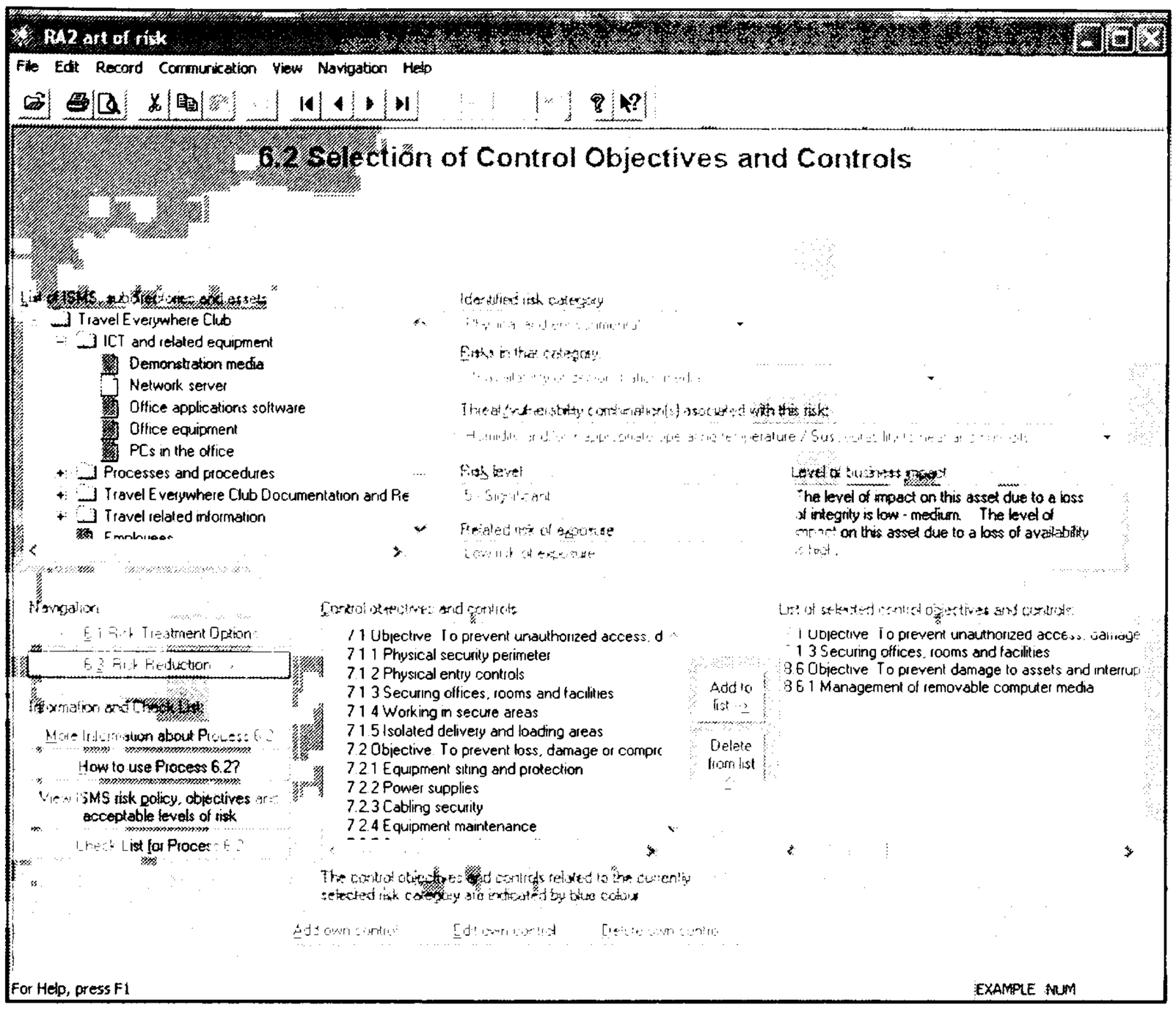


Figure 34: Selection of Controls in RA2

The final impression of RA2 is that it is a very detailed RA tool, containing a large database of threats and controls like the ISO standards. However, it is inappropriate for SMEs since it requires particular expertise to be able to identify and rate applicable threats and also select appropriate controls without any particular assistance. In its output, RA2 provides a 'gap analysis' of security controls that have been applied within the organisation being assessed and those available in the ISO standard. Again, thorough as it may be, this output is not particularly useful to SMEs as there is no assistance in acquiring, implementing and configuring controls. Therefore overall RA2 is a powerful RA tool but requires an expert in I.S. who also has very good knowledge of the organisation to use it (or a team of experts each from these fields). Leaving the use of the tool to someone else would produce inaccurate results and could easily disregard

important issues, making it inappropriate for SMEs that have been shown not to employ experts.

4.5 RA tools aimed at SMEs

Three established RA tools were identified as being advertised to be appropriate for SMEs, evaluation copies of these tools were obtained and they were used in this section to see whether they fulfil the requirements SMEs expect from a solution aiming to assist them with the analysis of assets and the management of risks. It was therefore possible to establish if this is the reason RA solutions are not popular with these organisations.

4.5.1 Evaluation Criteria

The requirements of SMEs from an I.T. security tool assessing risks have been generally discussed across this thesis this far. In this section however, they will be categorised and assigned marks to enable a proper evaluation of solutions. According to the characteristics of small and medium businesses, there were several criteria identified that a RA tool should encompass. These criteria were split into four categories for this evaluation, as illustrated in Table 4. There are elements a RA tool should have in **general** (i.e. these are marked after the whole procedure is finished) there are elements that should be presented to the user within the assessment **process**, there are certain elements that are necessary to be present at the **output** of a RA tool aimed at SMEs, and finally it should allow the user to perform certain actions after the assessment is finished, this way

providing with **support**. By splitting the criteria this way the evaluation is more structured, making the results straightforward to be compared.

Characteristics of SMEs	Evaluation Criteria			
	General	**Process**	**Output**	**Support**
Lack of Funding	Low cost	Help with selecting cost effective controls		
Lack of Expertise	Ease of use/specialty required,	User assistance during the process of the assessment	Assistance with setting up of the controls	
Lack of Managerial Awareness		Economic Elements such as ROI and ALE,	Comprehensive output reporting to the management	
Poor Selection of Controls		Assistance in choosing controls,		Feedback which allows corrections
Disruption	Length of process,		Output report not unnecessarily lengthy	Update and feedback not requiring re-running the process,

Table 4: How the evaluation criteria match the SME requirements

4.5.2 Rating the tools on criteria

The tools were evaluated on a five point scale that resembles a Guttman scale (O'Connor 2004). A Guttman scale was judged to be the most appropriate as it consists of a set of user defined items, ranked in order of importance relevant to what is being evaluated from the least extreme to the most extreme position (Arreola 2005). For example, a person scoring a "3" on a five item Guttmann scale will agree with items 1 to 3 and disagree with items 4, 5 (Trochim 2006). When performing an assessment using this scale, it is expected to select the list item which describes better what the evaluated items

characteristics are. Each of the list items is associated with a mark defined by the person that designed the list which corresponds to the score that the evaluated item will receive on that issue. In this case the aim is to determine a set of responses/criteria, equivalent to characteristics that a tool should have, which will range from good to bad that will have a mark associated with them which when added up altogether will give the overall mark for each category of characteristics, and eventually the overall mark for each tool. This will enable straightforward and comprehensive comparison when later evaluating the methodology and application designed and built for this research. Thus for each characteristic, a three point scale was determined with three possible elements, one which is good, one which is average, and one that is poor. The progression of the Guttman scale made here is that 'point fives' are allowed for scoring therefore the scale becomes a five point scale which will range from 1, 1.5, 2, 2.5, up to 3. The reason why halves were added in the scale is simple, among different tools there are different elements that can prevent it from getting full marks on one issue. This makes it impossible to set middle values that cover the whole range of tools and their characteristics. Setting the maximum, the middle and the minimum allows the scoring to be performed even if an element was not initially considered when developing the scale.

To illustrate this with a simple example from the assessment, in the characteristic of "Length of process" tools would score 1 if the process lasted more than a day and 2 if it lasted a few hours. Two of the tools achieved a 1.5 in this issue but each for different reasons. One because the process lasted a few hours but it should be run by several personnel (which might again last a few hours but it might last days if people are

unavailable) and the other because the process lasted a couple of hours but the assessment required that a user who does not have the appropriate knowledge might have to do some background research before responding on certain issues which could again make the process last for more than a day. It would be extremely difficult to research all the possible cases between the 2 and the 3 here and they could be numerous. Therefore it was judged that the results would be more realistic if a tool gathered .5 marks for a characteristic if, anything, prevents it from achieving full marks.

- **General.** This category of criteria includes elements that need be scored after the process has finished and the user has a complete idea of how the assessment worked and what the output was. These include:

  - *Cost*. The discussion in chapter 3 established that SMEs are not willing to spend more than a certain amount on a RA tool. The ratings on this characteristic are based on the SME survey responses on this issue.

Rating scheme: Cost			
Mark	1	2	3
Description	£3000+	£1000 -£2999	£0 - £999

  - *Ease of use* (expertise required). This criterion has to do with how easy the process is to use (meaning the required level of expertise from a user to perform an analysis), since SMEs require for a tool to enable a non-security expert.

Rating scheme: Ease of use			
Mark	1	2	3
Description	Whoever uses it needs expert training on the tool or the area	I.T. personnel can use it	Anyone with knowledge of the organisation can use it

- *Length of process*. How long did the process last? SMEs require a relatively short process, but we have seen in this chapter that solutions duration can range from less than an hour, (like the web-based tools described) to a few days (like the progressions of guidelines).

Rating scheme: Length of process			
Mark	1	2	3
Description	More than a day	Within a day	Less than an hour

- **Process.** This category refers to elements that SMEs require from an RA methodology which are apparent to the person conducting the assessment during the actual process.

- *Assistance to user* during the process of the assessment. This refers to how much the developers have considered that there exists sufficient assistance to the person conducting the assessment during the process either by

manuals or with help menus within the tool (such as glossaries and help icons) to assist the users with their selections with issues like what should be done next or terminology issues.

Rating scheme: Assistance to user			
Mark	1	2	3
Description	Neither	In the tool or with documents (only one of the two)	Within the tool and with documents

- *Risk Impact Analysis*. This characteristic refers to whether there is functionality in the tool to quantify the impact of a threat being realised, and therefore rate the importance of specific assets (by evaluating cost of asset, impact of downtime etc) so as to later assess them. This element is essential for an SME RA tool so as to assist with raising managerial awareness as described in Chapter 3.

Rating scheme: Risk Impact Analysis			
Mark	1	2	3
Description	Solutions are chosen without considering the importance of assets at all	Cost of assets or impact of breach of the assets is considered	Both cost of assets as well as impact of breach of the assets are considered

- *Assistance in selecting controls*. A common element noticed during the evaluation of the previous solutions is that controls were presented to the users in the form of lists including all the potential controls for each asset

or business function. An SME with no expert to judge and select which are appropriate requires from an RA tool as much assistance in selecting relevant controls as possible.

Rating scheme: Assistance in selecting controls			
Mark	1	2	3
Description	All controls are the same	There exist some way of suggesting some controls more than others	Application suggests controls in a clear manner based on the results or the risks analysis

- *Cost-effective controls*. Having identified and valued assets, does the tool provide any assistance with selecting cost effective countermeasures for example if the ROI offered by security solutions considered so that organisations avoid investing larger amounts on one asset than its actual value while at the same time neglecting other assets that might cause greater losses if compromised.

Rating scheme: Cost-effective controls			
Mark	1	2	3
Description	No consideration of cost effective solutions	Cost of controls or value of assets considered	Cost of controls & value of assets considered

- **Output.** This category refers to elements which should be included in the output provided by the tool to match SME requirements (i.e. a report with appropriate details

for the management, and assistance to the person who will then handle the implementation of the controls).

- *Comprehensive output*. An RA tool designed to match SMEs should produce a report that is comprehensive to an end-user who is not an expert on the risk assessment area and potentially neither an I.T. security practitioner. For this characteristic, RA tools shall be rated in terms of how much expertise is required to interpret the results.

Rating scheme: Comprehensive output			
Mark	1	2	3
Description	RA or I.S. expert	I.T. security staff	Anyone

- *Deployment assistance*. Not employing security experts, SMEs require not just a list of applicable controls (no matter how well-thought this list is) they also require as much possible assistance on how to set-up and configure these controls.

Rating scheme: Deployment assistance			
Mark	1	2	3
Description	None	Some assistance and guidance	Detailed instructions fully relevant to the identified required controls

- *Length of report*. The output report should not be unnecessarily lengthy but should still provide the necessary information. This helps to avoid intimidating the aforementioned parties (management and users) by providing too much detail causing unnecessary disruption to their normal tasks. At the same time it has been seen, from the papers on CRAMM discussed in chapter 2, that a quite large size of the report is always seen as a disadvantage.

Rating scheme: Length of report			
Mark	1	2	3
Description	A lot of the data is useless to the end user	Includes some data which would not be necessary	Only enough for the relevant data

- **Support.** What this category of criteria is concerned with, is what potential a tool has for future re-usability by the organisation, and what support it can provide to the SME after the RA process is finished. Essentially it concerns whether the elements of feedback and update are present.

  - *Dynamic Feedback*. For a number of reasons (such as the fact that without a security expert if the controls selected in the assessment are proved insufficient and threats keep occurring) there will be no-one to correct the situation and the organisation will then need to start looking for another solution once again. An RA tool for SMEs should allow SMEs to perform two operations: firstly report if there are still issues after having implemented the controls, and secondly to allow

reporting of assets added or removed. This would cause a re-assessment of the situation and provide with security recommendations according to the new structure without leaving assets unprotected until a new assessment is performed or a threat occurrence exposes that something should have been done when the asset was initially introduced.

Rating scheme: Dynamic feedback			
Mark	1	2	3
Description	Non-existent	User is required to re-run the application	Dynamic Feedback (including reporting breaches and changes in assets)

- Dynamic update. This refers to the actual updating of the tool to keep up to date with new threats discovered and controls. Therefore eliminating the need for an SME without a full-time expert to be on a constant lookout to keep up with new threats and technologies. Surveys discussed in Chapter 3 indicate that this is one of the most major concerns of the management. It would be useful to update with new threats-controls and re-assess the situation without re-running the whole process. That is where the dynamic refers to.

Rating scheme: Dynamic update			
Mark	1	2	3
Description	Non-existent	Updating by the organisation and need to acquire the new version	Dynamic update

4.6 Evaluated Tools

For the purposes of this assessment three tools were chosen and evaluated on the aforementioned criteria. These are three of the most well known RA solutions tools, which were chosen because they are advertised to be appropriate for SMEs. Furthermore, the three tools approach RA in three diverse ways, both in the way they collect information as well as in the manner they suggest controls, which makes this evaluation cover a wide section of the RA sector. The tools are:

- Cobra Security Risk Analysis & Assessment, created by C&A Systems Security Ltd (http://www.riskworld.net/)
- The Buddy System, created by Countermeasures Corporation, (www.buddysystem.net)
- Microsoft MRSAT Microsoft Security Risk Self-Assessment (https://www.securityguidance.com/v1/default.htm)

The results of the evaluation are presented to the user in the following format: First some general discussion on each tool, then a description of how the tool operates and how it approaches the assessment split in two parts (how it analyses the risks and how it manages the identified situation), followed by the actual results of the evaluation. Finally, summarising the most significant points, there is a discussion on the advantages and disadvantages of each tool and a conclusion on each of the tools. Giving the users a taste of how commercial RA tools generally operate is particularly useful for when discussing the tool developed later on for the purposes of this research.

4.6.1 MRSAT

MRSAT is a solution offered by Microsoft, available for download for free on the Internet, and promoted as being designed for SMEs.

4.6.1.1 Operation: Risk Analysis

This tool gathers information on the organisation by requiring the user to choose details by replying to 'yes' or 'no' questions (Figure 35, C) the details on six different aspects of the organisation (Figure 35, A). That is: Basic information (such as the size and the number of PCs and servers); Infrastructure security (e.g. if the company is connected to the Internet and for what services does it need to interact with users and partners via the Internet); Application security (a section basically concerned with whether the organisation develops applications, what privileges from an I.T. perspective does it allow to those who develop applications for the organisation and who has access to data); Operations security (essentially if critical data is stored and what reliance third parties have on data which is stored within the organisation); People security (On what criteria and who introduces new technologies in the infrastructure and who has access to data); Environment security (number of employees and effect of theft and fraud). A significant element is that the questions are not technical and in case the user still finds it complicated there is a help pop-up (Figure 35, D) which gives some more detail on the question.

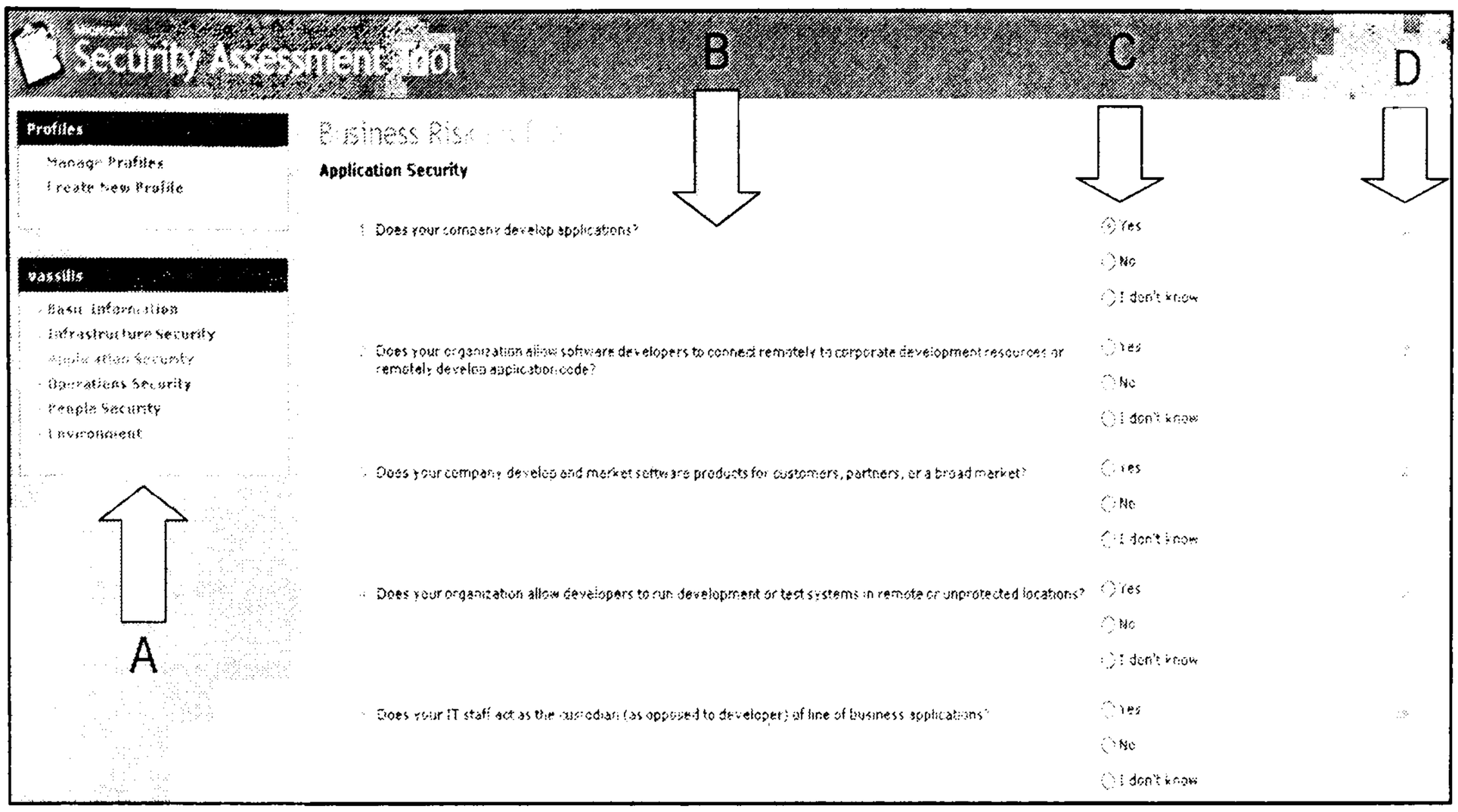


Figure 35: Using MRSAT to describe the organisations I.T.- based operations

Having described some of the organisations functions in this part, the tool proceeds to the second part of the analysis which is concerned with what security practices are employed within the organisation. This second part has the same layout as the first, this section uses again 'yes' or 'no' answers to assess existing security practices on the same six aspects described earlier. These include all the major security practices, such as use of controls (eg antivirus, IDS, firewalls), policies, operational plans and procedures, testing of solutions, I.S. training, backups and employment of I.T. security personnel

.

4.6.1.2 Risk Management

Having completed the analysis of the organisation's operation and security practices, the next step is to produce the results. MRSAT presents the user with three different outputs. First of all there is the 'summary report' which essentially is a, not so comprehensive,

graph illustrating the risk the organisation is under. Figure 36 presents this graph together with all the data provided by the tool to help the user interpret what it means.

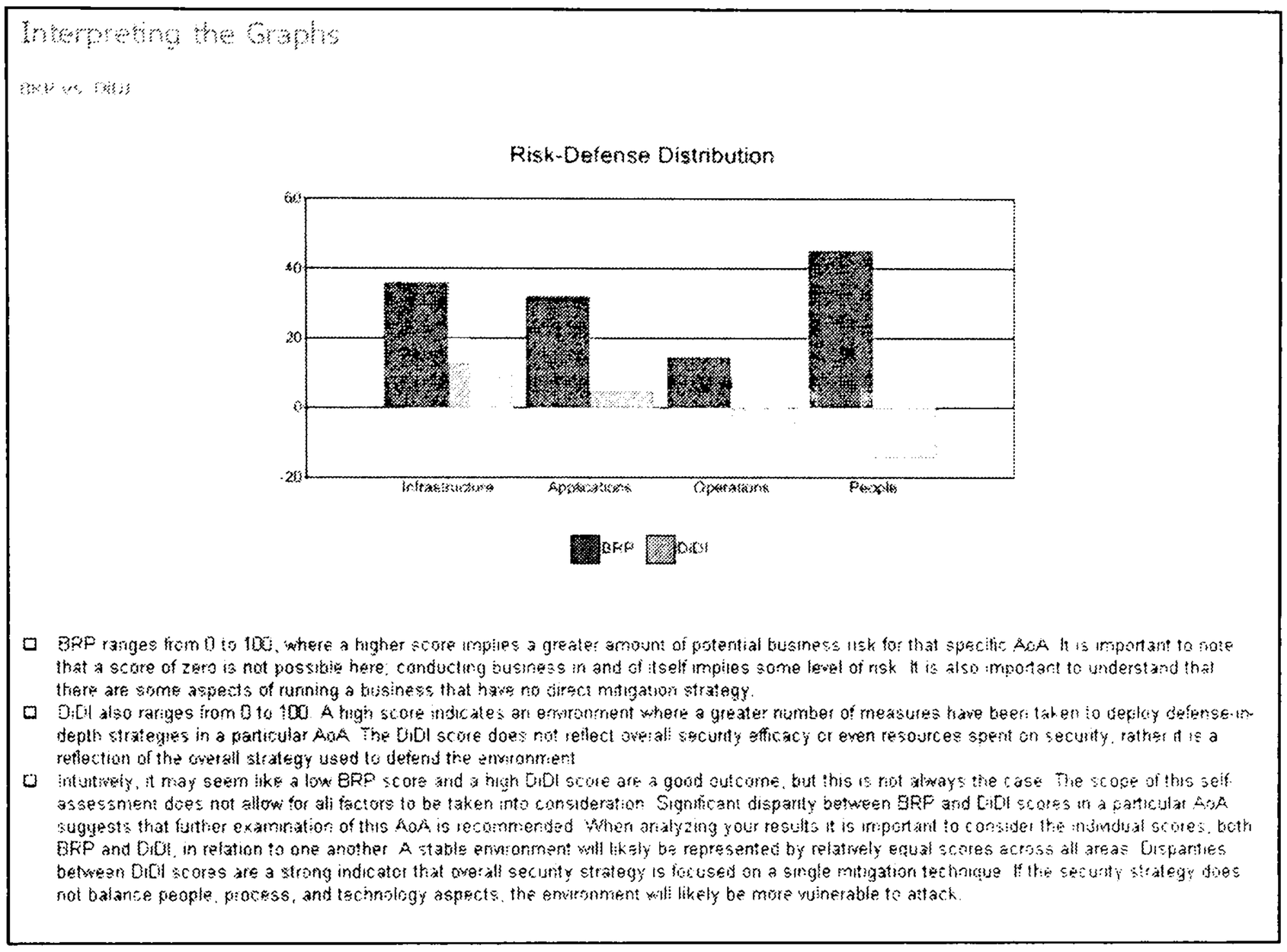


Figure 36: All the data presented to the user as the primary output of MRSAT

Even though this graph is hardly comprehensive, not even including an explanation of what the two elements being displayed, BRP and DiDI, are (BRP stands for Business Risk Profile, i.e. the risk the organisation is under, and DiDI is the Defence in Depth Index, i.e. the controls taken by the organisation), the second of the outputs of the tool is far more useful to an organisation assessing risks. There are three key elements included in the second part of MRSAT's output: The tool provides a list which, according to the users' input in the analysis, prioritises the controls that need to be taken care of (Figure 37, A). Unfortunately doubts can be raised as to why they have been prioritised like this from an assessment based on yes or no answers, meaning that these elements are there because the user has indicated they do not exist within the organisation and they have

been prioritised in a manner probably based on 'Importance scores' pre-determined by the developers, however different assets might have different importance to different organisations and this tool does not consider which assets are of major importance to the organisation being assessed before prioritising what should be secured first. The report also includes a list of brief recommendations on how to better secure areas that have been identified as problematic (Figure 37, B) and also presents the user with a complete list of security areas and controls, indicating which should be improved in the assessed organisation (Figure 37, C) without however taking any budget/cost considerations or again prioritising according to the organisations needs.

A

High Priority	Medium Priority	Low Priority
Password Policies - Administrator Account	Virus Signatures	Firewall Rules and Filters
Change Management and Configuration	Build	Anti-virus - Servers
Backup Media	Input Validation	Backup
Logging		Management Host
Governance		Anti-virus - Desktops

B

	Findings	Recommendations
Secure Build	You have indicated that your system builds include host-hardening procedures	

	Findings	Recommendations
Secure Build	You have indicated that personal firewalls have been installed on all workstations in the environment.	Consider deploying personal firewalls initially on all mobile desktops. By default, block all access to the workstation from the outside

	Findings	Recommendations
Secure Build	You have indicated that remote control/management software is not used in the environment.	Continue the practice of not using remote control/management software

C

Legend ● Meets best practice ● Needs improvement ● Severely lacking

Infrastructure	●	**Operations**	●
Perimeter Defense	●	**Environment**	●
Firewall Rules and Filters	●	Firewall Rules and Filters	●
Anti-virus	●	Administrative Users	●
Anti-virus - Desktops	●	Management Host	●
Anti-virus - Servers	●	Management Host - Servers	●
Remote Access	●	Management Host - Network Devices	●
Segmentation	●	**Security Policy**	●
Remote-Access Users	●	Secure Build	●
Intrusion-Detection System (IDS)	●	Protocols & Services	●
Wireless	●	User Account Management	●
Authentication	●	Security Requirements	●
Password Policies	●	Governance	●
Password Policies - Administrator Account	●	**Patch & Update Management**	●
Password Policies - User Account	●	Network Documentation	●
Password Policies - Remote-Access Account	●	Application Data Flow	●
Management and Monitoring	●	Patch Management	●
Build		Virus Signatures	

Figure 37: Key parts of the MRSAT output report

What follows the lists of controls and the brief explanations on what action should be taken is several links to a Microsoft database of I.S. security practices, which illustrate to the user how to implement solutions (not in very detailed way but comprehensive enough to give the user an opinion on the particular area of I.S.). The only setback is that all recommendations presented in this database only consider Windows systems.

Finally the third output comparison of this tool is a screen which allows the user to compare their results (the ones presented initially in the graph of Figure 36) with the average results of other organisations belonging to the same sector and size as seen in Figure 38.

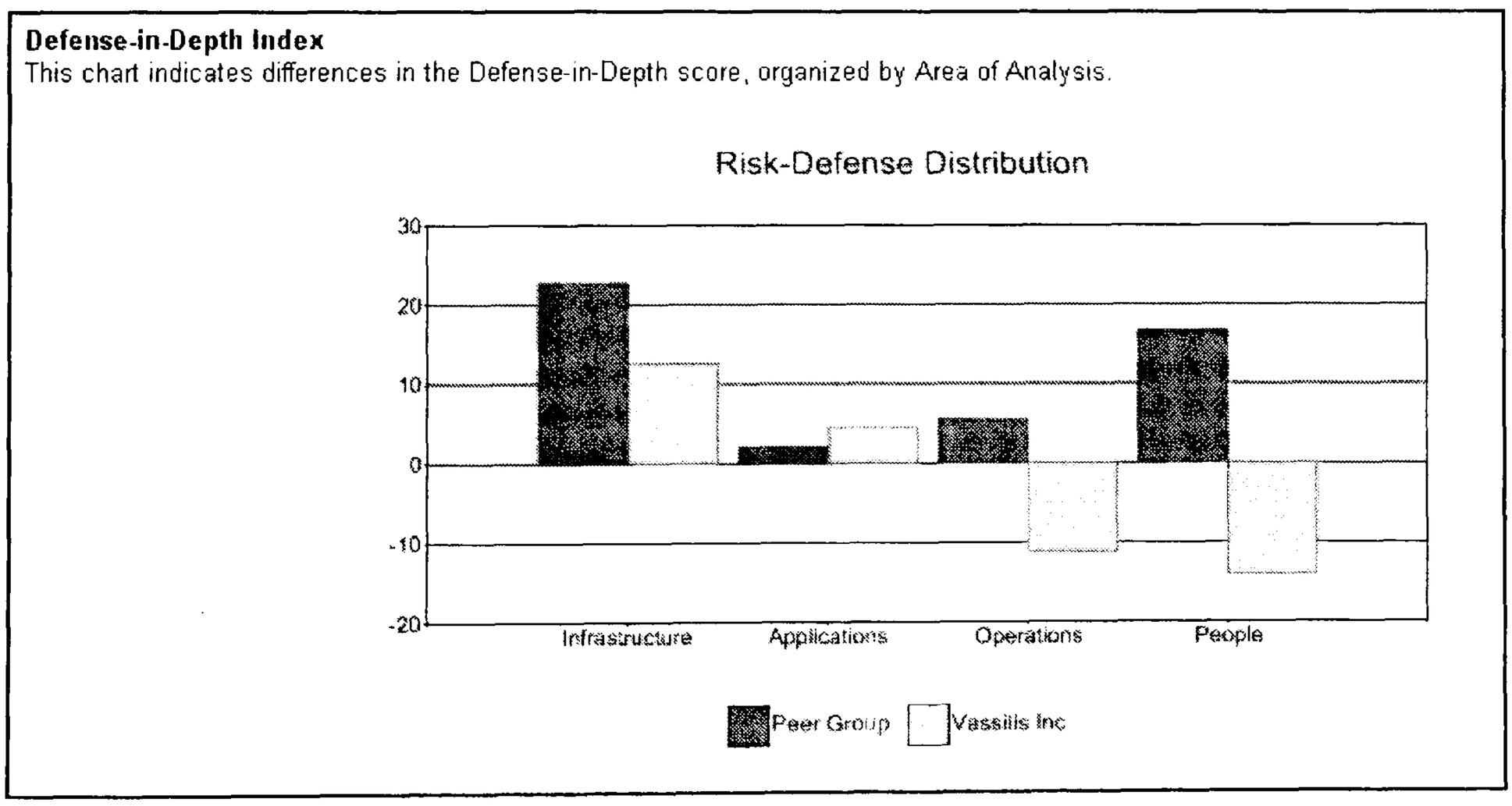


Figure 38: MRSAT compares the results to the industry sector average

This is quite a useful addition which can help the management see were they are lacking in security, however it requires uploading the assessment results to Microsoft, which

some organisations might find inappropriate from a privacy perspective (Morgan Research 2001) it also raises the issue of the reliability of the results from a tool which is freely available to everyone. Furthermore, only a well established organisation which gathers results from thousands of clients can incorporate such an element in a tool therefore it is not going to be considered as one of the elements that will be included in the new methodology.

4.6.1.3 Evaluation

Table 5 summarizes the scores achieved by MRSAT when evaluated against the criteria.

Requirement	Score	Justification
Cost	3	The tool is free to be downloaded by everyone
Ease of use	2.5	No particular expertise required, but it needs very good knowledge of the organisation and potentially some research
Length of Process	2	The assessment lasts approximately two to three hours
Assistance to user	3	There is both assistance within the tool as well as a user guide
Risk Impact Analysis	1	There is no point in the tool where the user can rate the assets or functions importance in any way
Assistance in choosing controls	2	There is some prioritisation of the required controls in the output report without, however, the criteria being clear since assets importance has not been considered
Cost – Effective Controls	1	There is no consideration on the value of the suggested controls versus the budget.
Comprehensive output	3	The tool output is a comprehensive report with great assistance and links to resources provided to the non-expert user
Deployment assistance	2	There are links provided which provide basic information on the set-up of controls. Not too detailed but sufficient to get started.
Length of Report	2.5	Very informative with very little unnecessary data

Dynamic Feedback	1.5	There is none provided, no consideration on the effectiveness of the solutions, can rerun the tool and select the newly implemented control as existent, however, there will still be no consideration of threats that occurred or losses
Dynamic Update	2	The update is not dynamic; however there should be good support by an established organisation such as Microsoft which shows an interest in the area. Tool is already in its second revision

Table 5: Evaluation Results and Justification for MRSAT

4.6.1.4 Advantages and Disadvantages

- Advantages:

  A major advantage of MRSAT compared to the majority of other solutions described is that it is offered free of charge. Furthermore it provides assistance with their selections to users by allowing clicking on the items and providing a pop-up box with explanations or examples. MRSAT is not "technical" meaning that it approaches RA from a point of view that no particular expertise is required to conduct the assessment just good knowledge of the organisations' I.T. functions, features and operations. Furthermore among the positive elements identified is the provision of recommendations and some assistance (links) on how to implement the appropriate controls. Finally, a good addition is the comparison against which areas of security other organisations of the same size and sector have already implemented.

- Disadvantages

  MRSAT does not take in consideration the organisation size and it has no impact on the analysis and valuing of threats towards the organisation. The process and, particularly, the report are a bit lengthy. MRSAT is good for identifying practices that

have been neglected when designing security and not yet implemented, but there still is the need for an expert to deploy the solutions. Furthermore there is no consideration of budgeting or cost effective solutions. Thus there are no financial elements, potential losses and other data of this sort, identified as essential for SMEs lacking budget, awareness and expertise. There is also no considering of what assets are important to the specific organisation; the results are independent of the sector, operation and requirements of the organisation on the contrary, the resulting recommendations are a listing of practices that in the analysis have been identified as not implemented. The only time that MRSAT considers the aforementioned elements is in the final output, where the results are compared with that of other organisations of the same size.

4.6.2 Cobra

Cobra is a commercial RA tool, based on ISO17799, which can be purchased from the organisations website where an evaluation copy can be downloaded from. This evaluation copy was used for this investigation. It offers full functionality, with the only limitation being that the output report cannot be printed on paper and may only be viewed on screen.

4.6.2.1 Operation: Risk Analysis

The Cobra tool approaches the security requirements of the organisation being assessed either from, as the developers describe these, an I.T. perspective or from a business perspective. Approaching the analysis from the I.T. perspective, the user is required to

complete four sets of questionnaires: one on integrity, one on availability, one on confidentiality and one on a business impact analysis. The first three essentially investigate what controls are in place in order to protect the integrity, availability and confidentiality of business assets. The fourth aims to establish what the revenues of the organisation are and what the business impact of a breach of integrity, availability and confidentiality of business information would be. In order to achieve the latter the user is required to reply to questions assessing financial damage should data be lost, accessed without permission or modified. Some of the first observations on this tool are the difficulty one gets around the menus and the relatively poor graphical interface. Furthermore the system does not rule out questions that contradict each-other meaning that straight after the user says there is no continuity plan in place, they still receive two questions asking how confident the user is on the continuity plan on which one can reply that they are 100% confident. Figure 39 illustrates the graphical interface of this tool.

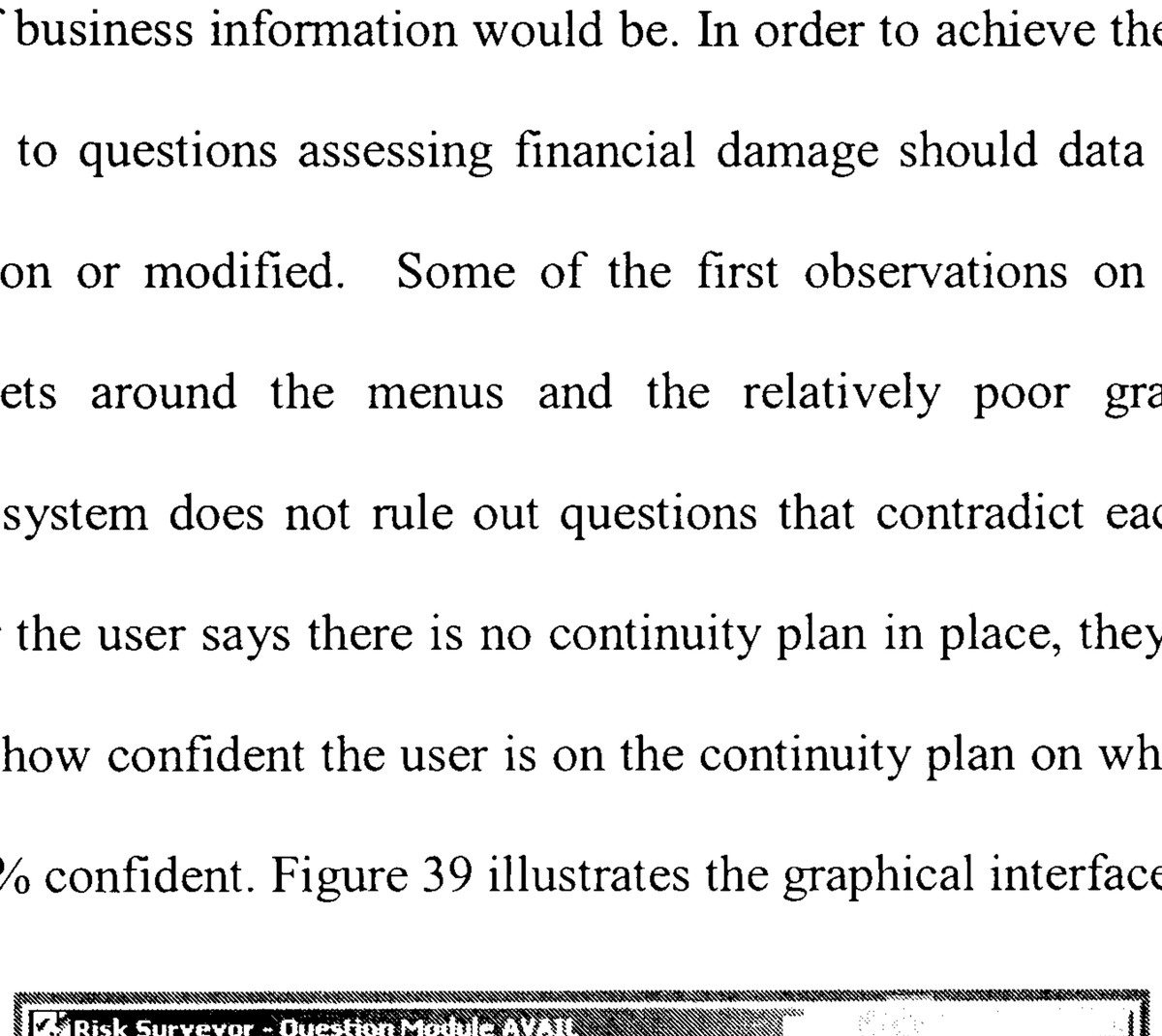


Figure 39: The GUI of cobra is not as evolved as that of the other tools

The listings in Figure 39 are actually how Cobra appears to select what threats the organisation is under (i.e. based on the user's judgement of what threats the organisation faces) which raises the question of how accurate the results are. Taking the other approach i.e. the BIA approach, the tool uses a larger number of questionnaires to basically assess certain I.T. security issues from a business perspective (e.g. what plans (continuity, backup, audit) are in place and whether or not they include certain elements).

4.6.2.2 Management

Having successfully completed the analysis, the Cobra tool produces the output report (Figure 40). The report is well structured and with a clear layout. An interesting feature of the tool is that based upon the responses of the user, presumably from the BIA questionnaire, the tool determines what the acceptable risk levels are, then according to the responses to the rest of the questionnaires the tool presents the user with a graph illustrating by how much the organisations risks have exceeded this acceptable level. Of course determining the acceptable level of risk is highly subjective and can easily lead to misconceptions, however since the mathematics behind how this was calculated are not explained, we cannot discuss the correctness of such a result. Assuming it is well-considered it does look as an informative output to the user.

Management Summary (continued)

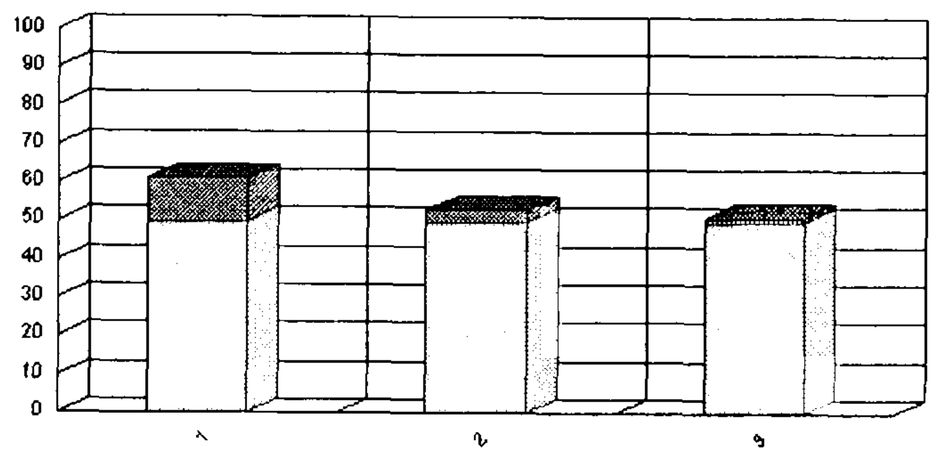
OVERALL AVERAGE

55.21 %

Please Note: This overall average should only be used as a guide to the average risk level which this assessment has identified. Reference should be made to the rest of the Management Summary to identify the specific areas which require attention.

THE FOLLOWING CATEGORIES REQUIRE PARTICULAR ATTENTION
AN ASSESSMENT OF EACH APPEARS IN THIS MANAGEMENT SUMMARY

Categories Above Threshold Of Acceptable Risk



	RISK CATEGORY	RISK FACTOR
1	Availability	61.24 %
2	Integrity	53.24 %
3	Confidentiality	51.15 %

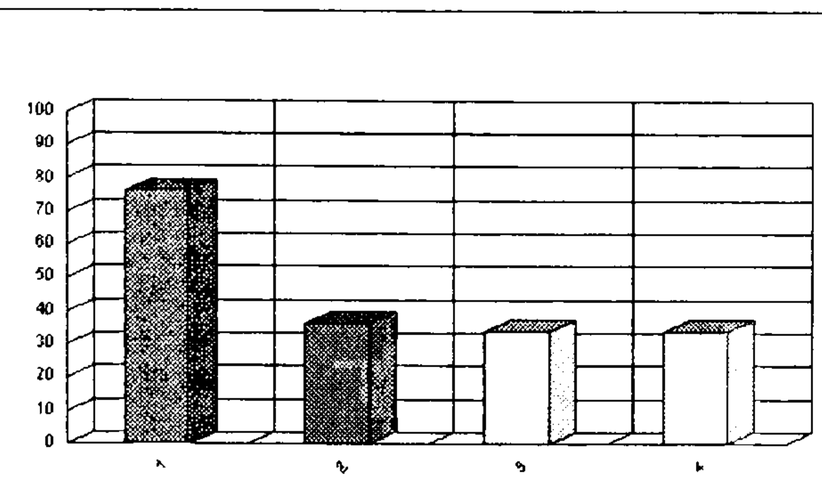
Figure 40: Cobra Report on the Acceptable Risk

Moving further down the report however the quality of the results starts going down. As Figure 41A illustrates there are graphs with no clear indications of what they mean. Finally there are the suggested countermeasures, which are essentially simply a list of all the available countermeasures in the tools database, excluding the ones the user stated that they exist within the organisation. Looking at Figure 41B, it is clear that the results are poor, providing with no explanations on why, how or where they should be implemented.

A

Business Impact Assessment (continued)

Buisiness Impact Levels



B

Counter Measures (continued)

Risk Category: ***Availability***

NUMBER	TEXT
6106	Urgent steps should be taken to reduce exposure to fire, flooding and explosion
6108	Urgent steps should be taken to reduce exposure to hardware, equipment and media unavailability
6113	Urgent steps should be taken to reduce exposure to Hacking/Electronic Sabotage
6114	Urgent steps should be taken to reduce exposure from the loss of third Party Service
6120	Physical access controls/practices for those areas that may hold sensitive/confidential information should be reviewed and stengthened
6121	Ensure that specific back-up and recovery measures are in place for both serious software error occur and loss of critical data.

Figure 41: Samples of cobra output

Essentially, disregarding if the I.T. or the BIA approach was taken, the feeling is that the tool simply has a database with all the available controls and practices, and the report is a listing of all those that were not selected by the user as existing in the analysis.

4.6.2.3 Evaluation

Table 6 presents a summary and the justification for the marks achieved by Cobra when evaluated.

Requirement	Score	Justification
Cost	2	The Cobra application costs £1100
Ease of use	2.5	The assessment is not oriented towards technical users. However, Cobra does not get full marks since the wording and menus are sometimes confusingly unclear.
Length of Process	1.5	The assessment takes two to three hours, but due to the I.T. and Business approaches to the assessment it might require more than one person completing the questionnaires introducing the relevant risks
Assistance to user	2	No assistance within the tool, however multiple documents provided including a worked example
Risk Impact Analysis	1	Even though the impact of certain threats realising is investigated in the analysis, such considerations are not really reflected in the report.
Assistance in choosing controls	1	There is none, the entire range of controls that correspond are presented to the user with no indication of order.
Cost – Effective Controls	1	There are no financial considerations on the value of the suggested controls versus the budget.
Comprehensive output	2	The output is very comprehensive in terms of language, will still not get full marks because it requires considerate improving
Deployment assistance	1	Cobra does not provide any assistance on how to implement these controls and hardly even explains what they are.
Length of Report	3	Cobra gets full marks on this issue since it presents the user with the option to select what sections they require in the report.
Dynamic Feedback	2	There is no feedback; the user would be required to re-run the process.
Dynamic Update	2	There is no update in place; it is up to the organisation to release complete updated versions of the tool.

Table 6: Evaluation Results and Justification for Cobra

4.6.2.4 Advantages and Disadvantages

- Advantages

  This tool includes what is missing from the Microsoft tool; it actually evaluates how important assets are to the organisation and how much a compromise would affect the organisations' operation.

- Disadvantages

  This information is not utilised in a useful manner in the output section, providing control suggestions that are lacking all of the elements we identified as required. Again the size of the organisation does not make any difference to the results provided to the user since the assessment is based solely on the available controls and the impact of breaches to the organisation without considering size neither in terms of employees or PCs and servers.

4.6.3 The Buddy System

The third and final RA tool evaluated for the purposes of this thesis is the Buddy System, a solution created by Countermeasures Inc. The latest version of the Buddy System, which was used in this evaluation is "Release 731".

4.6.3.1 Operation: Risk Analysis

Unlike the other two tools discussed in this section, the Buddy System does not use questionnaires to perform the analysis of the organisation and its threats. Instead this tool assesses certain areas of organisational structure and security (Figure 42, A) such as operational data (such as operating period, acceptable down-time), operating environment

(open-space office, room etc), types of information (financial, customer, student), uses drop-down menus (Figure 42, B) within a well-designed graphical interface. Having defined the general business environment the user moves to the 'asset configuration' menu where they are required to select from a list of assets (including communication equipment such as modems and routers, personnel found within the organisation, vendor software (such as Lotus and Corel draw), which the user needs to declare whether they exist within the organisation and for each asset whether they are shared and if they are considered to be critical.

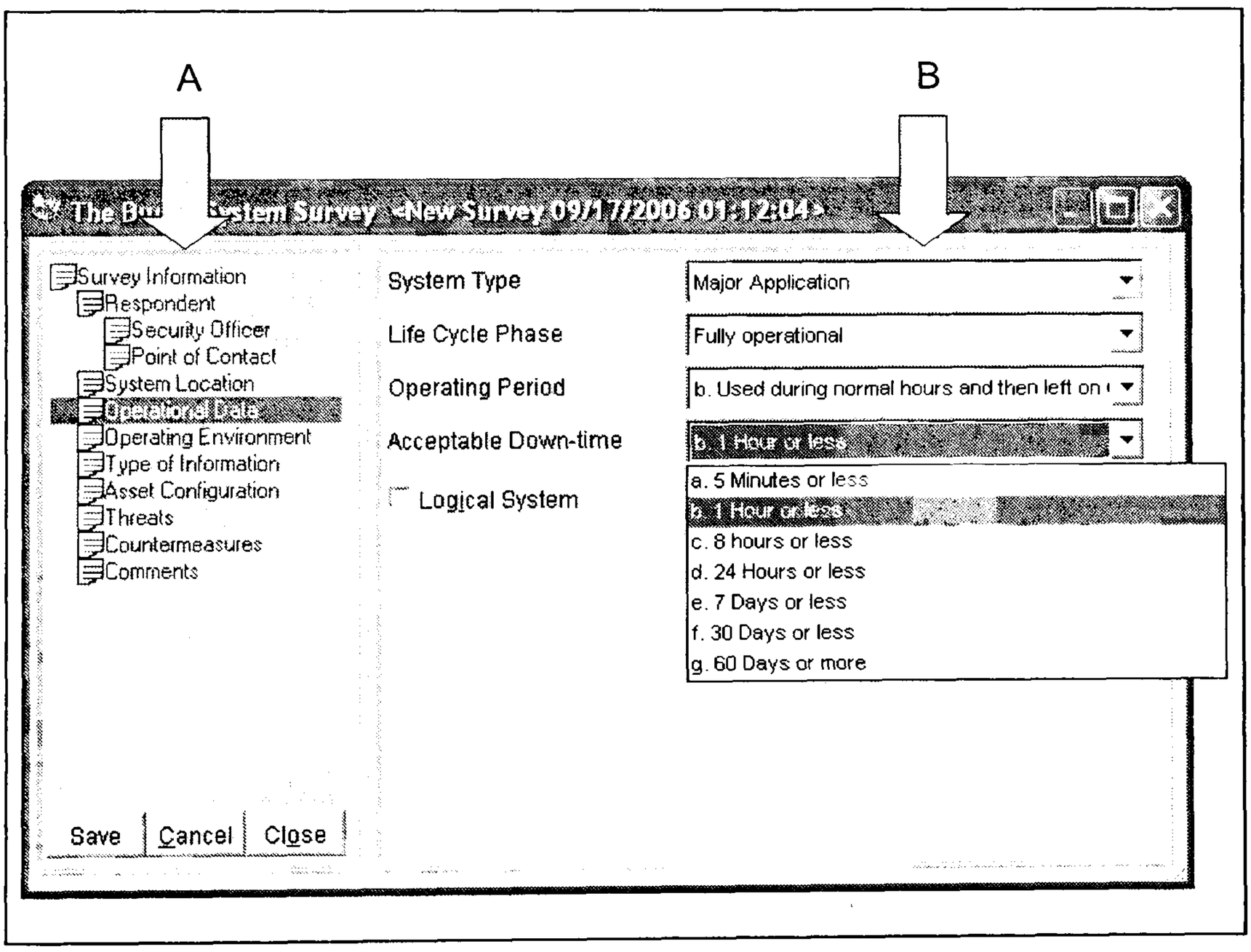


Figure 42: The Buddy system interface and analysis approach

Even though up to this point this tool would have looked as the most appropriate for an SME, moving away from identifying the assets the user proceeds to the 'Threats' part and

this is where this tool loses the game. In the threats part of the assessment, the users are actually required to select the threats their organisation and I.T. infrastructure are under themselves. As Figure 43 illustrates, a list of threats is presented to the user (such as power failure, software failure, theft, terrorist act) from which the user needs to select which are appropriate. To start with, comparing the list with the threats listed in the various surveys of Chapter 2, the list does not include all the possible threats to the organisation. Furthermore, even if we disregard this, what is introduced here is the likelihood that the user neglects a threat, either considering it unlikely to occur or simply not realising its importance. To take this into extremes but illustrate the problem here, not many I.T. users in the WTC would be likely to select they are susceptible to a terrorist threat or organisations in New Orleans that would claim they are vulnerable to natural disasters. The user also needs to select the frequency of occurrence of each threat they select (illustrated within the red circle in Figure 34) which again raises serious concerns on the correctness of the results produced by this assessment, the scaling used to select the frequency is also somewhat peculiar.

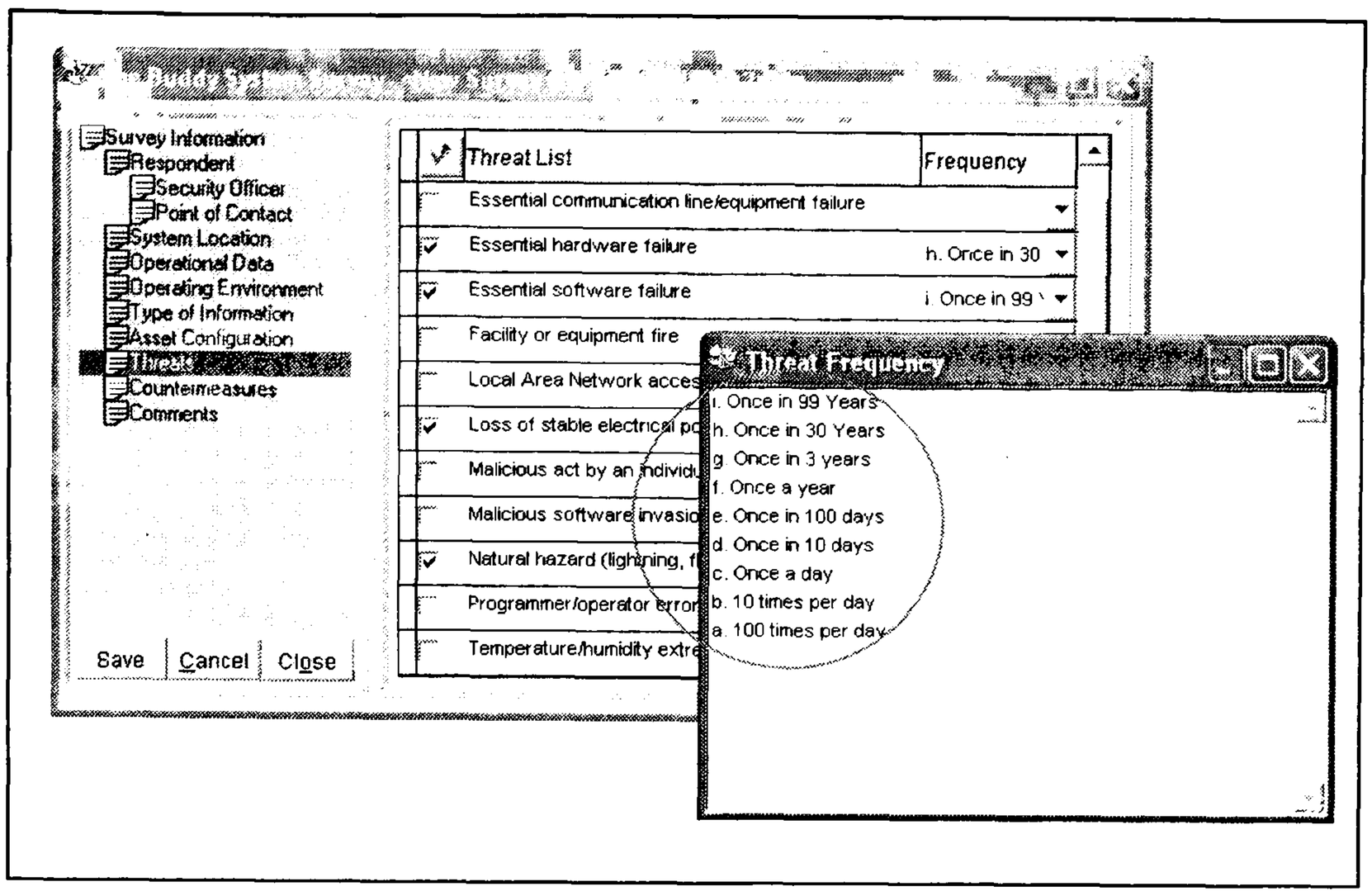


Figure 43: Threat selection in the Buddy System

Finally the user is presented with a list out of which they are required to select what countermeasures are already deployed within the organisation

This concludes the analysis module which ideally should, according to the makers of the software, also be filled by at least four other users within the organisation (including a security person, a manager, and end users). One can however proceed to managing the risks even if a single user has performed the assessment.

4.6.3.2 Risk Management

As Figure 44 illustrates, the risk management offered by the Buddy System includes an analysis of the threat levels (Figure 44, A) and for each of the threats the tool illustrates the existing controls and proposes certain other controls as required (Figure 44, B). The Buddy System is the only tool from those evaluated that actually recommends controls,

(even though the criteria upon which the controls are suggested are unknown) according to the needs of the organisation instead of presenting with a full list of all the controls that the user has not identified as already deployed.

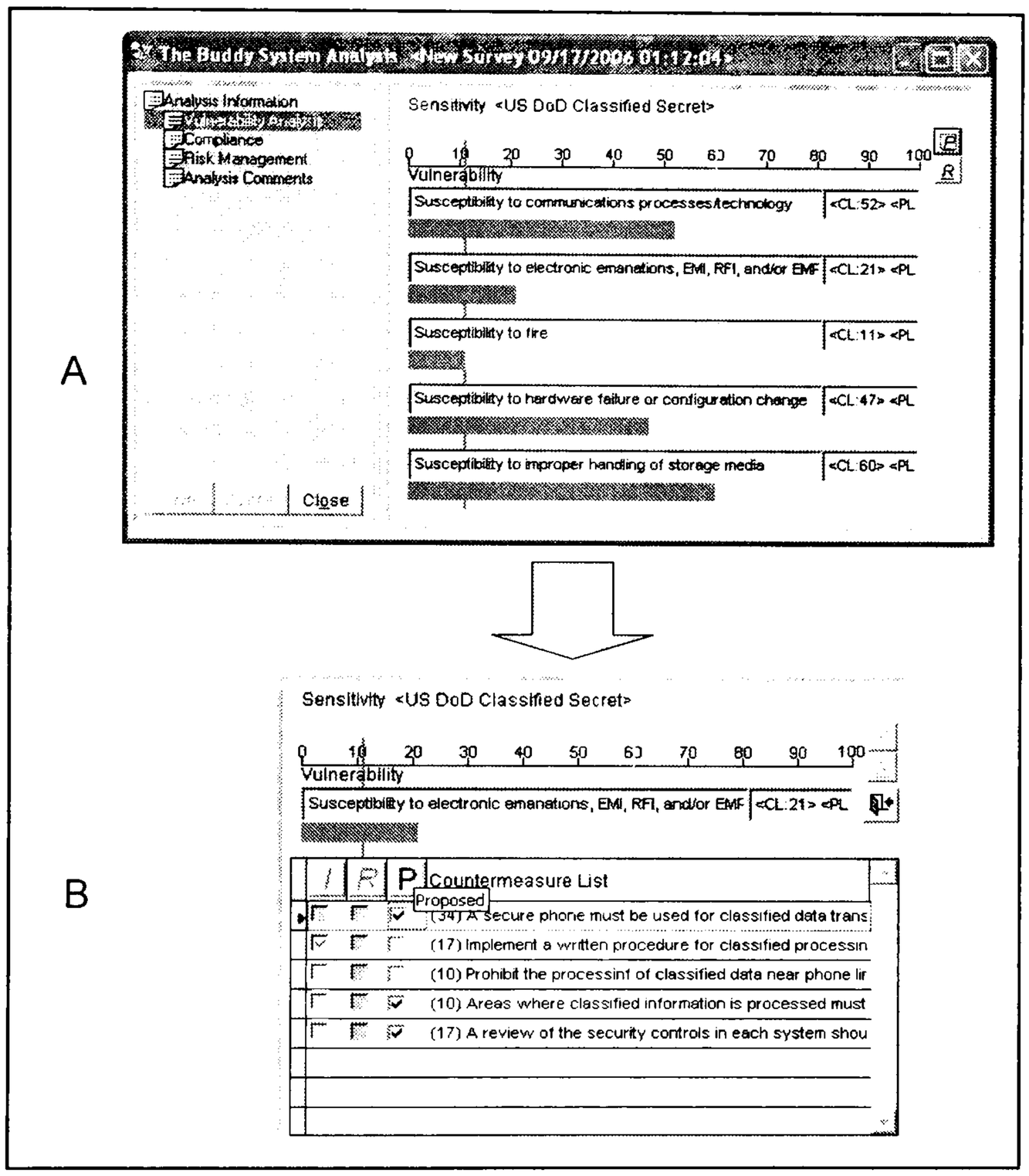


Figure 44: Proposal of controls in the Buddy System

4.6.3.3 Evaluation

Table 7 displays a listing of the scores achieved by the Buddy System when evaluated. The Table also includes a justification of why these scores were assigned to the tool for each of the characteristics.

Requirement	Score	Justification
Cost	2	The cost is unknown, but it will be assumed to be priced in the same range as the majority of RA tools
Ease of use	2	The Buddy assessment is not complicated enough to need I.T. security training. However it mainly includes I.T. related elements in the way RA is approached.
Length of Process	1.5	The process last approximately two hours, but it is recommended that multiple users perform it therefore introducing delays
Assistance to user	2	The Buddy System comes with a user guide
Risk Impact Analysis	2	The tool does consider the actual cost of the assets
Assistance in choosing controls	3	The Buddy System is the only tool that recommends solutions to the user as required.
Cost – Effective Controls	1	There is no consideration on the value of the suggested controls versus the budget.
Comprehensive output	1.5	Even though it is presented through a nice graphical interface, Buddy does not clarify much about what the recommended controls are, nor does it suggest some source that does.
Deployment assistance	1	the Buddy System does not provide with any information on how to set up the suggested controls
Length of Report	2	Buddy does not provide a report apart from the on-screen display, this makes it actually miss out on information that should have been presented to the user as there is limited space to provide enough information
Dynamic Feedback	2	There is none provided, no consideration on the effectiveness of the solutions, would require to re-run the application.
Dynamic Update	2	There is none suggested. User depends on the organisation releasing a new version of the tool.

Table 7: Evaluation Results and Justification for the Buddy System

4.6.3.4 Advantages and Disadvantages

- Advantages

No particular expertise is required, just knowledge of the organisation. The analysis can be easily performed by the management. It is the only one from the evaluated tools that

uses some type of asset valuing to then suggest controls. Buddy has a user friendly graphical interface.

- Disadvantages

Software and threat identification is limited to specific assets, For example when in the analysis the user is required to select types of software within the organisation, they are presented with a very short list which includes 22 specific programmes which can easily be questioned in terms of how inclusive it has been. Similarly, 'Essential hardware' includes only 12 devices, including CD-ROM, colour printer and scanner, laser printer and PCMCIA modem, not really the most essential bits of hardware, finally 'Essential information' only includes 4 types of information the user can choose from as existing within the organisation: operational, medical records, planning and tactical. Finally this tool takes no consideration at any part of the size of the organisation or the budget

4.7 Practical Assessment of the SME-oriented tools

This section will discuss how the tools were evaluated and how they coped with different SME organisations.

4.7.1 The SME scenarios used for the evaluation

In order to evaluate the tools, three scenarios were created targeting the organisation sizes this research is concerned with. The scenarios were based on real life organisations, one for a software and website development organisation with a size of less than 10

employees, one for a small education organisation with less than 50 employees, and one for a medium-sized healthcare organisation with less than 250 employees. An inventory of assets and applications commonly found within was created for each organisation; each organisation's security requirements as well as their main concerns from an I.S. perspective were also considered and documented. These scenarios are included in detail in Appendix A.

4.7.2 How the tools coped with the scenarios

Before the discussion on the overall scores achieved by the three RA tools for SMEs during their evaluation, it is worth analysing the outputs they provided and how each coped with the three different organisation scenarios (i.e. how the results of each tool was affected by the differences in the organisations size, sector and security needs). Some of the tools outputs are included in the discussion that follows while the entire range of screenshots of the tools outputs are included in Appendix E for reference.

4.7.2.1 MRSAT

This solution provides a prioritisation of controls (Figure 45) and enough links to information on what the suggested controls are.

Security Initiatives

The following areas fall short of best practices and should be addressed to increase the security of your environment. The Assessment Detail and Prioritized Action List sections of this report include further detail for each, including the findings, best practices, and recommendations

High Priority	Medium Priority	Low Priority
Logging	Virus Signatures	Firewall Rules and Filters
Change Management and Configuration	User Account Management	Governance
Backup Media	Security Policy	Build
Encryption	Input Validation	Password Policies - Administrator Account
Background Checks	Physical Security	Backup

Figure 45: Prioritisation of controls in MRSAT

A setback is that the tool does not illustrate at its output (nor considers in the assessment) the threats that the organisation faces and their levels. Instead, the means of judging whether security is sufficient is by comparing implemented security with those of other organisations of the same size and sector (Figure 46).

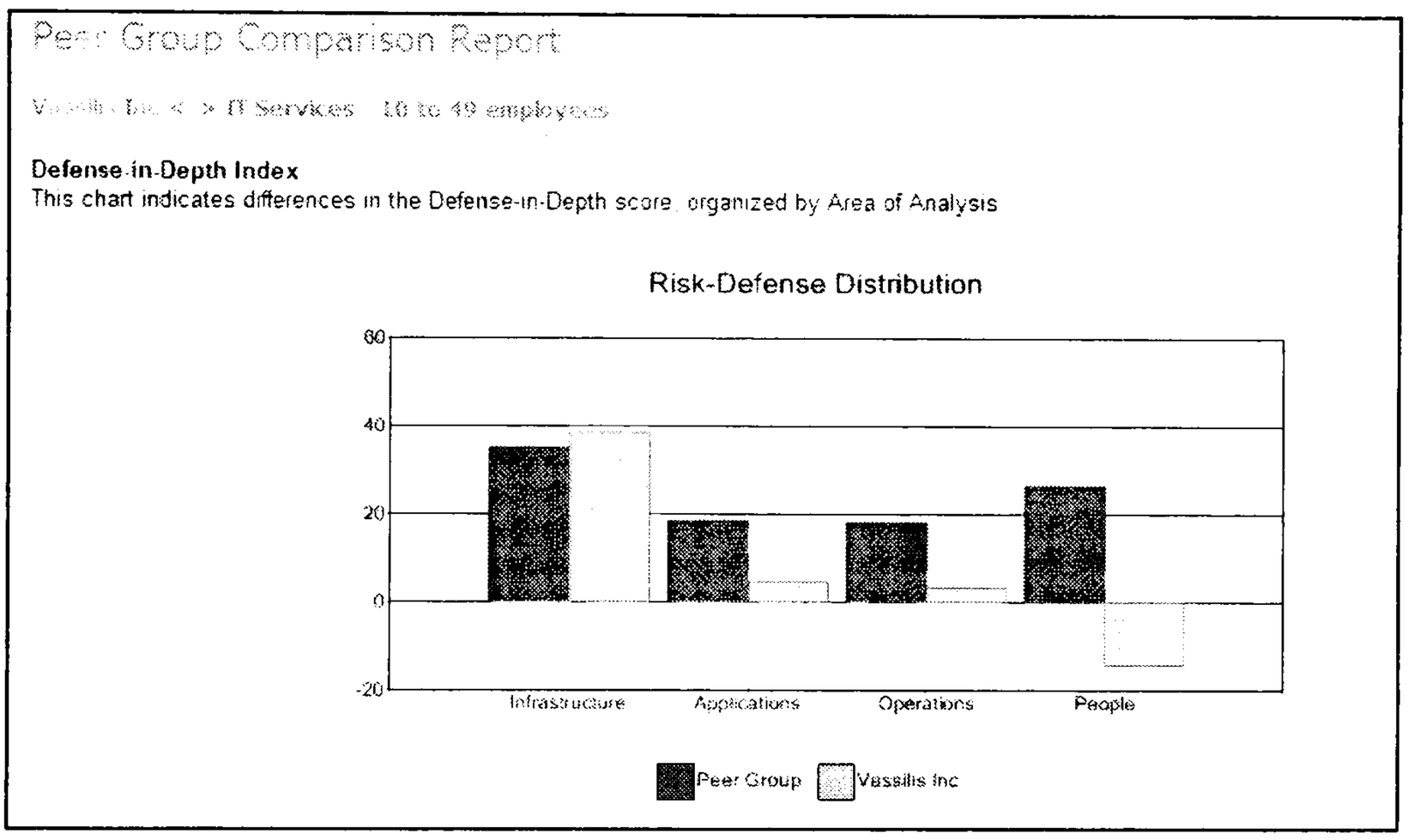


Figure 46: Comparison of security practices in MRSAT

Even so, this looks like a good element if your organisation is under-investing, however since it is not necessary that the other organisations have appropriate security it might actually lead to a misconception, especially if the organisation under assessment has implemented better security than other organisations in the sector (it may lead to a false perception that the organisation is safe or even that it is over-investing). Furthermore, what other organisations of the same size and sector are investing on security is not a particularly good justification to the management that they need to do the same.

On the issue of the three different scenarios MRSAT has suggested different controls and prioritised them differently. Figure 47A illustrates the recommended controls for scenario 1, Figure 47B for scenario 2 and Figure 47C for scenario D.

A

Security Initiatives

The following areas fall short of best practices and should be addressed to increase the security of your environment. The Assessment Detail and Prioritized Action List sections of this report include further detail for each, including the findings, best practices, and recommendations.

High Priority	Medium Priority	Low Priority
Change Management and Configuration	Virus Signatures	Firewall Rules and Filters
Log Files	Security Requirements	Backup
Anti-virus - Servers	Patch Management	Anti-virus - Desktops
Backup Media		
Password Policies - Administrator Account		

B

Security Initiatives

The following areas fall short of best practices and should be addressed to increase the security of your environment. The Assessment Detail and Prioritized Action List sections of this report include further detail for each, including the findings, best practices, and recommendations.

High Priority	Medium Priority	Low Priority
Logging	Virus Signatures	Firewall Rules and Filters
Change Management and Configuration	User Account Management	Governance
Backup Media	Security Policy	Build
Encryption	Input Validation	Password Policies - Administrator Account
Background Checks	Physical Security	Backup

C

High Priority	Medium Priority	Low Priority
Anti-virus - Servers	Virus Signatures	Firewall Rules and Filters
Change Management and Configuration	Protocols & Services	Build
Input Validation	Backup Media	Governance
Password Policies - Remote-Access Account	Logging	Backup
Background Checks	Secure Build	Acceptable Use

Figure 47: recommended controls for the three scenarios by MRSAT

However, during the assessment and due to the nature of the questions it involved, this did not appear to have anything to do with the different sectors or sizes. Instead, this different output was essentially due to the different choices of the controls that the organisations have in place. Thus it appeared that the system suggested to the user those controls that they have selected as non-existent within their organisation. Therefore as can be seen in the three different 'Risk–defence distribution' graphs in Figure 48 (again

A for scenario 1, B for scenario 2 and C for scenario 3), the larger the organisation got, the better their security.

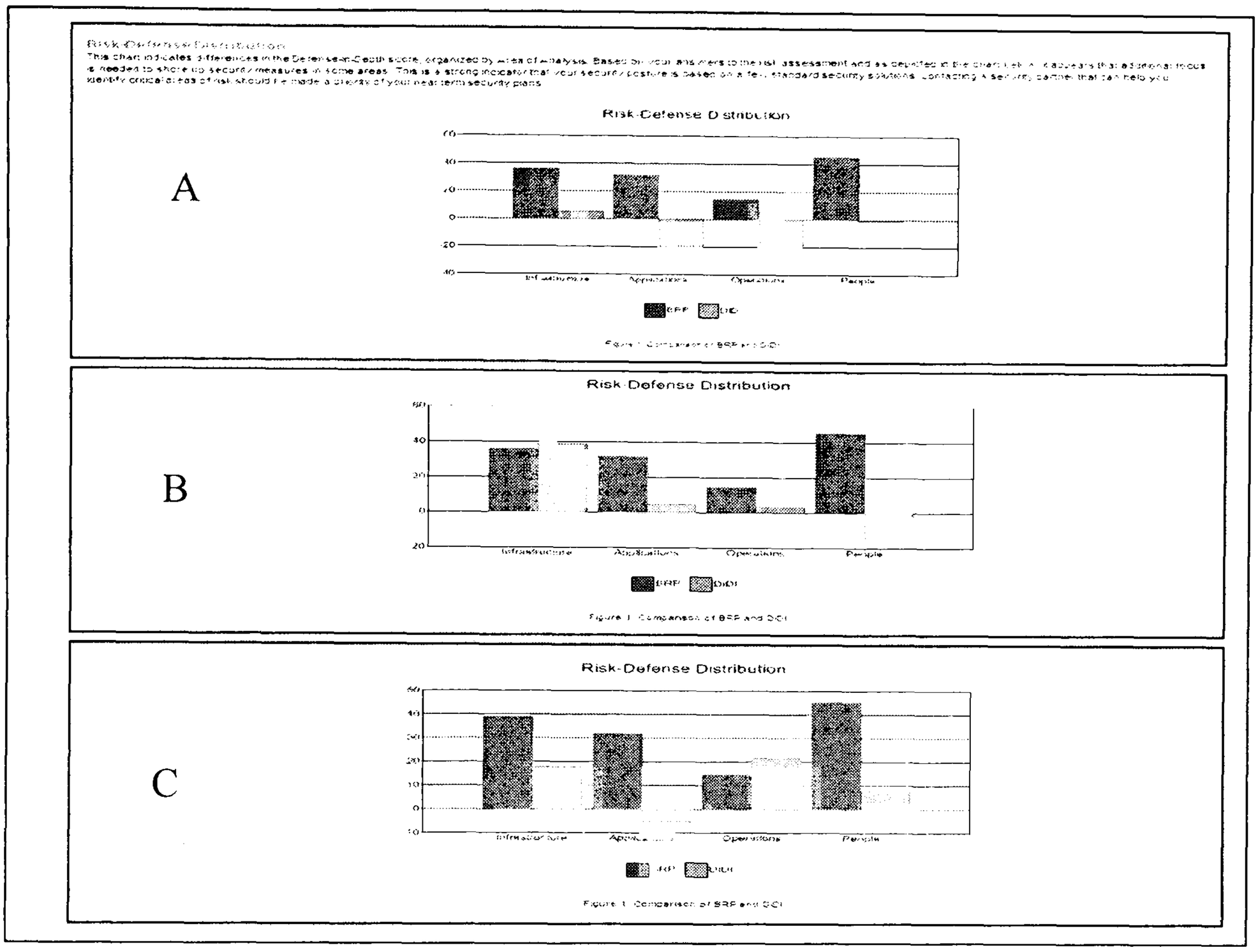


Figure 48: Risk variations according to the evaluation scenarios in MRSAT

For the home-office organisation 'Applications' and 'Operations' security is particularly bad since there exist no policies, response plans and no passwords or logs are used, the small research organisation has all security issues improved apart from 'People' security since users have quite high network privileges and access to resources in order to be able to perform their research tasks properly and finally the medium sized organisation copes better in all areas since physical security is more thorough, access to data is controlled here and people are made aware of policies. The only time that it was apparent that the system took the size and sector into consideration was at the end of the report were there

is the comparison graph with the other organisations (and again that may not be applicable to all the organisations undertaking the assessment as some may have privacy issues with sharing this data with Microsoft).

4.7.2.2 Cobra

Cobra's identification of the threats was based on the users responses of what the threats they are worried about are and the valuing of the risk the organisation is under came from the users own estimation of how confident they are of security. It is a logical progression therefore that the quality of the controls suggested in the output report would not be neither well considered nor thorough.

Counter Measures (continued)

Risk Category: ***Availability***

NUMBER	TEXT
6106	Urgent steps should be taken to reduce exposure to fire, flooding and explosion.
6108	Urgent steps should be taken to reduce exposure to hardware, equipment and media unavailability.
6113	Urgent steps should be taken to reduce exposure to Hacking/Electronic Sabotage.
6114	Urgent steps should be taken to reduce exposure from the loss of third Party Service.

Figure 49: Recommendations in the Cobra output report

Looking at Cobra's output reports in Figure 49 confirms this speculation since the level of detail it went into the suggested controls is for example: 'Urgent steps should be taken to reduce exposure to hacking". This type of result might be a bit useful to a user with extremely good knowledge of I.S., however it would not be useful to an SME user or manager.

Cobra's output had absolutely no relevance with what industry sector or size the organisation being assessed belongs to since these issues are not needed at all in the analysis. Besides the 'required actions' (which as just been described do not depend on the organisation at all but on the user's judgement instead) there are essentially three figures presented to the user, as illustrated in Figure 50. These are: The level of risk (Figure 50A), the Thresholds of acceptable risk level (Figure 50B) and the Business Impact of loss of Confidentiality, Integrity and Availability (Figure 50C).

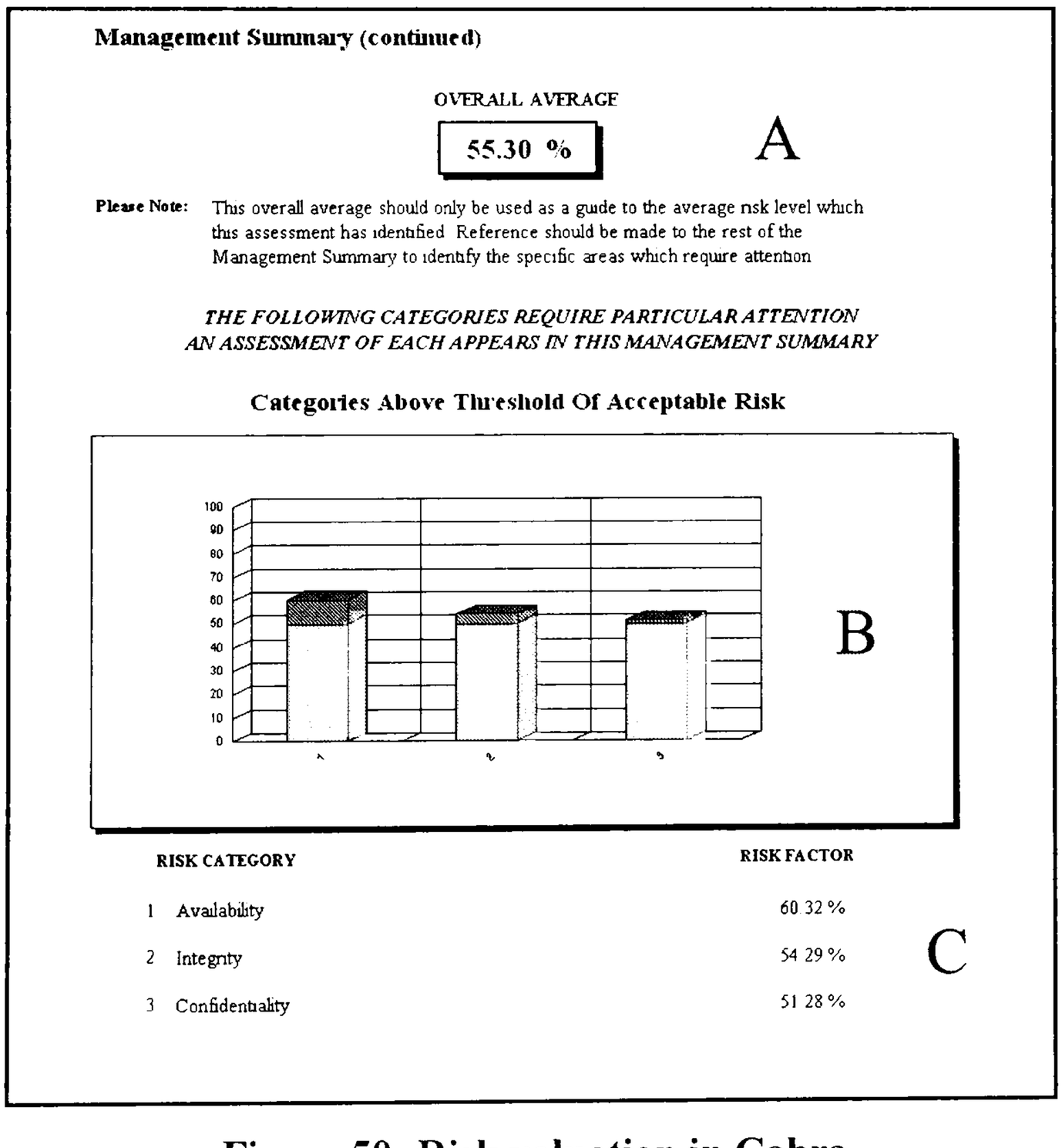


Figure 50: Risk valuation in Cobra

Out of these, the first appears to be based on the users response of how worried they are for each occurring, the threshold seems to be based on the user's selections of how long

after C, I or A have been compromised will the organisation start facing damage, finally the last seems to be an output of the users selections of how much a breach would cost to the organisation. This explains the rising figures in the 'Business Impact' output of Cobra in Table 8 (data taken from the Cobra output reports which can be seen in full detail in Appendix E) since the larger the organisation scenario that was assessed, the larger the impact of breach and the lesser the acceptable downtime were stated to be.

Scenario / Category	A: Home office	B: Small Enterprise	C: Medium sized Enterprise
Confidentiality	25%	44.74%	86.11%
Integrity	25%	44.74%	100%
Availability	41.9%	68.23%	78.22%

Table 8: Impact of C,I,A breach from Cobra's output against the 3 scenarios

Furthermore it explains the reduction of the risk as the size of the organisation rises since the larger the organisation the more confident the user was chosen to appear on the possibility of breaches, to illustrate what the output would be if as the organisations become larger, the manager who is supposedly performing the assessment is less aware of anything related with what is happening in the IT department. If this assessment was considered the other way round (i.e. to be performed by a member of I.T., the results would probably be more inaccurate since the whole assessment is based on the user's perception of the business impact of breaches.

4.7.2.3 The Buddy System

Out of the three evaluated tools, the Buddy System's output to the user was probably the most useful to an SME user, based on the fact that it is the only one with the functionality which enables the user, after the initial threat has been calculated, to allow the system to automatically reduce it to an acceptable level and suggest the controls that would help achieve this (Figure 51).

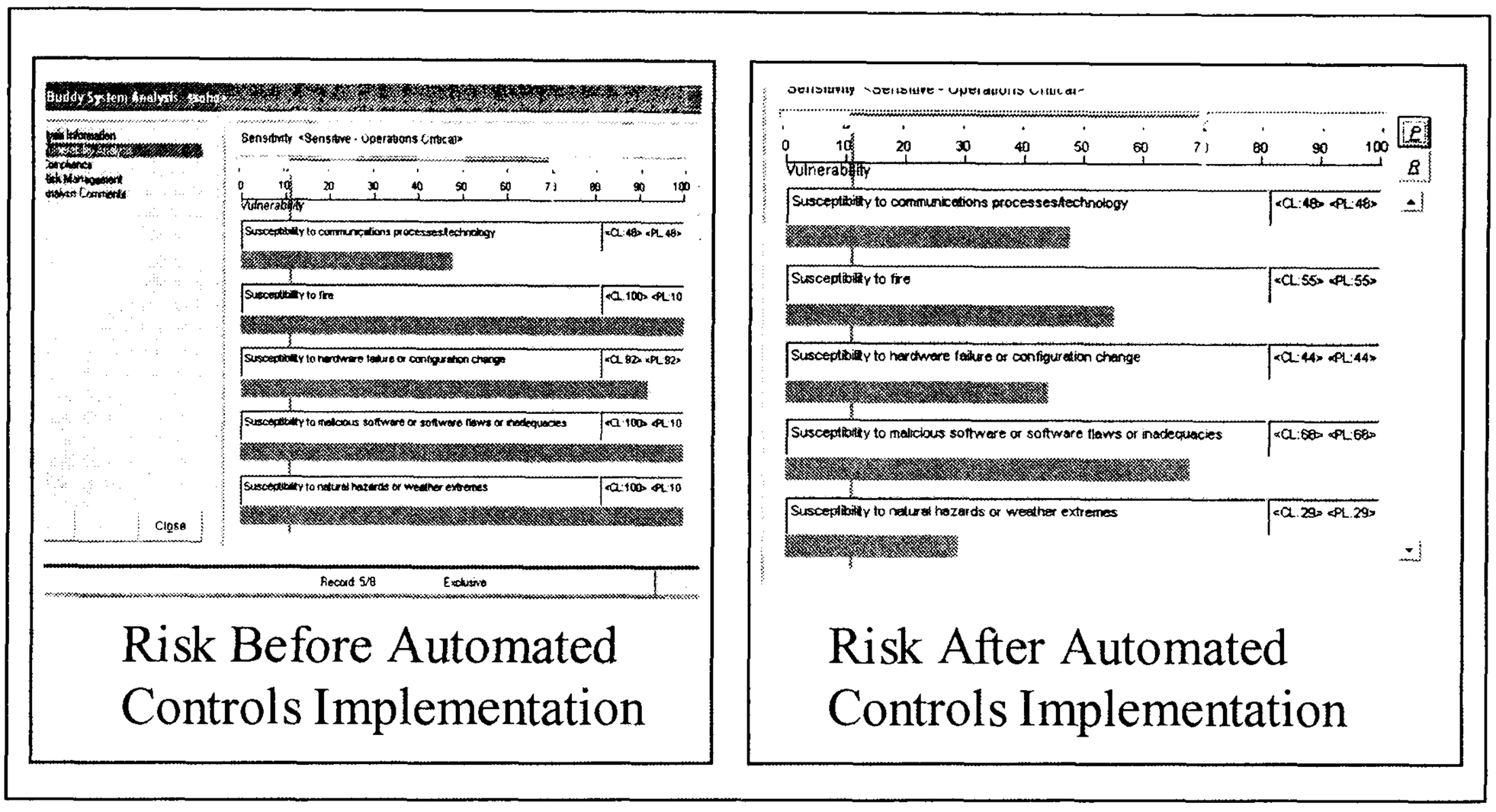


Figure 51: Automated risk reduction in Buddy System

The Buddy system also considers both the organisation size in terms of I.T. as well as personnel and also requires the user to estimate value of assets in dollars as well as in terms of acceptable downtime and frequency of occurrence of incidents therefore appears to have a more credible estimation in its output of the risks the organisation is under (especially considering what has just been written for Cobra's estimation and that MRSAT does not provide with one). As illustrated in Figure 52 (full scale images of each output are available in the Appendix E for reference), the buddy system is the only tool

that does provide with different outputs for the three different evaluated organisations and, judging by the detail of information the user is required to input in the analysis, these results do appear more credible and well-considered than those of the other tools.

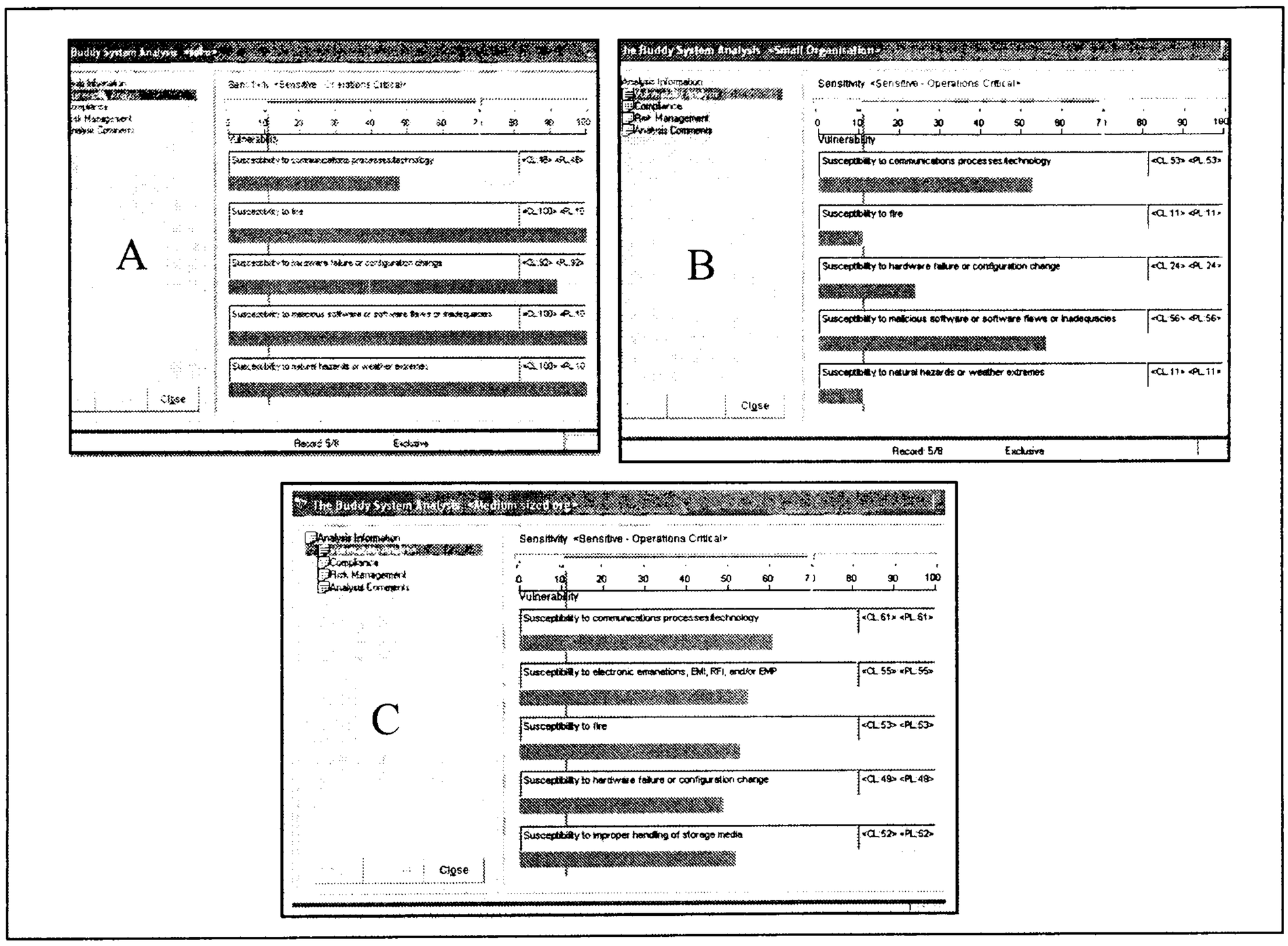


Figure 52: Levels of Risk as presented by the Buddy system for the three different scenarios (A: Home office, B: Small Organisation C: Medium Enterprise)

However where the Buddy system falls behind is the very limited database it provides in terms of controls (also in terms of threats and assets as mentioned in the analysis earlier) and the fact that it does not provide any information on these controls either. Buddy's controls are similar to Cobra's, using the following as an illustrative example 'Sensitive application systems should have access control implemented' such recommendations

would not provide any useful information to the SME user unless they are trained in I.S. which, as seen by the survey findings, is very unlikely.

4.8 Summary and discussion of evaluation results

Table 9 presents a collection of all the characteristics of the tools and illustrates what elements have made existing RA tools inappropriate to be used by SMEs.

Category	Criteria	MRSAT	Cobra	Buddy
General	Cost	3	2	2
	Ease of use	2.5	2.5	2
	Length of process	2	1.5	1.5
Process	Assistance to user	3	2	2
	Risk Impact Analysis	1	1	2
	Assistance in choosing controls	2	1	3
	Cost – Effective Controls	1	1	1
Output	Comprehensive output	3	2	1.5
	Deployment assistance	2	1	1
	Length of Report	2.5	3	2
Support	Dynamic Feedback	1.5	2	2
	Dynamic Update	2	2	2
Overall	Category: General	7.5/9	6/9	5.5/9
	Category: Process	7/12	5/12	8/12
	Category: Output	7.5/9	6/9	4.5/9
	Category: After	3.5/6	4/6	4/6
	Total (out of 36):	**25.5**	**21**	**22**

Table 9: Comparison of the scores achieved by the tools

As it was apparent from the evaluation, the MRSAT tool was the most appropriate to correspond to the requirements of SMEs. This application provides a relatively easy analysis process and the most comprehensive results from all tools. However it fails to be judged as appropriate for organisations since it does not take any consideration of what

assets are important, and how important, to the specific organisation and prioritise the suggested controls based on that. It also does not provide with any method of assessing whether the suggested controls were successful and what threats still keep occurring and causing losses to the organisation. Second highest scoring was the Buddy System, mainly because of its nice graphical interface and for being the only tool considering the organisations needs and cost of assets when suggesting controls. However the Buddy system does not provide any information on these suggested controls or assistance with their implementation. There is no feedback and updating it is questionable since the lists of assets and recommendations presented by the tool looks rather out of date. Finally the Cobra tool has very few good features, essentially only that the terminology is comprehensive and that the report can be fitted to the users' needs. However there is no suggestion of importance of controls of any sort, which controls are vital, which are recommended etc. The applications output is plainly a list of all the possible controls, again without any explanations on what they are or how they are used.

Another criticism is that none of the tools takes into consideration the industry sector, organisations from different sectors have different security requirements, (e.g. an educational organisation would require less security, but easier employee access, than a military organisation. Finally none of the tools produce any different outputs according to the size of organisation. Size relates to budget (another element that is not considered is the organisations I.T. security budget) as well as costs for controls, these are neglected in all tools. The only tool that considers these two elements is MRSAT which only

considers them to compare the results with other organisations not to adjust the output to these.

4.9 Conclusion

In this chapter the potential solutions for SMEs needing to structure and implement security have been investigated. The first category of solutions was judged to be inappropriate for SMEs primarily since they only provided guidance without adapting to the requirements and characteristics of organisations. By contrasting these solutions to the requirements of SMEs from such a solution it was apparent that an automated tool that assists users with selecting and valuing assets and then suggests appropriate controls was in order. Therefore some of the major RA tools that claim they are appropriate for SMEs were properly evaluated and the output proved that they were all lacking in some of the major requirements, which is probably why RA is not being adopted by SMEs.

The requirements of SMEs, plus those that were identified as good characteristics, and those identified as missing from the existing tools, will be used in the following chapter to constitute the basis for a novel methodology that covers the needs of organisations in automated security planning and efficiently selecting, implementing and assessing the effectiveness of controls.

5 A New Methodology for SME Risk Assessment

In this chapter the design and parts that constitute the novel methodology which is suited to the needs of SMEs from such a solution is discussed.

5.1 Introduction

Chapter 2 established RA is not being adopted by SMEs. By then investigating certain I.S. surveys and the details of the major possible solutions for SMEs, Chapters 3 and 4 established that a successful methodology for SME RA has certain requirements. The following section summarizes how these requirements, identified in the previous chapters, can be grouped together to establish four key aspects necessary in RA addressing SMEs:

- Focus on the characteristics of the SME users. This means it should be easy to use (not getting too technical) enabling a non trained user to perform the assessment, provide the necessary assistance to the user and the process to be relatively short enough so as not to cause disruption, definitely not require multiple people therefore making it expand over multiple days. To provide with the appropriate assistance to the user it is necessary that an automated tool assists the user with all the selections by indicating relations between assets, threats and controls. According to this, the target SME user (and the person described when mentioning 'SME user' from now on in this thesis) is a single person who has been assigned with performing the assessment, coming from the 'business/management' side of the organisation with certainly no I.S. training,

and potentially some limited knowledge of I.T. This user will however have knowledge of the purpose of the organisations I.T. system, the existence and importance of major I.T. assets such as an Internet connection, a website, a print server, a mail server and so on.

- Adapt to the organisation being assessed. In contrast to baseline guidelines and the RA tools evaluated in Chapter 4 that have the similar approach in identifying risks, this framework should consider the actual organisation sector, requirements and characteristics as the basis of suggesting and selecting controls. This solution should address organisation-specific issues that the existing solutions do not, such as considering appropriately the size, budget and value of assets to the organisation, considering impact of risks to the organisation, the organisations desired security requirements/levels and based on these suggest appropriate while at the same time cost-effective controls.

- Produce a comprehensive output. Care should be given to the final output to the user. The framework should provide a concise but comprehensive output report which gives the user the no more than the appropriate information to justify risks and spending to the management, and to assist the user assigned with the task with the setting up of the controls.

- Manage security weaknesses and risks even after the end of the RA. To be successful, information security solutions need to be managed, not simply

deployed (Chong 2003). Management should not end when the appropriate controls having been suggested but also provide the SME with support afterwards. The framework should allow reporting of the effectiveness of controls and appropriate updating of the organisations profile (created by the assessment) in case there is a change in the assets. It should also include an administrative interface which enables the easy updating of the tools lists of assets, risks and controls to ensure an organisations estimated risks and implemented security are always up to date.

5.2 Elements used to address these requirements

There were certain elements conceived which enable this framework to address all the requirements. Before discussing the details of the operation of each of the process engines in the methodology, those elements that will provide the required functionality will be discussed.

5.2.1 Focus on the characteristics of the SME users

Instead of "traditional" methods and mainly the use of questionnaires in order to collect data from the user, this framework makes use of profiling in order to make the whole process more efficient and more comprehensive to the user. The idea of using profiling for I.S. purposes has been introduced by Commoncriteria with their 'Protection Profiles (PP)' (Commoncriteria 1999). According to Commoncriteria, "*A PP is an implementation independent statement of security requirements that is shown to address*

threats that exist in a specified environment". What profiling means is the grouping of similar items with similar requirements together. When designing this methodology profiling was used in several occasions: applications that require the same background assets were grouped together to make *application profiles*, threats that have the same source and require similar controls to protect against were grouped in to *threat profiles* and finally controls were profiled by including all controls that are essentially the same but with slight variations under the same categories (e.g. all controls that assess malicious code were grouped under antivirus, instead of including all possible makes and variations of antivirus software). A preliminary paper that discusses how profiling can be used to simplify the process of Risk Assessment has been published by the author in 2004 (Dimopoulos et al., 2004c)

Finally, an organisation profile is created during the risks analysis which contains all the user-selected information regarding the organisation. This organisation profile is used to store information as it is identified so it can be used by later modules.

5.2.2 Adapt to the organisation being assessed

This is achieved by requiring the user to input specific data which is then used to consider what the organisation needs to protect from more (the threats against the organisation and their likelihood and impact), what budget should be devoted and so on. Such information is the sector, the size and I.T. budget of the organisation. Another required input is what the applications used within the organisation are and a rating of their importance. The importance will be rated in terms of C-I-A to the organisations' operation, this type of

rating is widely recognised as the basis for valuing information (Alred 2001). Moreover, specific rating of price may mislead the user into not considering some cost element (the cost factors range from physical damage to loss of information and from downtime because of a threat occurrence to damaged reputation therefore making the process more complicated and introducing grounds for a false input (Pfleeger 2006)) and provide false results or may require the user to contact other users who know this information therefore introducing delay. To also comply with the first requirement described in this section for ease of use, the rating needs to be performed in such a way that all a user is required to know in order to perform the RA is good knowledge of the organisations function.

5.2.3 Produce a Comprehensive output

As discussed earlier the output needs to include certain elements that are required by the SME user and the management. Such elements are definitely a projection of the cost of controls vs the reduced risk levels to justify such spending to the management if required and also appropriate assistance in explaining what the selected controls actually are and how they should be implemented successfully.

5.2.4 Manage security weaknesses and risks even after the end of the RA

This will be achieved by providing feedback on two issues. The first will enable the user to provide feedback on whether the recommended controls are adequate (for instance, has a threat kept occurring after implementing the controls and how often and what losses has it caused?). This sort of information will adapt the tool more to the organisation by

updating the data in the *organisational profile* therefore re-assess the situation with more realistic data providing a more suitable output each time. This constitutes an element not offered by existing RA solutions but also very useful to SMEs with no full time expert in-house that would not otherwise be able to rearrange their security plan to the new situation. The second type of feedback, also useful for the same reasons is feedback on applications that have been added or removed from the organisations profile, which require re-considering security.

Finally this lack of security personnel to perform this task necessitates for the methodology to be easily updatable so as to be constantly up to date with new applications, threats, their effect and controls, without needing the time and effort to have a member of personnel who is normally assigned with something else to also be responsible for this task.

5.3 Overview of methodology

Figure 53 illustrates how the typical RA process as described in Chapter 2 needs to be altered to include the elements discussed above and solve the problems prohibiting SMEs from adopting RA.

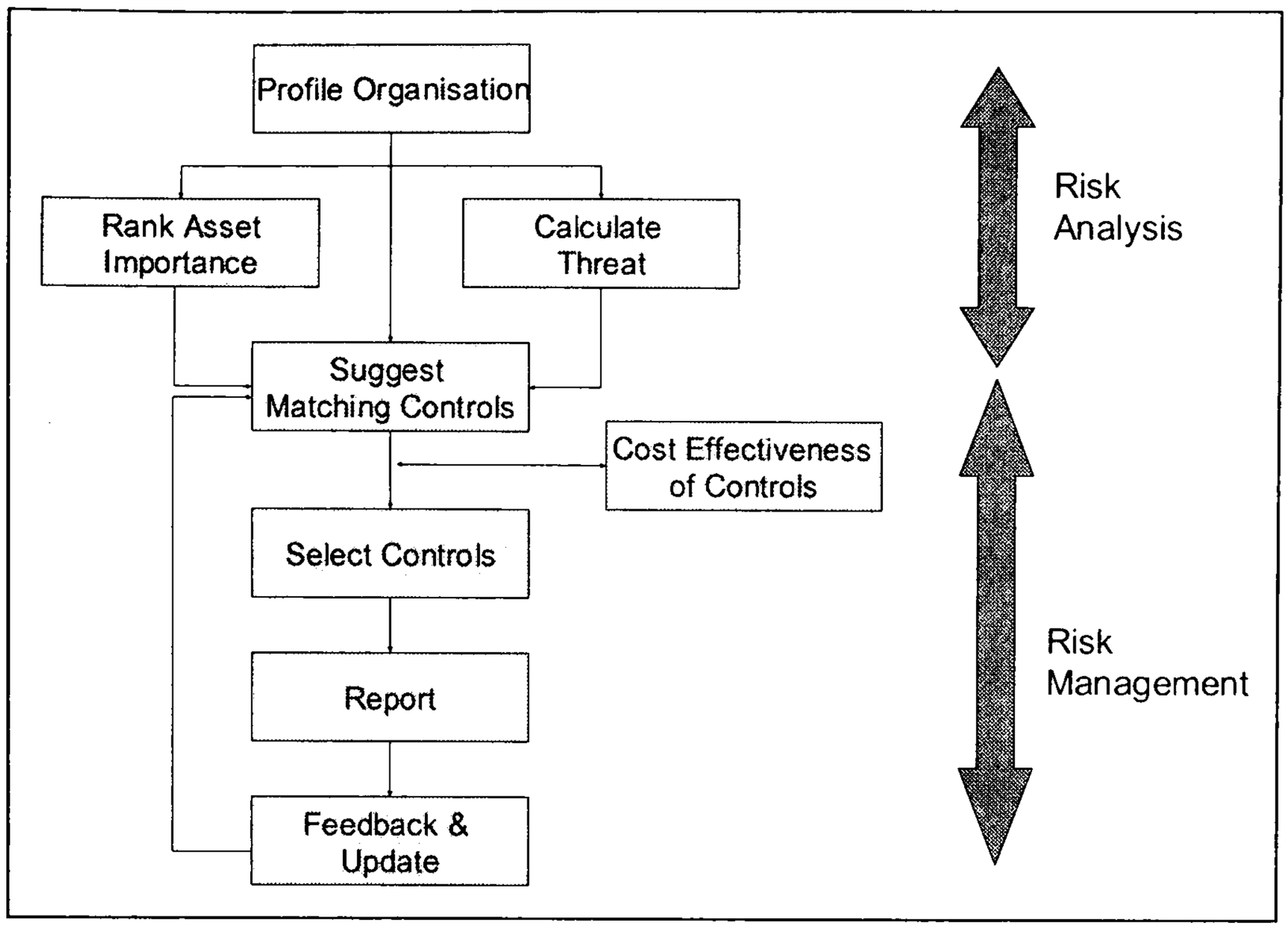


Figure 53: The RA process which suits SME Requirements

The 3 main elements within a risk analysis methodology are Assets (included within applications in this case), Risks and Controls. Risk can be the connection between the applications and the controls. Certain applications introduce certain risks and then certain controls reduce these risks. What is then further needed is to evaluate how important these applications are to the organisation to establish which needs more protection and what the organisation is spending on security controls to choose the most cost effective solutions from the whole list of controls.

This section explains what the steps in the novel RA methodology actually are and the actions they include.

5.3.1 Risk Analysis Phase

This section suggests how the analysis of risks should be approached in the proposed methodology.

- Profile the organisation

  The first part of the methodology aims at gathering the required information on the organisation being assessed from the user performing the assessment, such information will be general data on the organisation and the applications that are used within it.

- Rank Asset importance

  Having obtained information on the organisation, the user is required to rate the importance of the applications selected as existing in order to prioritise the applications/functions in order of importance.

- Calculate threat

  The identified and rated applications are subject to certain threats. Having pre-determined the threats that correspond to the application profiles the user has selected, these threats are awarded points to generate the 'threat scores' that quantify how much each threat may affect the organisation

5.3.2 Risk Management Phase

Following the analysis of the risks, the novel methodology should include these steps in order to manage them.

- Suggest Matching controls

  The methodology needs to suggest controls to the user. Therefore in this part controls that correspond to the threats the organisation is under while at the same time are appropriate for the selected as available applications need to be pointed out to the user

- Cost effectiveness of controls

  Having established which controls are appropriate for the organisations' needs, a final criterion assisting the user with the selection of the desired best options is the consideration of the cost effectiveness of the controls. The user can here consider which controls are cost-effective judging by the suitability of a control to protect an asset and reduce a threat (presented to the user previously), the importance of this control and the potential losses by the threats it is under versus the cost of implementing the controls.

- Select Controls

  Considering this information, enables the user to select the best options for the SME's limited budget. In this section the methodology should illustrate to the user how selected controls affect the risk levels the organisation is under, as well

as how it affects the budget. Once the user is satisfied with the achieved levels for both these, the process is virtually finished and can present an output to the user

- Report

  Because the report is addressing SME personnel with all the characteristics identified earlier, presenting a report with the selected controls to the user does not make the end of the risk management stage. To successfully manage risks, controls need to be implemented correctly therefore sufficient information to realise this should be provided.

- Feedback

  Managing the risks does not end at deploying countermeasures either, and as such, a methodology that aims to overcome problems related with existing RA solutions should ensure that, in the absence of a security expert, the organisation receives the appropriate level of assistance even after the controls have been implemented

The idea behind how controls are selected is, at a certain stage, similar to the philosophy used by CRAMM. CRAMM *"uses the measures of risks determined during the previous stage and compares them against the security level (a threshold level associated with each countermeasure) in order to identify if the risks are sufficiently great to justify the installation of a particular countermeasure*" (CRAMM 2006b). The difference with CRAMM is that after calculating the risk levels the organisation is under, the choice of

controls is left to the users' judgement, having presented them with the appropriate data to facilitate the decision (risk levels for the organisation, applications found within ranked in terms of importance and economic considerations such as ROI and ALE).

5.4 Process Engines

This far the requirements and how the methodology was conceived has been described. In order however to achieve this desired methodology in practice several process engines need to be designed and their inputs and outputs combined together appropriately. The following five process engines have been used to create a framework that effectively addresses all the requirements.

- Organisation Profiler Engine (OPE)
- Application Importance Rating Engine (AIRE)
- Risk Ranking Engine (RRE)
- Cost Effective Risk Management Engine (CERME)
- Feedback/Update Engine (FUE)

This section will describe the function of these process engines before moving to the discussion on the background components (i.e. those components that perform the background calculations that allow for the process engines to present the desired output to the user). The databases and other background engines and mathematics used to produce results will be discussed in detail in the architecture chapter. For the purposes of this chapter, which are to illustrate the functionality of the framework, any input to the

process engines that is either created by the framework or predetermined within the prototype will be referred to as 'system' and any input required by the user will be referred to as 'user'.

5.4.1 Organisation profiler engine

This engine is required to perform the initial profiling of the organisation. To achieve this, some specific information is required and the input source for this engine is the user. The following section will describe what information is needed and how it is used.

5.4.1.1 Process Engine's Required Inputs

The sector an organisation belongs in, as previously mentioned in Chapter 2, is inherently related with the level of threat the organisation is under. To illustrate this, according to the findings of the Symantec survey, the 'Accounting industry' receives 18% of the targeted attacks while at the same time organisations belonging to the arts/media sector only receive 1% of the entire spectrum of attacks. This methodology attempts to first evaluate what levels of threat the organisations are under therefore it is logical that the first factor in estimating threat will be the inherited risk due to the industry sector an organisation belongs to.

The size of the organisation is required to determine the cost of controls when examining cost effective solutions. Even the simplest of controls is relevant to the organisations' size, from physical controls such as safe doors to software controls such as antivirus, all

their costs rise according to the size of the organisation since the larger the organisation the more of them are required. For the same reasons of evaluating the cost-effectiveness of the possible controls, the I.T. budget is required at this stage. Furthermore the I.T. budget, combined with the number of employees and certain surveys that point out the spending of organisations belonging to specific industry sectors per employee, can determine a recommended minimum security spending to the user in case they are not sure what percentage of the budget they should devote to I.T. security.

Another novel point of this methodology is to consider what the I.T. security requirements of the organisation are. It has already been discussed that different organisations have different I.S. requirements and for instance an academic organisation would require easier access for its users in contrast to the more intrusive and need for constant security (e.g. identity authentication) within a military organisation. This methodology, which aims at assisting organisations structure their security, should consider which of the approaches the organisation being assessed desires in order to suggest more appropriate controls later on.

Finally, the main information required from the user here are the applications found within the organisation. The user will be required to declare what applications/types of data and functions can be found within the organisations' I.T. infrastructure. These introduce the corresponding risks towards the organisation..

5.4.1.2 Use of Collected data

What the Profiler engine essentially does is gather specific information about the organisation from the user and then store it in specific locations and order (the organisation profile) so as to enable the following process engines to later on, when required, access and retrieve or update this information. Figure 54 illustrates what information from this first stage is needed by which following stage.

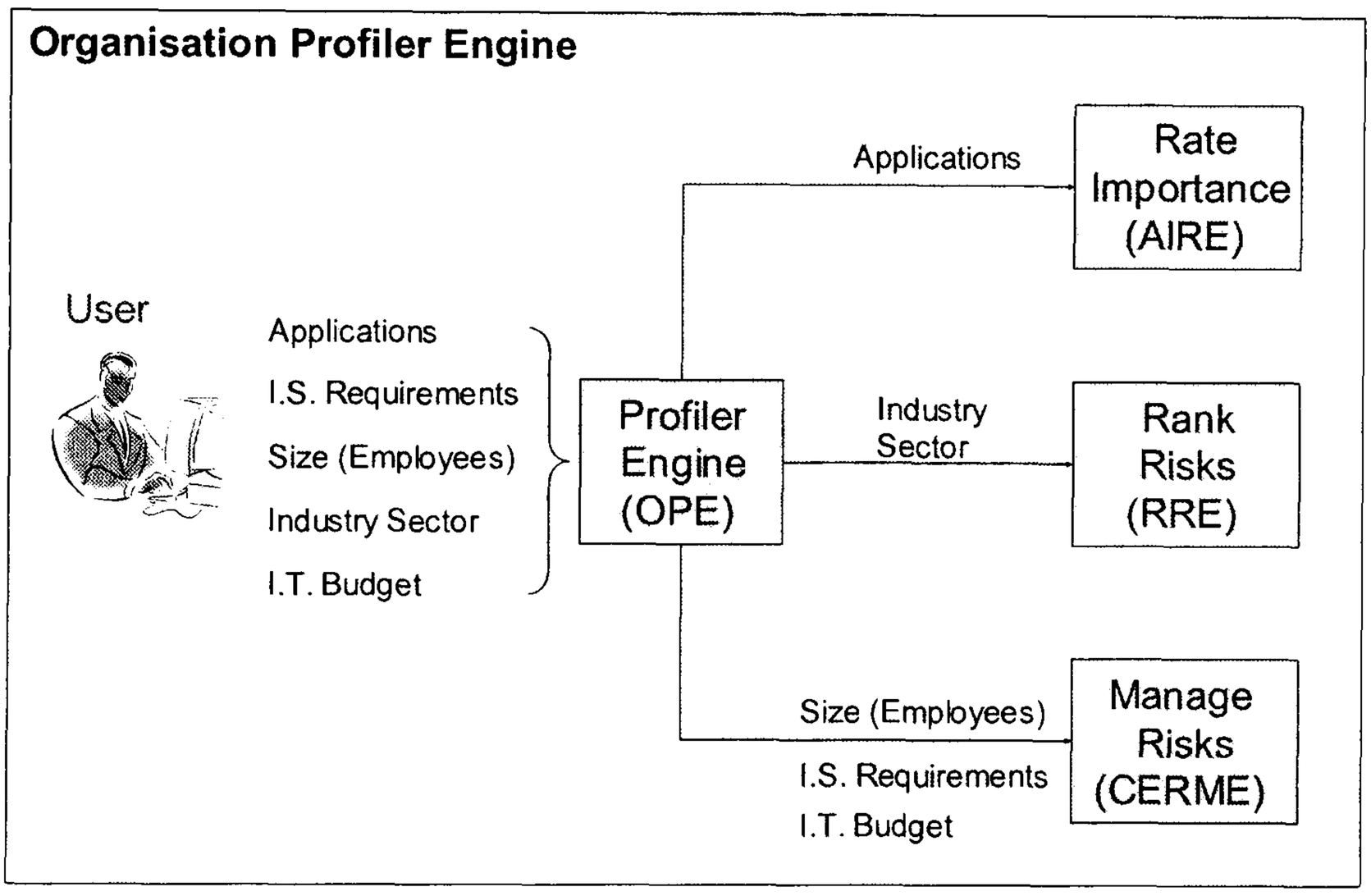


Figure 54: Relationships between Profiler Engine and later stages

To illustrate why this specific data is required from the user, this process engine is the product of reverse engineering, meaning that the information needed by the remaining modules was identified and this engine provides the interface for the framework to acquire this information. The user selected applications that exist within the organisation will at a later stage be required by the AIRE engine so that the applications' importance is rated. The industry sector information is required by the engine that calculates risks to

provide an initial input. The size, I.S. requirements and I.T. budget information are all considered when selecting controls in the CERME engine. The CERME engine addresses SME requirements of ease of use by not requiring technical details (but instead hiding it in the background i.e. recognising technical information according to applications) and length of process by introducing profiling instead of lengthy questionnaires

5.4.2 Application Importance Rating Engine (AIRE)

The function of this process engine is straightforward: It should first access the 'organisational profile' and retrieve the selected as 'existing applications' and then prompt the user to rate their importance.

5.4.2.1 AIRE's Required Inputs

There are three essential inputs to the AIRE process engine, all related to each other:

- First there is the input, from the previous engine, of the applications/functions that exist within the organisations I.T. infrastructure.

- This is complimented with help text. This is predetermined text within the tool that is linked to each application, this process engine retrieves the text that is relevant to the selected applications and provides information on how such applications can be compromised and what the results are. Providing information

like this to the user makes the scoring of the applications more accurate as it ensures the user will not misconceive how a compromise of an application and its related assets might affect the organisation.

- The applications and the 'help text' are then presented to the user who is required to consider how a compromise of each application may affect the organisation and therefore rate the importance of each application on the three fields described earlier: what the effect of loss of confidentiality could be, what the results of a compromise of integrity, and how the organisation is affected if application availability is lost.

5.4.2.2 Use of Collected data

The sole output of this process engine is an updated 'organisational profile' where the users' ratings of applications importance have been added next to each of the previously selected applications. As Figure 55 illustrates, this output provides the basis for two considerations in the subsequent engines.

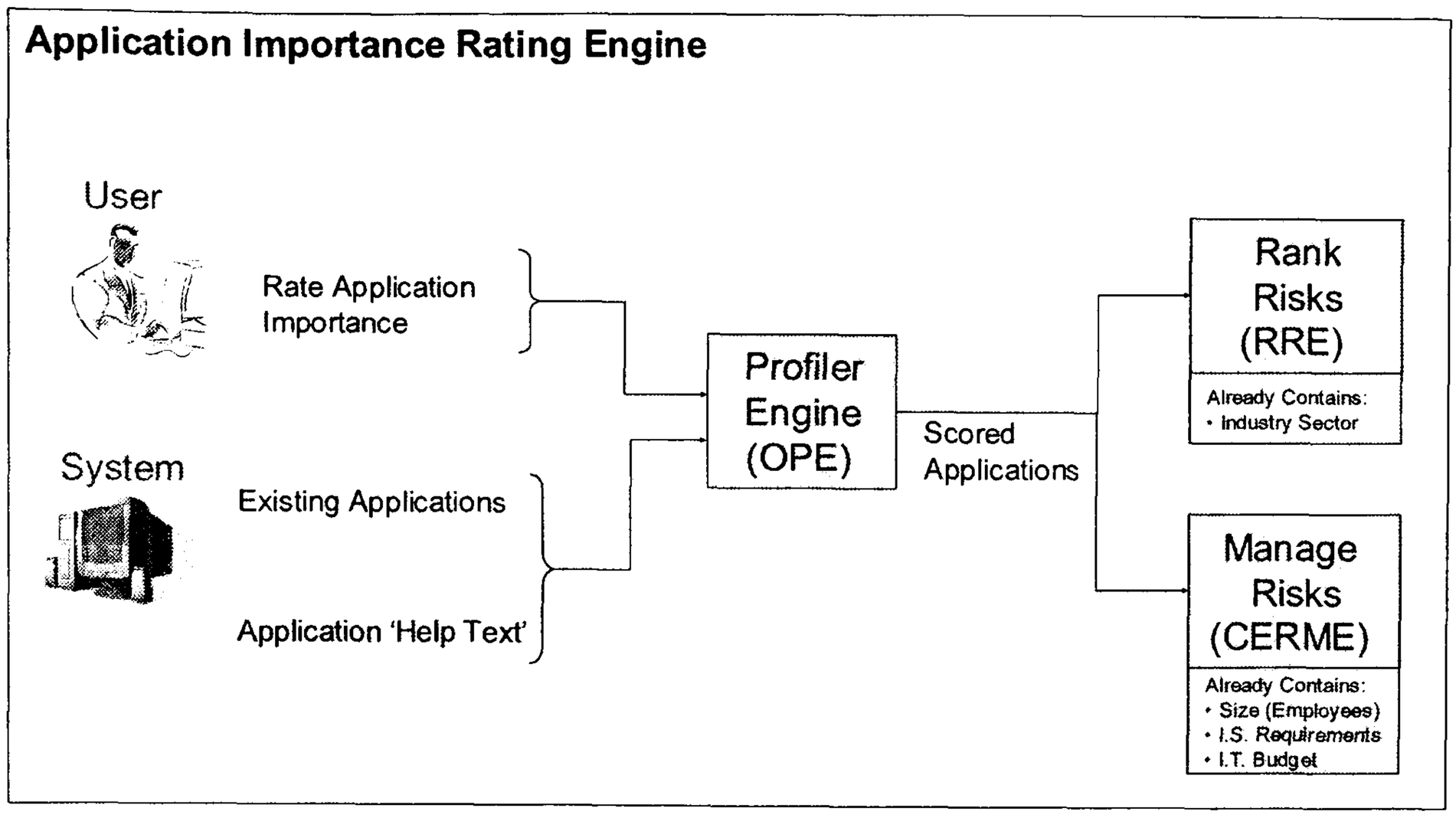


Figure 55: Scoring applications using the AIRE

Firstly it constitutes the second element that determines the level of threat the organisation is under based on predetermined lists of threats that correspond to applications (essentially threats that have been introduce because of the existence of an application). Furthermore the output of the AIRE engine provides one of the inputs to the CERME, the engine that assists in the selection of controls, since one of the criteria, the recommendation of appropriate controls by the framework to the user, is naturally that the controls are suitable and applicable to the available applications requiring protection. The SME requirement addressed by the AIRE engine is to provide assistance to user (partly since at this stage the user is assisted with understanding the importance of applications and rating it more accurately).

5.4.3 Risk Ranking Engine

This process engine (Figure 56) utilises the data output from the two previous engines (Industry sector and existing applications rated in terms of importance to the organisation) combined with survey data to establish how much the organisation is at risk from existing threats. Risk is what connects the analysis with the management.

5.4.3.1 Process Engine's Required Inputs

As discussed earlier, the industry sector that an organisation belongs to generally determines how likely it is for the organisation to be the target of an attack. Furthermore, each application/function that constitutes the organisations' I.T. infrastructure introduces certain threats itself. The new element added here is predetermined values for threat impact. These are initially (since later on in the feedback they are adapted to the organisation according to the users input) taken from survey findings and are a product of the reported annual losses due to threats and the frequency of occurrence of a threat. The reason behind using all this information for estimating the risk levels is that there was a need to adapt these values of risk to the organisation as much as possible since later on it is the basis for selecting controls. Using the traditional values on effect of a threat and frequency from surveys would give a threat score for each threat which however would be the same for all organisations. The requirement for this methodology was to assess the requirements of different organisations, operating differently and relying more upon different assets (e.g. there is a different dependence, and associated losses, of a bank to customer details than of a university). Therefore the specific risk associated with an industry sector an organisation belongs to was considered and furthermore the threats and

potential losses because of the specific applications and types of data the organisation being assessed has that make its environment unique from the rest and especially differentiate it from organisations from different sectors.

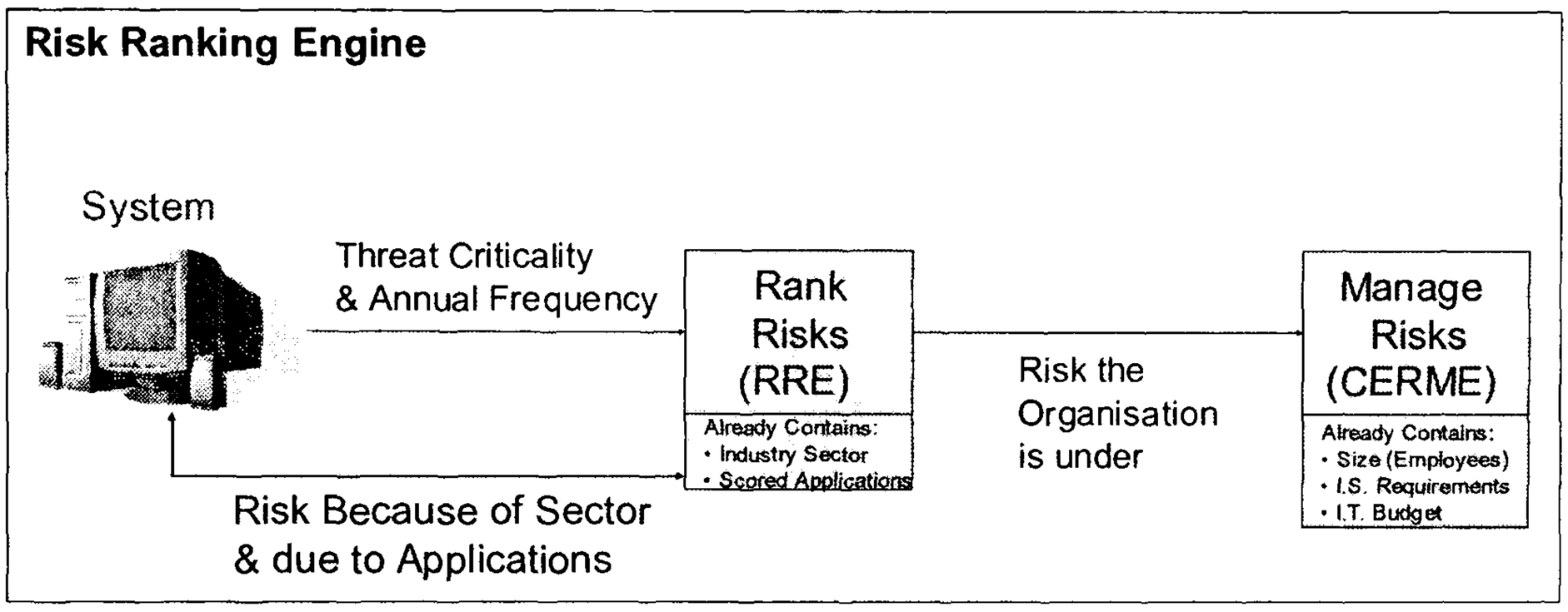


Figure 56: Risk calculation using the RRE

The RRE engine addresses the requirement of SMEs for Risk Impact Analysis and consideration of threats specific to the organisation.

5.4.3.2 Use of Collected data

All these factors sum up to produce a threat factor for each threat which is the main function of this module. These threat factors are all progressed to the Risk Management engine which is where they find their primary use.

5.4.4 Cost-Effective Risk Management Engine (CERME)

The previously described process engines mainly constitute the risk analysis part of the framework and gather all the required data and process it so as to feed it to this process engine. The CERME process engine is basically the risk management part.

5.4.4.1 Process Engine's Required Inputs

This engine (Figure 57) is the 'heart' of the RA framework, its basic function is to gather all the information from the previous modules and transform it to useful information for the user. The information gathered includes, organization budget, size, I.S. requirements, all available applications and the risk levels the organisation is under. The reasons why all this information has been gathered is clear when looking at the output of this engine.

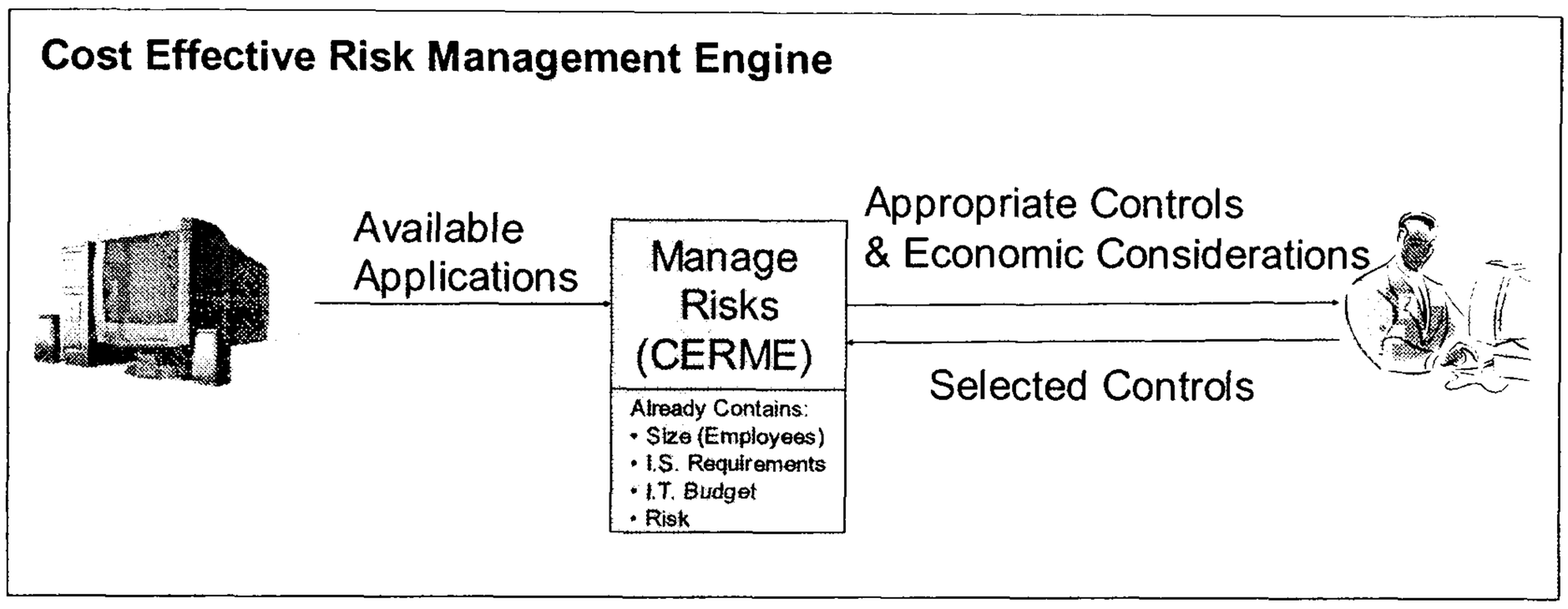


Figure 57: Selecting appropriate controls with the assistance of CERME

5.4.4.2 Use of Collected data

As Figure 39 illustrates, the use, in this process engine, of all this collected data is to be presented to the user in a comprehensive way, so as to facilitate the users' decision of what controls should be implemented (addressing the SME requirements for assistance in choosing controls and suggesting cost effective controls). In order to achieve this, while at the same time cover all the requirements that have been identified that an RA methodology should include, this data presented to the user is:

- The 'threat profiles' including Annual Loss Expectancy. To begin with, the user should be made aware of the level of risk the organisation is under and what the likelihood of occurrence is. Also the system should indicate what potential losses may result should these risks occur. It is required that this data is presented in a comprehensive manner in order to be useful, therefore the idea conceived here is to include a graphical display which progresses from green to amber and then red and the threats are illustrated on it being the more into red as the threat increases. Equally when controls are chosen later on the threats can decrease into green according to the effect of the control on each threat.

- The framework needs not just to present a list of all available controls but should distinguish and assist the user by presenting those controls that correspond to the available applications and the specific risks the organisation is under. Also before distinguishing those controls the framework should consider what the I.S. requirements of the organisation are, security or easier access.

- Having presented the user with only the potential losses from threats and a list of all the appropriate controls (as indicated in various sources such as ISO 27001 which includes a comprehensive overview of all controls, Muller (2003) that focuses on network security and Garfinkel (1997) focusing on server security), the framework should also present to the user what the cost of controls is and therefore assist them in selecting the most cost-effective options while at the same time reducing the risks at the desired levels. Having been illustrated this

information, an option for the user is also to accept the risk (Meritt 1998) if the level of risk or the ALE does not justify a required high investment for securing this risk. Addressing an SME user, the framework should avoid leaving the budget allocation entirely up to a user who is not particularly security aware, it will be therefore useful to also provide recommendations of what budget should be spent on security controls by the organisation. Considering the size sector and budget the system can suggest a minimum security spending based on survey data of what other organisations with the same characteristics do.

Therefore the whole concept of the CERME is to display the current risks and risk levels to the user, then suggest what controls, based on statistics, correspond to the organisations requirements by illustrating those that match the specific identified risks and applications. The controls will be ranked also after considering the level of 'intrusive/hard' security the organisation requires. This will have enabled the user to select controls that are matching to the organisations characteristics, what the framework should now do is suggest what budget should be devoted to I.S. controls and allow the user to experiment with different configurations, illustrating each time the cost of controls against the budget, the potential loss because of a threat and the effect the controls have on the existing identified threats. This should enable the user to eventually select the most appropriate controls that reduce the risks to acceptable levels while at the same time not exceed a certain budget or the actual losses from a compromise. This provides the organisations that will adopt this methodology with a form of ROI consideration when selecting security solutions. By establishing ROI data, the

management can make more informed decisions regarding which controls to implement, based upon initial cost, but also on the current threat exposure of the organization (Hamilton 2002).

There is the possibility for the tool to suggest certain controls according to the highest ranking threats and the corresponding controls and budget. However for the prototype it was selected not to use this approach, as the appropriateness of its output would be questionable, introducing some of the difficulties related with the existing RA tools and not considering what the organisation is actually interested in protecting more. Thus it is preferred to present the user with as much data as possible to allow them to make the selection. Such an addition is still possible, but for the time being it was preferred to use human judgement as means of selecting appropriate controls.

5.4.5 The overall output

It was identified in the requirements that the output of such a framework should be a report with all the necessary elements considering the described characteristics of the users that it addresses and aims to assist.

For this reason, the report of this framework includes certain key elements:

- The applications identified as existing within the organisation and a graphical representation of the levels of risk they are under.

- Naturally this is followed by a list of the selected controls, including their costs and another graphical representation of how much the risks have been reduced after the controls have been applied.
- Finally another essential element in such a report is the required explanations on how to set-up, configure and use these controls. This information will be presented to the user as selected links to resources appropriate for the SME target user.

Therefore the SME requirements for a comprehensive output and deployment assistance are addressed by this engine.

5.4.6 Feedback & Update Engine (FUE)

This engine provides an element identified as missing from the existing solutions to the SME that uses this framework. That is the ability to also maintain secure and adapt to situations that were not foreseen or did not even exist when security solutions were initially considered and implemented.

5.4.6.1 Process Engine's Required Inputs

This is a supplementary process engine, as it is not part of the actual RA process and does not need to be run when performing the assessment. It is a "support" engine, only used after the RA should certain specific situations occur, this is why its function shall not be

analysed as with the previous process engines but instead both the input and output information is described in brief. The FUE performs three distinct functions that each requires different inputs and produces different outputs. These are:

1. Assess the effectiveness of the implemented controls. In order to check if the implemented controls have been successful, this module requires the user to declare what threats have occurred during the period that the controls have been applied. The controls have been selected according to the risks the organisation is under which in turn are related to survey data on the annual frequency of a risk occurring and the potential losses. Here the framework can estimate annual occurrence rates and losses due to risks which are specific for this organisation. If these exceed the ones that were the basis for the selected controls then the framework should re-assess the situation by calculating this time the risks based on the actual figures provided by the user. This way selected controls can be re-considered based on more realistic data.

2. Reconsider security if the organisation profile is altered, that is if new applications are introduced or old ones removed. Both of these situations can have an effect on security. The first might leave new applications vulnerable or introduce new risks while the latter may leave the organisations with controls in place that are no longer needed. To ensure both these situations are avoided this framework enables the user to modify the applications within the 'organisation profile' and reconsider the risks the organisation is under and the selected,

required controls. A necessary requirement here is to enable the user to do this without wasting user time and constituting a disruption to the normal operations therefore not requiring the user to go through the entire process from the beginning.

3. Easy update to the framework's data with new information. This is required for two reasons. Firstly the data used to perform the calculations behind the framework is based on the most recent survey data, especially on the risks and their likelihood and impact. It would be useful to be able to perform a straightforward update to this information when newer is available. Secondly, there is the need for the framework to always be up to date with available applications and controls since there is no security expert to do this for SMEs. Thus the input here is all the aforementioned data but through an easy to use administrative interface. The primary goal is to enable the update of the framework's data without need rebuilding the whole application, acquiring it, installing it and performing the whole process again.

Even though they were not identified anywhere, this functionality should be included to any tool that claims to offer management of risks, since management does not end when the controls have been deployed. Risks continue to exist even after this and any of these three situations described can have a disastrous effect to an organisations security if they are not considered. What is stressed here is that risk management should be ongoing and occur as threats occur, assets changed or new data becomes available, if instead it is

performed periodically it leaves an organisation vulnerable and exposed from the time any of the three happens to the time the re-assessment takes place.

This process engine even enables SMEs that have already deployed security solutions to check the appropriateness of the selected controls by going through the whole framework and then suggesting to this engine certain threats that have occurred and see what improvements they can deploy to the current security. This engine therefore covers the SME requirement for dynamic feedback and update.

5.5 Other Components

In order to achieve the desired results, there are some additional engines that need to be used in the background by the methodology. These are needed to perform the mathematical calculations, the storing of information and the tasks associated with creating and printing a report document. Since established programs that perform these functions already exist and work well with existing programming languages (using which the methodology will be implemented into a prototype), there is no need to produce new since there is the possibility to use the existing. Because there is the need for these programs to exist within the system that the framework is installed, all three were chosen to be elements of MS Office since it is most commonly found on PCs than any other similar application. Thus, Access was chosen to be the database engine, Excel was used to perform all the background calculations, and Word was the tool that provides with a report at the end of the assessment.

5.6 Conclusions

This section summarizes how, by using the process engines described in this chapter into a framework, all the requirements identified as needed from an RA tool were assessed.

- The methodology included many elements throughout to achieve the first requirement and enable its use by, non-experienced in the sector, users. The use of profiles is the main element which simplifies the process as it eliminates the technical part of an RA and also significantly reduces time needed to perform an assessment. Using applications instead of specific assets as means for identifying threats makes the analysis process suitable for every user with some knowledge of the organisation. Rating the applications importance in terms of importance of C-I-A instead of actual economic value also simplifies the use of the tool and widens the spectrum of personnel within the organisation that are able to perform the analysis. Furthermore, including graphical displays and maximum assistance and backup data to the user throughout the process and particularly with the selection of controls, a stage which includes significant decisions by the user, has reduced the complexity compared to traditional RA.

- Probably the most important addition to this framework that overcomes problems related with existing RA methodologies and their suitability for SMEs is the inclusion of cost effective considerations when selecting controls and the actual suggestion of controls based explicitly on the organisations needs, namely both the exact levels of threats the organisation is under (based on both sector and

applications within) as well as the actual applications that can be found within the organisation (and at the same time considering which applications are the most important to the specific organisation).

- The output report by this framework is short but practical as it includes all the data identified as necessary in the requirements. A graphical illustration of the risk and how it can be reduced with the selected countermeasures (and their cost), in order to raise awareness and justify spending to the management. A description of the nature and operation of the controls, together with external links on how they should be implemented, configured and used, will enable the targeted SME user to select, acquire and deploy security solutions.

- The feedback and update process engine enables users to re-assess the organisations I.S. situation if the selected measures have not been successful or if there is a change in the organisational structure, providing real-time support to the SME management that does not employ someone who can otherwise do this.

Chapter 6 will illustrate how the process engines of the perceived methodology will be used in practice to constitute a working prototype RA tool.

6 A Functional Prototype of the RA methodology

This chapter will discuss how the novel RA methodology proposed in Chapter 5 has been realised in a framework and working tool. The resulting prototype has been named PRAM, which stands for Profile-based Risk Analysis Method

6.1 Introduction

A prototype is a working sample system, the visual representation of how the system will look and function after it is complete. Therefore the main purpose of this prototype is not to have exhaustive databases or precise values for, as an example, costs of controls. That would be the purpose of an actual commercial implementation of this methodology. Here the aim is to create a prototype that illustrates the effectiveness of the methodology in addressing the identified requirements and (at a later part of this thesis) allow the comparison of this novel methodology with the existing solutions.

6.2 The Architecture Topology

This section describes what operations are performed throughout the prototype in order to collect the required data and present the desired output to the user. Figure 58 illustrates a top level view of the actions that are performed within the PRAM prototype and what data is communicated between processes.

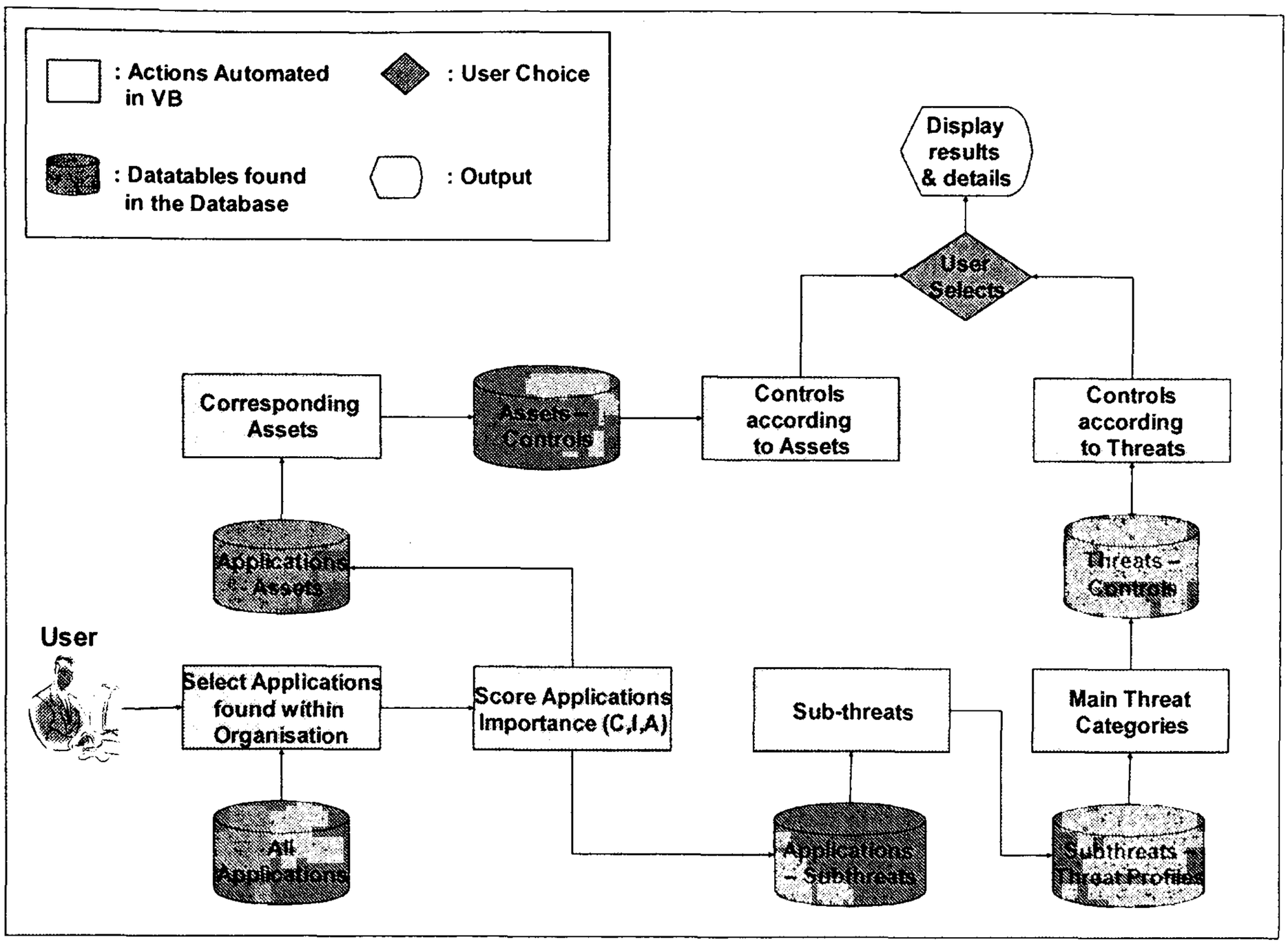


Figure 58: The process used in PRAM

The analysis begins when the user selects what applications exist within the organisation on the PRAM interface, based on a database of possible applications.

As already discussed, using the application profiles, but knowing what assets typically lay behind these applications simplifies the RA process. This way it is not required for the user to rate the importance of let's say, a web server, the server O.S., and the information within, but simply the importance to the organisation of the website (which is made up of these assets but is easier to be understood and its importance appreciated by the non-security, or even I.T. trained, SME user).

Having created a list of the available application profiles within the organisation, it is required that the user scores each application's importance to the organisation in terms of

Confidentiality, Integrity and Availability, the three recognised, within ISO17799, measures of valuing asset importance also used to rate assets importance in CRAMM (Yazak 2002). The applications are therefore now ranked in terms of importance and the assessment then takes two paths: the first is based on the threats the organisation faces and the second on the assets that exist within the organisation.

6.2.1 Route 1: Threat based, having rated the importance of applications.

The system looks up a database of 'sub-threats' that correspond to each application. Sub-threats are threats that when grouped together will constitute the threat profiles. For example, sub-threats virus, Trojan, worms and adware all constitute the threat category 'malicious code'. Thus by knowing the importance of an application, the system looks up in the datatable that links applications with sub-threats which can effect these applications and identifies all threats introduced to the organisation because of this application. Sub-threats have a score associated with them, based on survey findings, therefore the system will then look at the next datatable which will link sub-threats to the threat category they belong to and add up each sub-threats threat score to make up the overall threat levels for each threat category. As described in Chapter 1, based on the definitions of the DTI, there are essentially 5 main threat categories that include all the possible sub-threats. These are Malicious code, Insider, Outsider, Theft or fraud and Accidental (use main threats for simplicity of the on-screen output the user sees as a list of all threats would be inconveniently long). Having identified the overall threat, the system proceeds into looking up a datatable which links threats to controls. The user can use a visual interface illustrating the risk levels the organisation is under to decide which

threats they wish to address and select controls from a list of those that correspond to each threat.

6.2.2 Route 2 Asset based, having rated the importance of the applications.

Starting again from the applications rated in terms of importance, the system will look up at a database which will link each selected application with the assets that typically underlie this application. This list of assets does not need to be exhaustive but typically each application will have certain assets behind it such as hardware, software and information assets. Having built a table with all the existing assets, rated in terms of importance (by the user), the system will link these, through another datatable with the controls that correspond to these assets. In the same way as in route 1, it is preferable for simplicity to the users if the list of assets is not displayed to them but the applications instead. This way the user has the option to select applications according to the applications/business functions they mostly wish to protect.

6.2.3 Combining the outputs of the two routes

Both these routes outputs are graphically illustrated to the users allowing them to select from a list of controls that is specifically adapted to the risks and the assets of the organisation. The system presents only those applications appropriate and all the necessary support material to allow even the non - security trained SME user to select and implement appropriate controls.

This part aimed to give an overall idea of how the framework operates. Specific details regarding how controls are linked to applications and threats, how threat scores have been assigned, why five threat categories have been chosen to represent all sub-threats at the graphical display and what data is presented to the user which enables the selection and implementation of controls will be discussed in the appropriate parts of the following sections, where a more in-depth description of the tools modules is presented.

6.2.4 Linking of threats and applications with controls

In a fully functional (commercial) version according to the type of assets that are listed behind the application-profiles (i.e. information, software and hardware) assets will be linked with controls that have an impact upon this type of asset. As an example an antivirus has an effect on assets belonging to the information and software categories but not to hardware assets (meaning that it has no physical effect upon hardware) (Tipton 2003). A similar approach will be taken when linking threats to applications. E.g. a virus will have an effect on information and software assets (and therefore to applications that have such underlying assets) but not to hardware. Since these compromises have been made for the prototype and the underlying assets have not been included, for the framework's purposes these specific links have been made based on background literature which illustrates which applications are effected by what threats and what controls need be applied for each application and threat.

This part aimed to give an overall idea of how the framework operates. Specific details regarding how controls are linked to applications and threats, how threat scores have been assigned, why five threat categories have been chosen to represent all sub-threats at the graphical display and what data is presented to the user which enables the selection and implementation of controls will be discussed in the appropriate parts of the following sections, where a more in-depth description of the tools modules is presented.

6.2.4 Linking of threats and applications with controls

In a fully functional (commercial) version according to the type of assets that are listed behind the application-profiles (i.e. information, software and hardware) assets will be linked with controls that have an impact upon this type of asset. As an example an antivirus has an effect on assets belonging to the information and software categories but not to hardware assets (meaning that it has no physical effect upon hardware) (Tipton 2003). A similar approach will be taken when linking threats to applications. E.g. a virus will have an effect on information and software assets (and therefore to applications that have such underlying assets) but not to hardware. Since these compromises have been made for the prototype and the underlying assets have not been included, for the framework's purposes these specific links have been made based on background literature which illustrates which applications are effected by what threats and what controls need be applied for each application and threat.

6.2.5 Compromises

Since this is not a proper commercial version of the software but a framework to support the PhD research, two compromises have been made when converting the methodology into a software tool.

- Threats and underlying sub-threats: For the purposes of this prototype, the sub-threats have been left out. The system essentially links applications straight to the five main threat categories themselves which does not make any difference to the process from the users' perspective since both the user input (applications and scores) as well as the output (display with the main threat categories) will be the same. It does however simplify, (essentially make shorter) the background calculations. If the subthreat data was to be used, survey data for each of the subthreats importance would have been used and then all added up to each main threat category. For this prototype survey data on the five main threat categories was used directly, which saved having to add up all the numerous sub-threats to establish the threat levels

- Applications and underlying assets: The second compromise for the purposes of simplicity of the prototype is similar to the first. For this prototype, applications are linked straight to controls instead of using underlying assets in between. This way for example, a website is linked to an antivirus, firewall, encryption of stored data etc instead of linking the website, again for example, with a web server an O.S. and customer information, then the O.S. to a firewall and an antivirus and so

on. Again this compromise does not require a different input or present a different output to the user, but simply saves from increased complexity in the underlying databases. Ideally if a commercial working model of this framework was to be created, these compromises would be addressed to get somewhat more accurate results.

- Quantifying a lot of the elements related with a RA (such as the effect of threats and the cost of controls) is inherently difficult when performing a RA. There are many factors that cannot be calculated as for example when calculating the effect of a threat occurring, it is relatively straightforward to evaluate the costs due to damaged hardware, software and potentially information can also be assigned a price. There are a large number of factors however, such as loss of customer confidence and damaged reputation that simply cannot be precisely calculated when evaluating the effect of threats (GAO 1999). Furthermore attempting to estimate the precise cost of controls is difficult since such costs will change very regularly. Therefore in this RA framework when such figures are assigned to threats or controls, they are not meant to be precise values, they are however designed to inform and illustrate to the user the relative effect of threats and cost of controls to inform and raise awareness on these issues. In a fully-working model of this framework care should be taken to match these figures better to real-life figures.

6.3 Implementing the methodology

What the user sees when assessing risks and selecting controls is the interface of the prototype. This was designed using Visual Basic .NET 2005 to provide a graphical, user friendly, simple interface. However most of the intelligence of the idea is based on the architecture (i.e. the background idea which eliminates all the setbacks of existing RA tools) the database structure and the use of Excel and Excel calculations. What the Visual Basic coding does is to display these elements to the user, obtain certain selections and then display the results again. All the functionality of displaying details on applications, assets and controls, the effect of threats and controls etc is purely based on the database structure, and all the calculations and results on Excel. The function of the GUI is to simplify all this for the user. The database contains all the data and Excel performs the calculations. It is, however, the VB interface that ties the whole framework together (Figure 59) by acquiring the remaining missing bits of data from the user and performing complex database handling and Excel and Word automation.

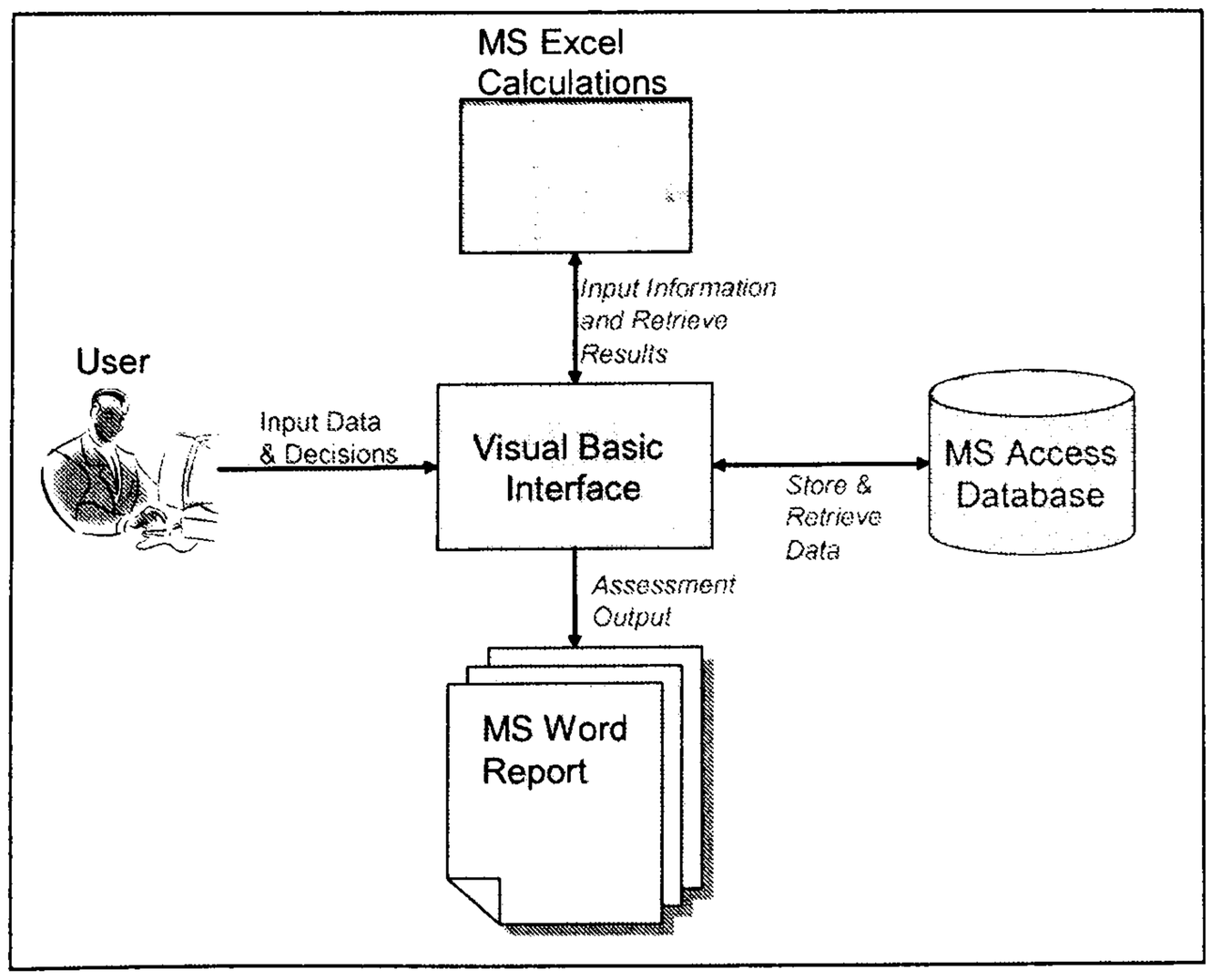


Figure 59: The interaction between processes in PRAM

Using technology like Excel and Word for these purposes was simpler from a development perspective. A commercial version of PRAM would not use them.

6.3.1 Data and Report

Before proceeding to discuss the calculations found in the background of PRAM, this section describes what background information is stored in PRAM's database and what in the report provided to the user.

6.3.1.1 The Database

The database tables together with a large group of SQL queries introduce a large amount of PRAM's functionality. The database includes all the information that at various stages of PRAM is presented to the user such as the lists of applications, threats, controls and store the user selected applications and controls to new database tables which can then be used by the modules. These tables also include the locations in Excel where either an applications importance score or a controls effect has been stored in Excel (in order to consider its value in a mathematical equation to produce a result visible to the user) enabling this way the system to alter the selected applications or controls when necessary by knowing where new values should be stored to overwrite the old ones.

6.3.2.1 The Database tables

Figure 60 illustrates what tables exist within PRAM's database and how they are related.

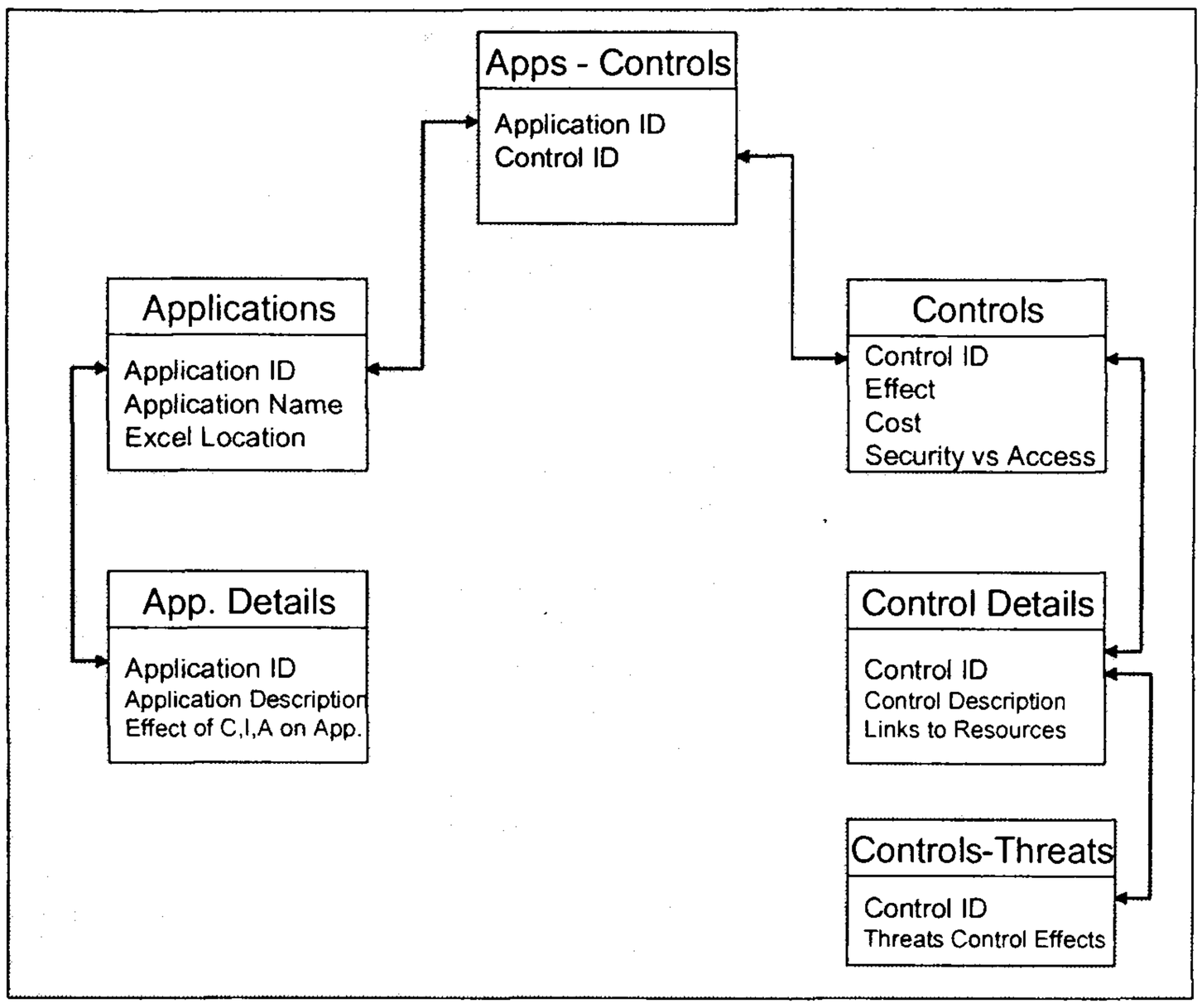


Figure 60: Tables found within PRAMs database

As far as the tables are concerned there is one containing all the applications, their unique identifier and the location in Excel where the importance score associated with that application should be stored. Also as far as the applications are concerned there is a table with all the descriptions of the applications and a description of what might breach of C-I-A mean for each application, these are used as help material in the handler module.

The next set of tables in the database is related with the controls, thus we have one table which includes all the controls together with their effect, cost and how robust it is (ranked from 1 to 3 in terms of low, medium high). This is used to rank the displayed controls if the user has selected productivity, what it means is how easy is it for users to 'live' with this control meaning how much in the way of working does it get (e.g. employing a clear desk policy will require the user to have to go through the records every time a document is required therefore slow them down). Therefore the values can be from 1 (once

configured there is little left to do such as antivirus), 2 (it will keep requiring some user input, such as firewall) or 3 (it will always require the user to provide with input such as biometrics (Nanavati 2002)).

Furthermore there is a table with the relations between controls and threats (i.e. what controls have an effect upon which threat). Another table includes the implementation details for each control, included in the report so as to give some additional assistance to the user. Finally there is again a blank database table where all the user selected controls are stored together with, the main purpose of this table, a generated by the tool cell location where the controls' effect has been stored in Excel element 5 described earlier. This table is looked up every time a control is removed in order to have its effect also removed from Excel and therefore return the total threat score to its previous value.

With the use of SQL queries the system is able to join different database tables therefore illustrate to the user controls that correspond to selected threats and applications, assisting the user with the selection of appropriate controls as described earlier. Finally, using databases enables the update of the tool with newer data without needing to make any changes in the software which would be more complicated and require a specialist to perform as well as more time-consuming. Using databases introduces several ways straightforward updating can be performed.

6.3.1.3 The Output Report

Since MS Word is a word processor fully compatible with Visual Basic but also that exists in the majority of computers today, it has been chosen to be automated by PRAM in order to provide the user with an output report against other software that could perform the same task (such as 'Crystal Reports', a component of Visual Basic 2005, which would however need to reside on the PRAM users' computer).

6.3.1.4 Elements in the report

The report provided by PRAM starts by including a list of the applications found within the organisation as selected by the user supplemented by a graph, prepared in Excel illustrating the initial threat levels the organisation is under. The second group of information included in the report are the selected controls together with another graph which illustrates how the threat levels have dropped after the controls have been implemented. Finally there is the support, to the selected controls, data which includes a description of the control together with links to websites describing how to implement and configure each control.

6.3.2 Calculation of results

Excel is the "heart" of the prototype that performs all the calculations according to predetermined or entered by the user, and provides the results which are transformed to the graphical illustrations that the user sees on the interface. Furthermore, Excel provides functionality in the easy updating of the tool (e.g. when new surveys come out which

indicate different attack trends or percentage of threat occurrences) one can easily update the tool by altering the spreadsheet values

6.3.2.1 Handling of equations inputs and outputs by PRAM

Through VB commands the Excel template is opened by PRAM, and for each item the user selects or inputs in the interface, the system looks up a database with the cell locations this item should be stored and enters it in Excel. Similarly when the output of a calculation in Excel is required by the system so as to be presented to the user, these locations of the equations outputs are already known to the system and therefore all that is required is to open the spreadsheet, acquire the value already in the predetermined cell and store it in a variable which can then be utilised accordingly in the software.

6.3.2.2 Included Elements

Excel was judged appropriate to be used with PRAM for making financial calculations and displaying their results graphically. Furthermore, it is used as it is practical for different modules of the prototype to store information which can be accessed and manipulated by latter modules. In this case, the software requires some input from the user which is then stored in appropriate cells in Excel in such a way that as soon as the information is entered it immediately becomes part of certain pre-determined equations, producing this way an output at a predetermined cell. The interfaces' function here is to know where each bit of information should be stored in Excel as well as where to retrieve

the output from. At the same time the system remembers where each bit of information is located to enable any changes.

The following section justifies what information is entered by PRAM at specific locations in Excel as inputs to formulas which in turn provide with the desired outputs. By having an Excel template which includes certain predetermined information (such as the threat scores from surveys), and adding the organisation-specific information that the user has entered in the PRAM interface, six key operations are performed within Excel, each providing with different outputs.

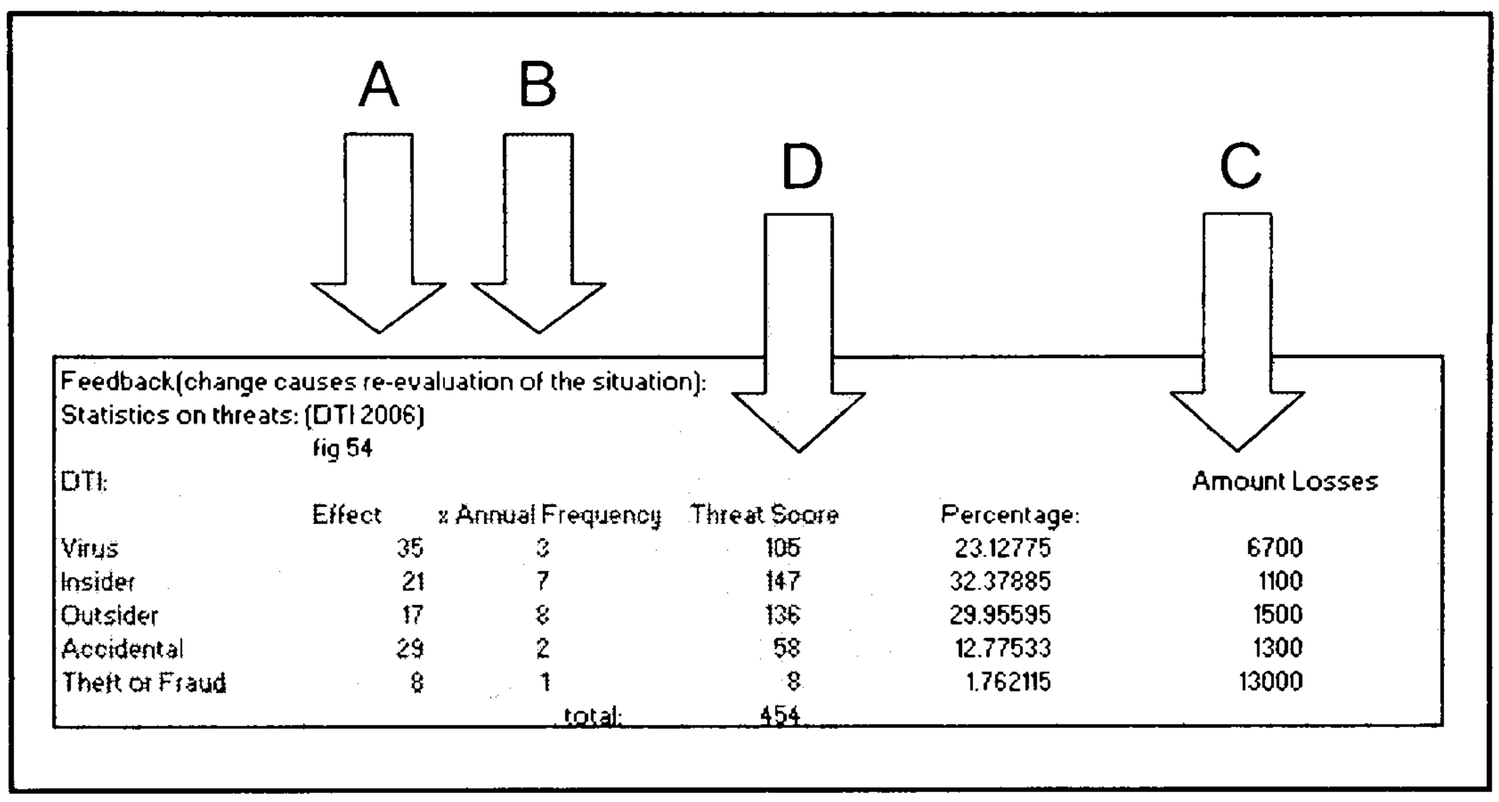
Element 1: The Initial Threat Scores

This element includes predetermined factors which are the severity of each threat (Figure 61A) (based on the impact of each threat from the DTI survey), the annual frequency of a threats' occurrence (Figure 61B) (again from DTI) and the financial losses caused by the occurrence of a threat (Figure 61C) (As reported by DTI and CSI in their surveys). All these factors are used to estimate the threat score for each threat (Figure 61D) (used for the calculations in element 2). Furthermore they are used in the assessor to present in a pop up display when the user clicks on a threat label the potential ALE by this threat.

- ***Initial Threat Scores = Threat Effect x Annual Frequency of threat***

- ***ALE for each threat = Reported Losses for each threat x Annual Frequency of threat*** (Endorf 2003)

Even though these factors are all initially predetermined by survey findings, they are later updated by the feedback module of PRAM to produce organisation-specific figures. All these elements as well as the annual loss are updated after the feedback to adapt specifically to the organisations characteristics.



	Effect	x Annual Frequency	Threat Score	Percentage:	
Virus	35	3	105	23.12775	6700
Insider	21	7	147	32.37885	1100
Outsider	17	8	136	29.95595	1500
Accidental	29	2	58	12.77533	1300
Theft or Fraud	8	1	8	1.762115	13000
		total:	454		

Figure 61: Survey data used to calculate the likelihood of and ALE from threats

What is achieved in this element is an estimation of the initial level of threat without considering any characteristics of the organisation but solely the 'threat that is out there' and the potential losses because of each threat and its occurrence rate (one of the identified financial elements that SMEs require from an RA methodology). The importance of this element however is that it then feeds into element 2 to calculate the specific threats to the organisation and secondly that after the users' feedback on the particular threat occurrence to their organisation this element provides specific threat figures for the organisations employing PRAM to calculate risks. In a commercial version including the sub-threats previously mentioned then more exhaustive

investigation into the survey results would be made to assign the sub-threats with the equivalent reported scores.

Element 2: The Risk scores.

Traditionally risk is calculated as the factor of (Gray 2005):

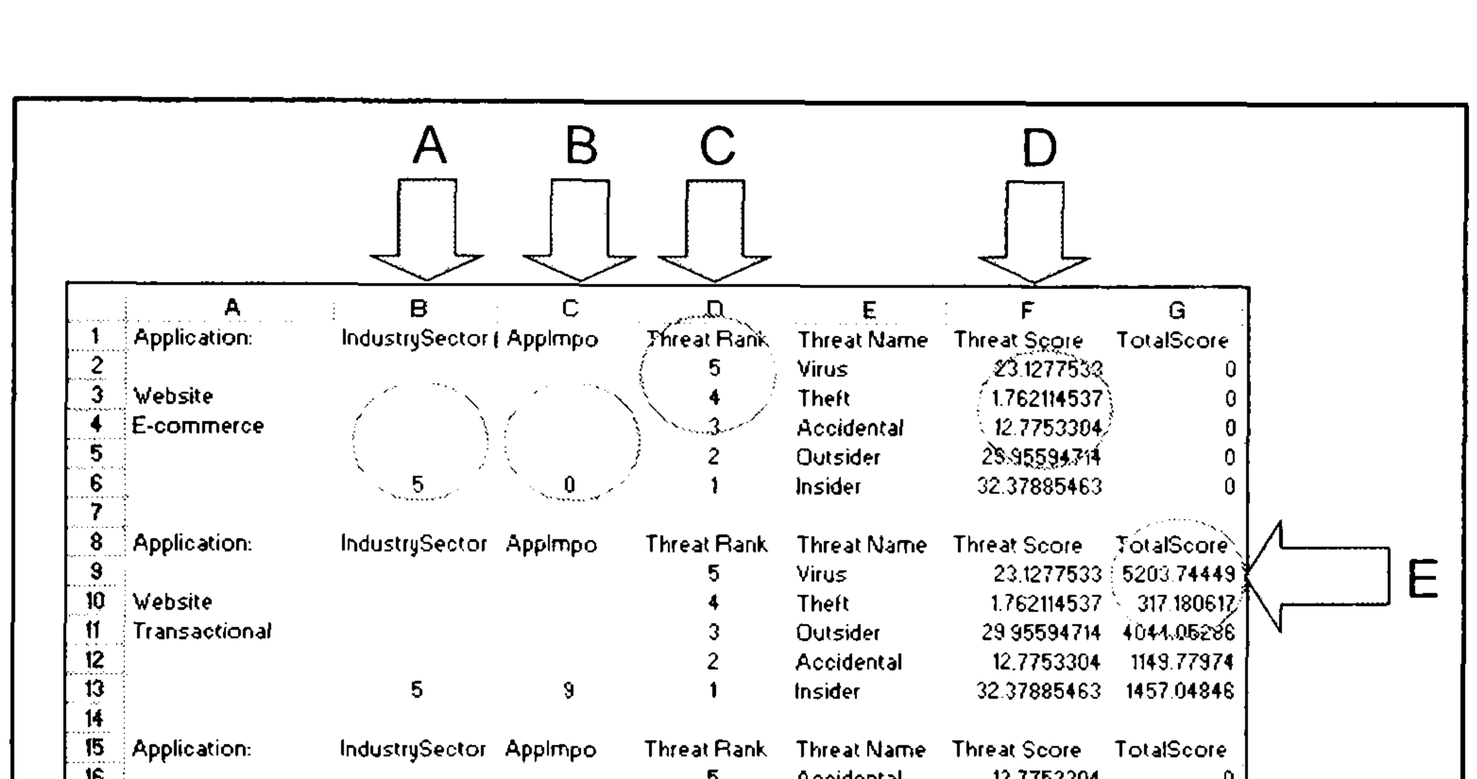
Risk **(to effort, organization, or object) =** ***Threat x Vulnerability*** **(of the threat)** ***x Impact*** **(asset value)**

In this element 'Threat' is the 'Threat Rank to Application' (i.e. a measurement of how much each application is endangered by a specific threat), Vulnerability is the 'Initial Threat Score' (i.e. the product of each threat's impact and likelihood) and Impact, which is the asset's value, is in this case the C-I-A rating of the asset's importance. Another factor that affects the risk towards applications is the industry sector the organisation belongs to since different types of organisation are subject to different volumes of attacks and I.S. breaches. Therefore this was the last factor added to PRAM's formula for estimating risk:

- ***Risk Scores = Industry specific attack activity x Application Importance (C-I-A) x Threat Rank to Application x Initial Threat Score (from element 1)***

This element includes a score stored by the profiler module of the tool based on the Symantec threat report results. Data from the Threat Report indicating the 'attack activity by industry' (Figure 33 of the report) is used to give a multiplier for the threat score (Figure 62A). This illustrates the specific threat the organisation faces solely due to the industry sector it belongs to. What is stored next in this element is the users' score of

each application C-I-A (Figure 62B), including the importance rating. This way the most important the application – the greater the resulting threat score is. Threat Rank to Application (Figure 62C) refers to a pre-determined ranking of the threats to the specific applications. For example while the biggest threats due to the application 'Internet connection' might be the introduction of Malicious Code, Insider Misuse and Attack by Outsider, for removable backup media the biggest threats are more likely to be Accidental Loss and Theft. Finally the threat score for each threat which is produced by element 1 is used in this equation (Figure 62D).



	A	B	C	D	E	F	G
1	Application:	IndustrySector	AppImpo	Threat Rank	Threat Name	Threat Score	TotalScore
2				5	Virus	23.1277533	0
3	Website			4	Theft	1.762114537	0
4	E-commerce			3	Accidental	12.7753304	0
5				2	Outsider	29.95594714	0
6		5	0	1	Insider	32.37885463	0
7							
8	Application:	IndustrySector	AppImpo	Threat Rank	Threat Name	Threat Score	TotalScore
9				5	Virus	23.1277533	5203.74449
10	Website			4	Theft	1.762114537	317.180612
11	Transactional			3	Outsider	29.95594714	4044.05286
12				2	Accidental	12.7753304	1149.77974
13		5	9	1	Insider	32.37885463	1457.04846
14							
15	Application:	IndustrySector	AppImpo	Threat Rank	Threat Name	Threat Score	TotalScore
16				5	Accidental	12.7753304	0
17	Website			4	Virus	23.1277533	0
18	Displays			3	Outsider	29.95594714	0
19	Information			2	Theft	1.762114537	0
20	only	5	0	1	Insider	32.37885463	0
21							
22	Application:	IndustrySector	AppImpo	Threat Rank	Threat Name	Threat Score	TotalScore
23				5	Outsider	29.95594714	0
24	Website			4	Insider	32.37885463	0
25	Contains User			3	Accidental	12.7753304	0
26	Information			2	Theft	1.762114537	0
27		5	0	1	Virus	23.1277533	0
28							
29	Application:	IndustrySector	AppImpo	Threat Rank	Threat Name	Threat Score	TotalScore
30				5	Accidental	12.7753304	2235.68282
31	Office Applications			4	Virus	23.1277533	3237.88546
32	excel			3	Insider	32.37885463	3399.77974
33				2	Outsider	29.95594714	2096.9163
34		5	7	1	Theft	1.762114537	61.6740088
35							
36	Application:	IndustrySector	AppImpo	Threat Rank	Threat Name	Threat Score	TotalScore
37				5	Accidental	12.7753304	1916.29956
38	Office Applications			4	Virus	23.1277533	2775.3304
39	Word			3	Insider	32.37885463	2914.09692
40				2	Outsider	29.95594714	1797.35683
41		5	6	1	Theft	1.762114537	52.8634361

Figure 62: How each application introduces threats to the organisation

Element 1 provides with a generic estimation of the severity of each risk without any consideration of specific threat levels for the particular organisation being assessed. By adding a threat score because of the industry sector and threats introduced because of the applications that exist within the organisation. What is achieved here will enable PRAM to produce threat estimations which match the specific characteristics of the organisation being assessed, addressing this identified requirement of SMEs of an RA solution. The outputs of this element (i.e. the overall risk score for each threat introduced by each application) (Figure 62E) are fed to element 4 to produce the overall threat score. .

Element 3: The Financial considerations/Calculations

Three bits of data are stored within this element, the organisations size (in terms of employees) (Figure 63A) and the organisations I.T. budget (Figure 45B) as entered by the user in the profiler module and a value stored by the VB project according to the users selection of industry type (Figure 63C), that is the average, according to CSI, spending per employee on security according to the industry sector. These elements are used to calculate and suggest a minimum security spending to the organisation (Figure 63D) and what percentage of the overall budget that is. The size element is also used in assessor to provide with a multiplier by which the controls price is multiplied.

- ***Recommended Budget = Size of organisation x Reported spending per employee for industry sector***

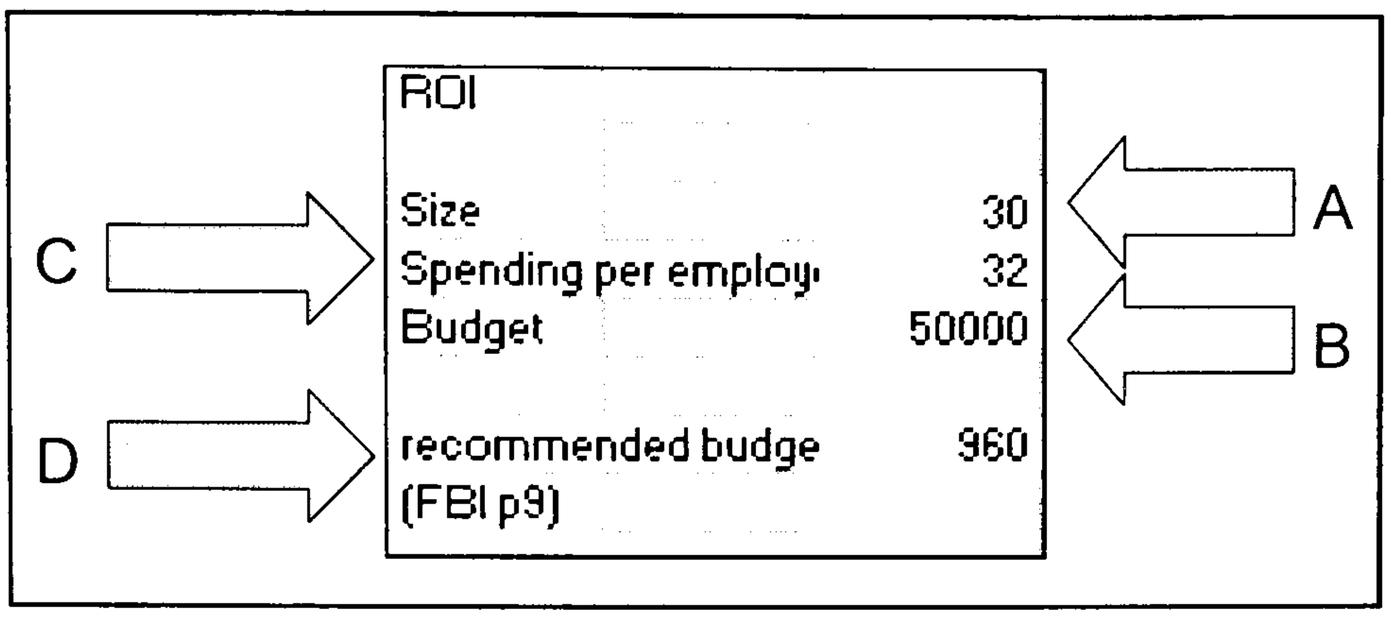


Figure 63: Survey Data is used to suggest minimum spending on I.S.

The recommendation of a minimum budget that should be spent per employee (and according to industry sector) on security, by the organisation managing its risks by using PRAM, is an essential component for the SME user in need of guidance on what they should spend on security. These financial figures are then used in the assessor when providing ROI assistance to the user selecting controls, addressing this way the requirement of SMEs for assistance in the financial considerations of IT security.

Element 4: Final threat scores

The function of this element is to gather all the individual risk scores as they have been calculated for each application (in element 2) and add them all up (Figure 64A), then divide them by the number of total applications found within the organisation (Figure 64B) to produce an average of the Overall Threat Score for each threat (Figure 64C). This is the actual score that is displayed in the red-amber-green display on the PRAM interface.

- ***Overall Threat displayed to user = Risk Scores / Number of applications***

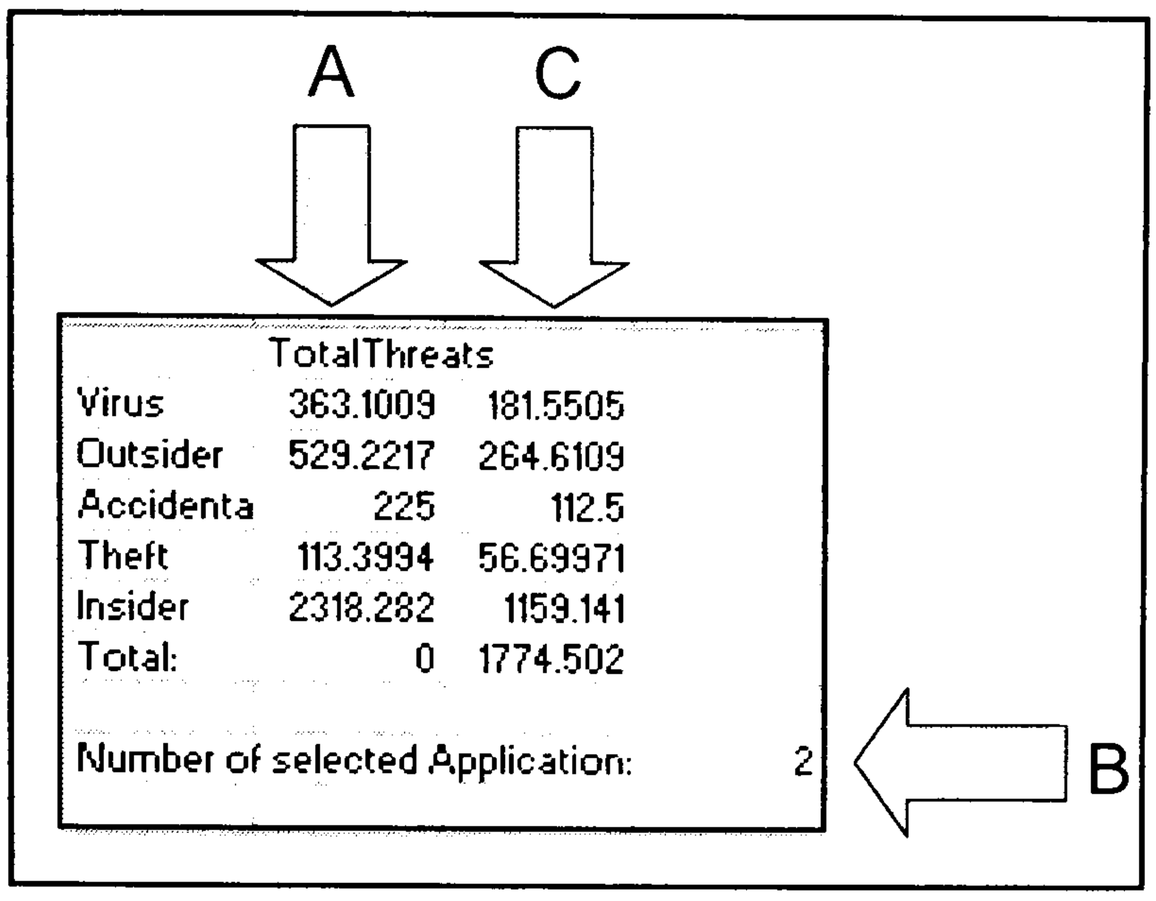


Figure 64: Threat by Applications is averaged to give the overall threat as illustrated graphically to the user

By providing the figures that, through the VB interface are then illustrated graphically to the user, another requirement of SMEs is addressed by PRAM, that is the need for a comprehensive interface which the user can look and immediately realise what risks the organisation faces and how much these are reduced by the selected controls.

Element 5: The controls effect

When the user selects a control in the assessor module, there is a 'control effect score', which is based on statistical data, already stored in the database which is associated with each control. This effect is stored here under the threat it applies to (i.e. the threats this selected control has an effect upon e.g. control 'Antivirus' will have an effect of 75% and will be stored underneath threat 'Virus') and the threat's score is divided by the controls effect (Figure 65A) to provide a threat score after the control has been applied (Figure 65B). This will happen as many times as long as the user selects controls that apply to threats while their score is still over zero. If the threats score reaches zero the user is

alerted there is no need to select more controls for this threat. At the same time, the change on the overall threat score is displayed to the user in the red-amber -green display of the assessor every time a control is added and the user can make the decision of whether the threat has been reduced to acceptable levels.

- ***Threat after applying control = Old Threat / Controls effect*** (Allard 2003)

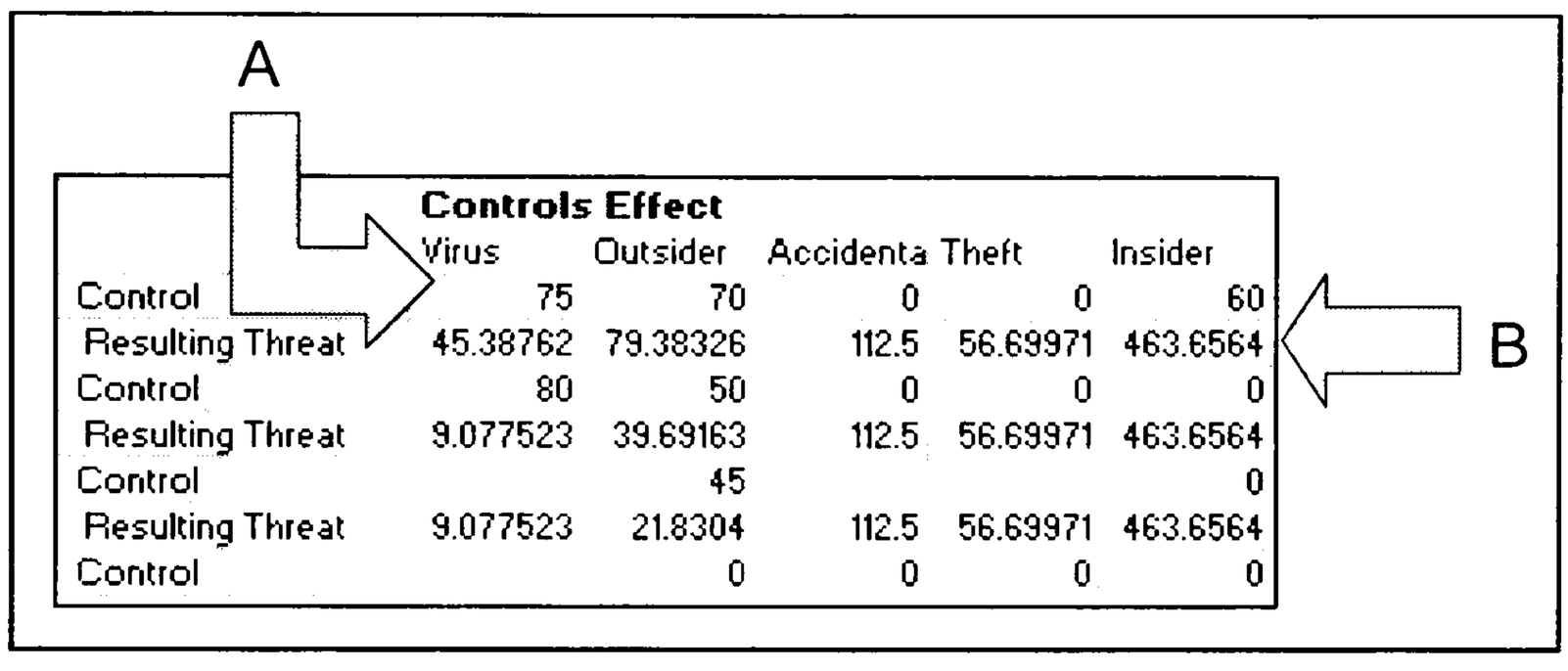


Figure 65: The predetermined effects of controls are used to reduce the threat scores

The output of this element achieves in illustrating the effect of the user-selected controls on the already calculated overall risk that the organisation faces. Every time the user adds a control and the related threat scores are reduced, this reduction in threat is illustrated to the user on the assessor display allowing the comparison between the effect of the control and its cost achieving this way the requirement of SMEs for assistance in selecting cost-effective controls with as much impact on threats as possible. In a commercial version one would wish more accurate scores on the effect controls have on threats. This would ideally be achieved by conducting an investigation and querying people involved in the

I.S., RA and countermeasures industry what percentage effect they judge each control to have. Then for each control calculate the average, from the responses, score and include that in the database. This is what was meant earlier when saying that the effect of controls is based on statistical data. In the case of the prototype however, where the purpose is to illustrate the functionality of the framework, the effect of the controls has been estimated either from personal experience having used certain controls for some of the applications or from survey data and reading material.

Element 6: The threat score graphs

In this element the initial (Figure 66A) and final (Figure 66B) (i.e. after the controls have been applied) threat scores are displayed, these are then used to create two graphs in Excel

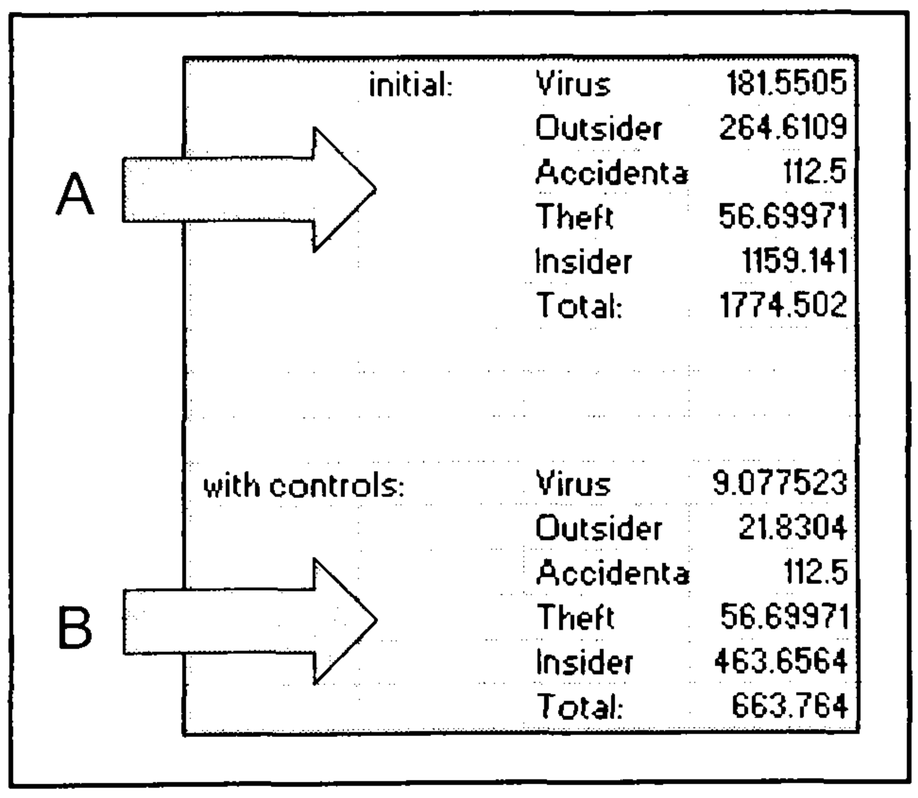


Figure 66: The initial and final threat scores assist in drawing graphs for the final report

These are used in the report and their purpose is to illustrate to the user conducting the assessment and to the management what the threats (and how high) towards the organisation are and the effect of the selected controls. Including these graphs of how much threats are reduced, together with information on the selected controls and primarily their cost is useful information to raise managerial awareness and justify the expense for securing assets.

6.4 The PRAM Risk Analysis prototype

Having discussed how results are created in the background, this section will describe how the interface works to obtain and display information to and from the user. Essentially, to perform the operations identified in the requirements and discussed in the methodology, there are four modules that should make up the PRAM interface.

- The Organisation Profiler for profiling the organisation.
- The Application Handler used for rating the applications importance.
- The Assessor which addresses identified threats with the appropriate controls.
- The Feedback and Update module.

6.4.1 The Organisation Profiler

As the name implies, this module creates the initial profile of the organisation. PRAM requires the user to input specific data on the organisation at this stage which will be

stored and utilised by the modules that follow. As Figure 67 illustrates, this module has two main displays: the Initial Profiling display and the Applications/Departments display.

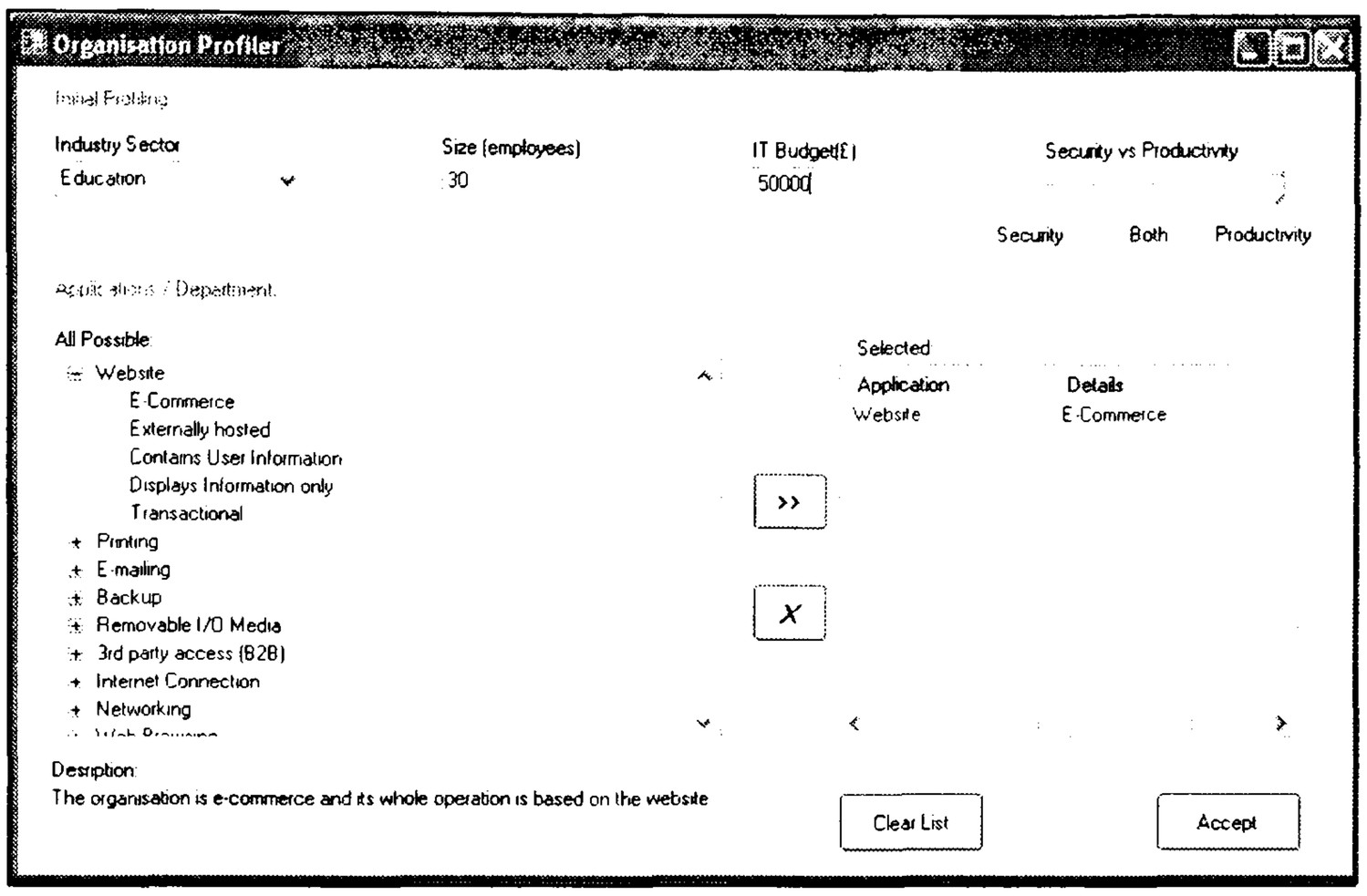


Figure 67: The initial profiler interface

6.4.1.1 Initial Profiling Display

More specifically the user is required to enter the nature (industry sector) of the organisation, which this determines one of the factors used to estimate the threat score for the organisation. Also required here is the size of the organisation in terms of employees, used to suggest the recommended I.S. spending and also calculate the cost of controls at the final stage which is also where the I.T. security budget required input is later used. The final required user input is setting the value of the Security vs. Productivity bar which will determine the way controls are displayed to the user later on. This bar enables the user to select from three settings: security, productivity or both.

6.4.1.2 Applications/departments Display

The goal here is to simplify the user input and avoid the lengthy questionnaires and other input methods found in risk analysis tools. For this, a tree-view control is used which presents the user with a list of all possible applications that can be found within an organisation. Approaching the analysis this way eliminates the need to identify specific assets, the basis of the tool are the Risks that the organisation faces and these can be scored just as well according to the applications used. Nevertheless, and because the aim is not to be exhaustive, a lot of the assets found within the organisation can be guessed according to the applications (eg if local email is used there will be hardware assets such as a server and clients, software assets such as specific server O.S., and information assets such as the actual messages which travel through the network and the internet and are stored somewhere within the server or the desktops (Buchanan 1999)). Here is the first use of profiles we have in the tool, where the assets are hidden behind the applications and as the user selects applications, a list of more specific assets can be populated. Every application selected by the user is copied to a list-view display, from there the user can then remove applications, clear the list and start over. If the user is happy with these selections they can proceed which will store in a database all the selected applications data. It will also cause the values entered by the user for organisation size, budget etc to be stored in Excel.

6.4.2 The application handler module

The handler (Figure 68) is a straightforward application which lets the user score the importance of the previously selected applications.

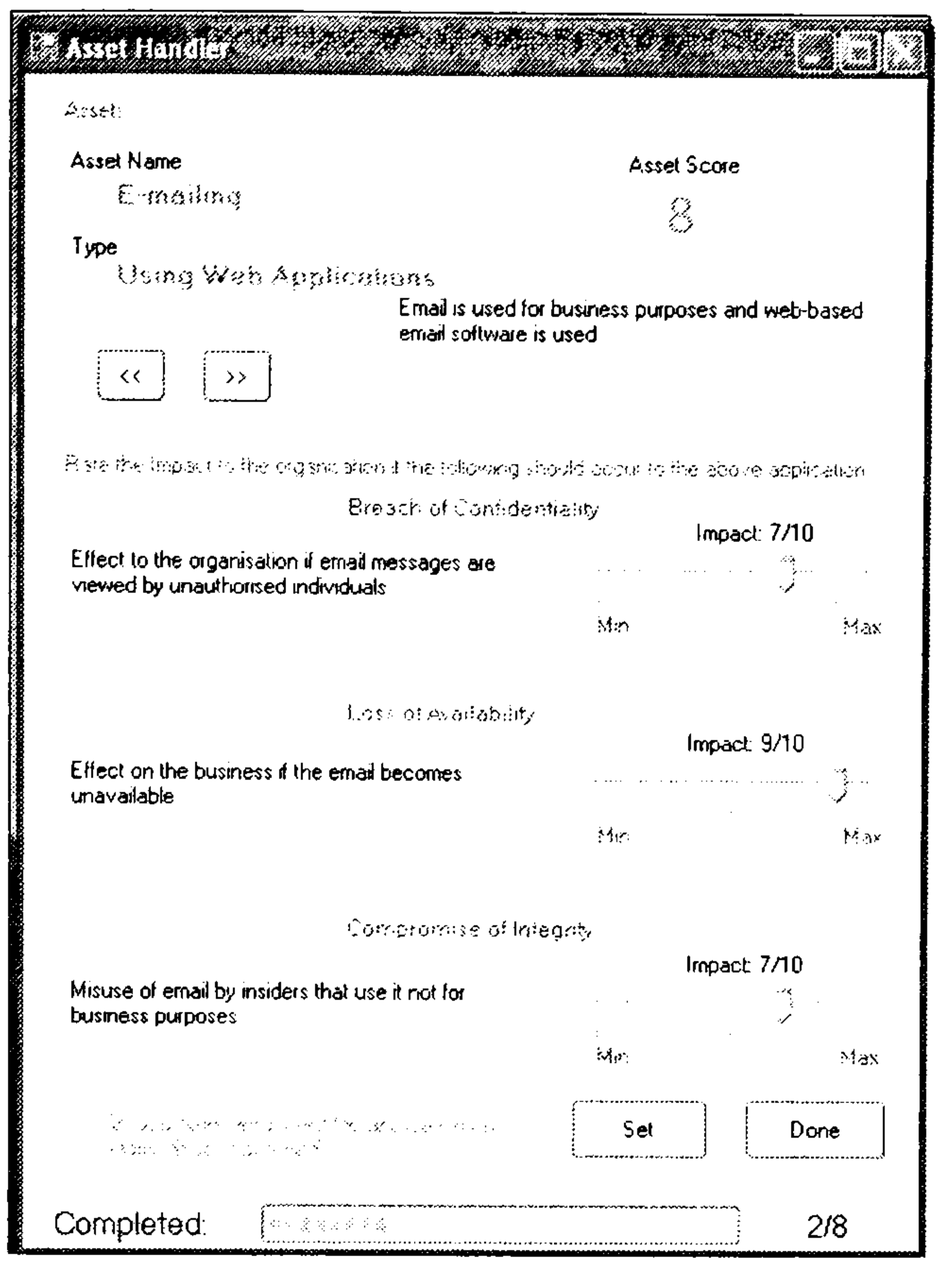


Figure 68: Rating the selected applications importance

What is meant by straightforward is that there are no assumptions made or survey data used in this part in order to obtain results. The database where all the user selected applications have been stored by the previous module is opened; the applications are displayed to the user one by one and the user who is required to score these applications importance. That is done by the user rating on a 0 to 10 scale, 0 being minimum and 10 the maximum, what the effect to the organisations operation would be if the each of the three factors determined by ISO17799 occur to the application. That is breach of confidentiality, compromise of integrity and loss of availability. The 10-point scale (also used by CRAMM (Yazak 2002)) was selected to allow the user a more precise rating than, for example, if it was a low-medium-high scale. However what scale is used here is not the essence as the overall importance score provides a multiplier (described in section

6.3.2.2) for the overall risk scores, therefore whichever the scale was, the output risk scores introduced by each application would still be likewise proportional to the importance of the applications as rated by the user. A progress-bar and a label at the bottom of the module illustrate how far down the list of all selected applications the user is in terms of scoring. When all applications have been scored, PRAM utilises the user ratings to calculate the level of risks the organisation is under. To achieve this, two different displays are used within the module: the Assets Display and the Impact Display.

6.4.2.1 The assets display

The application name and details are displayed at the top half of the module together with some information on the application. There are also controls which allow the user to navigate, so as to view and score, through the selected applications and at the top right of the display the average score of the applications importance can be seen, if the user has already scored that asset, or is updated in real time while the user uses the bottom 'impact' display to score it.

6.4.2.2 Impact display

This is the bit of the module where the scoring of the application takes place, it includes three slide-bars by moving which the user determines the impact of the C, I or A element occurring, and three text-boxes which provide the user with useful information in order to achieve the most realistic score possible. Having used the slidebars to score the importance of the application, the user can press 'set' to move to the next application..

When the scoring process for an application is finished, the average value of the user scores is stored next to the corresponding application in order to be used for sorting the applications in later parts of the tool and in the appropriate locations.

6.4.3 The Initial threat display

When the user is done with scoring the assets they can press 'Done' which will present them with the 'initial threats display' shown in Figure 69.

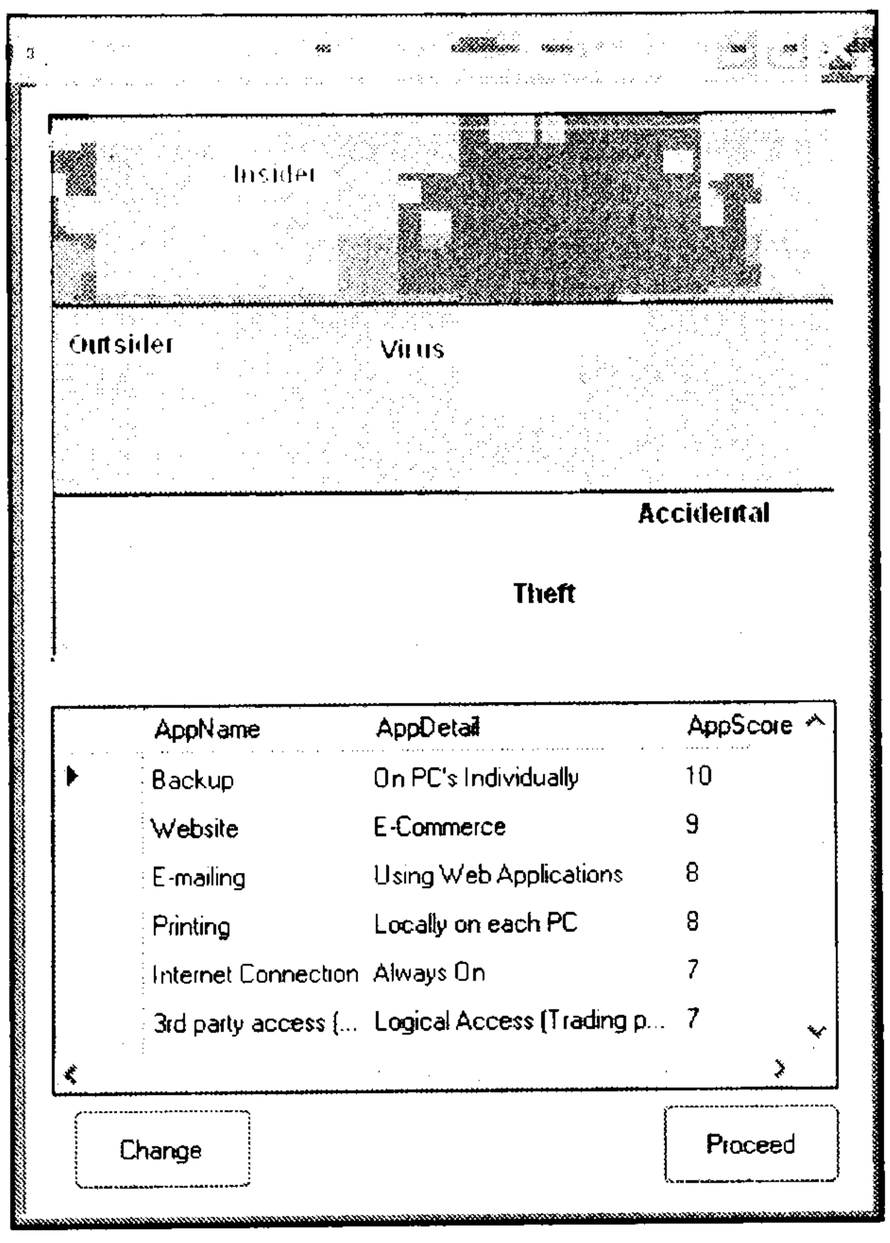


Figure 69: The initial threat display

As the threats are calculated in Excel, their final scores are obtained by this part of the tool and the threats are displayed graphically against a red-amber-green display which illustrates, as a threat moves more towards the upper bit of the display (the more into the red section it is) the more the likelihood and damage that may be caused by that threat. A

data-gridview style table underneath displays at the same time the lists of all the selected applications together with their scores, all ranked in terms of importance.

For the purposes of simplicity required from this framework, instead of using exhaustive lists of threats as found in the various surveys, all the threats have been categorised under five main categories, forming this way the basis for the 'threat profiles' (which will mainly be used in the next part). Table 10 illustrates the categories under which all major threats have been grouped in a similar way as the DTI 2006 survey groups them.

Threat Category	Malicious Code	Insider Misuse of information systems	Unauthorised Access by Outsiders	Theft or Fraud involving computers	Accidental Systems Failure or data corruption
Example Contained Threats	Virus	Misuse of web access	Actual penetration into network	Financial Fraud	Power supply failure
	Trojans	Misuse of e-mail access	Denial of service attack	Physical theft of computer equipment	Environment control failure
	Ad-ware	Unauthorized access to systems data	Company impersonated on Internet	Telecoms fraud	Network Overload

Table 10: Threats with similar characteristics grouped together form threat profiles

6.4.4 The Assessor

This is the module that makes the decisions, fed with the level of risk the organisation is under and the significance of applications to the organisation, the controls that correspond to the organisations profile and needs are chosen and prioritised accordingly. The following Figure shows the decision process that follows:

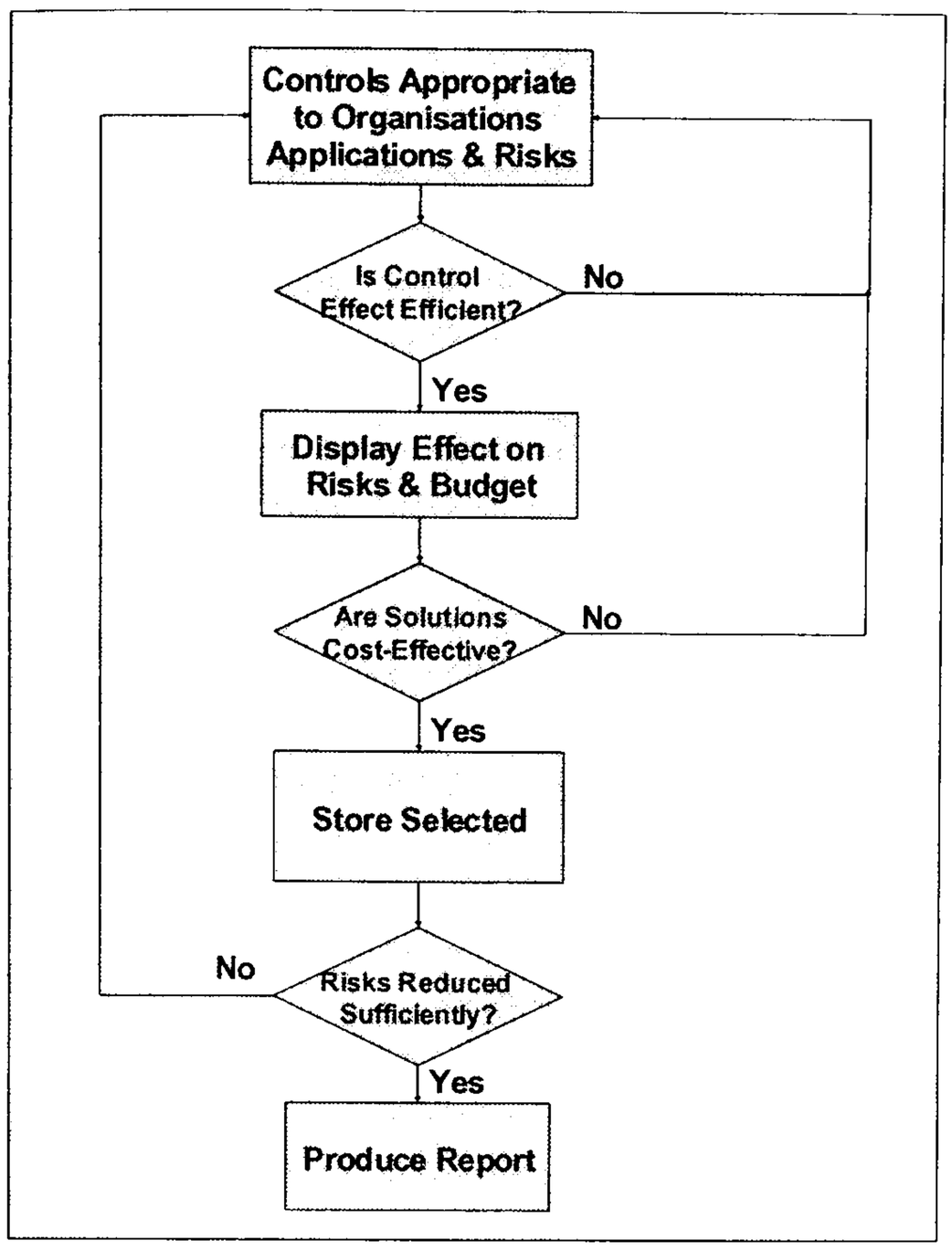


Figure 70: The decision process for selecting controls

As described earlier, this constitutes the management fragment of the RA. The aim is to achieve simplicity and assist the user by using multiple graphical displays. There are three main displays, one about the budget, one on the current threat, and one about the available and selected controls. Three displays are used to achieve this: the Threat Display, the ROI display and the Threats – Applications – Controls Display.

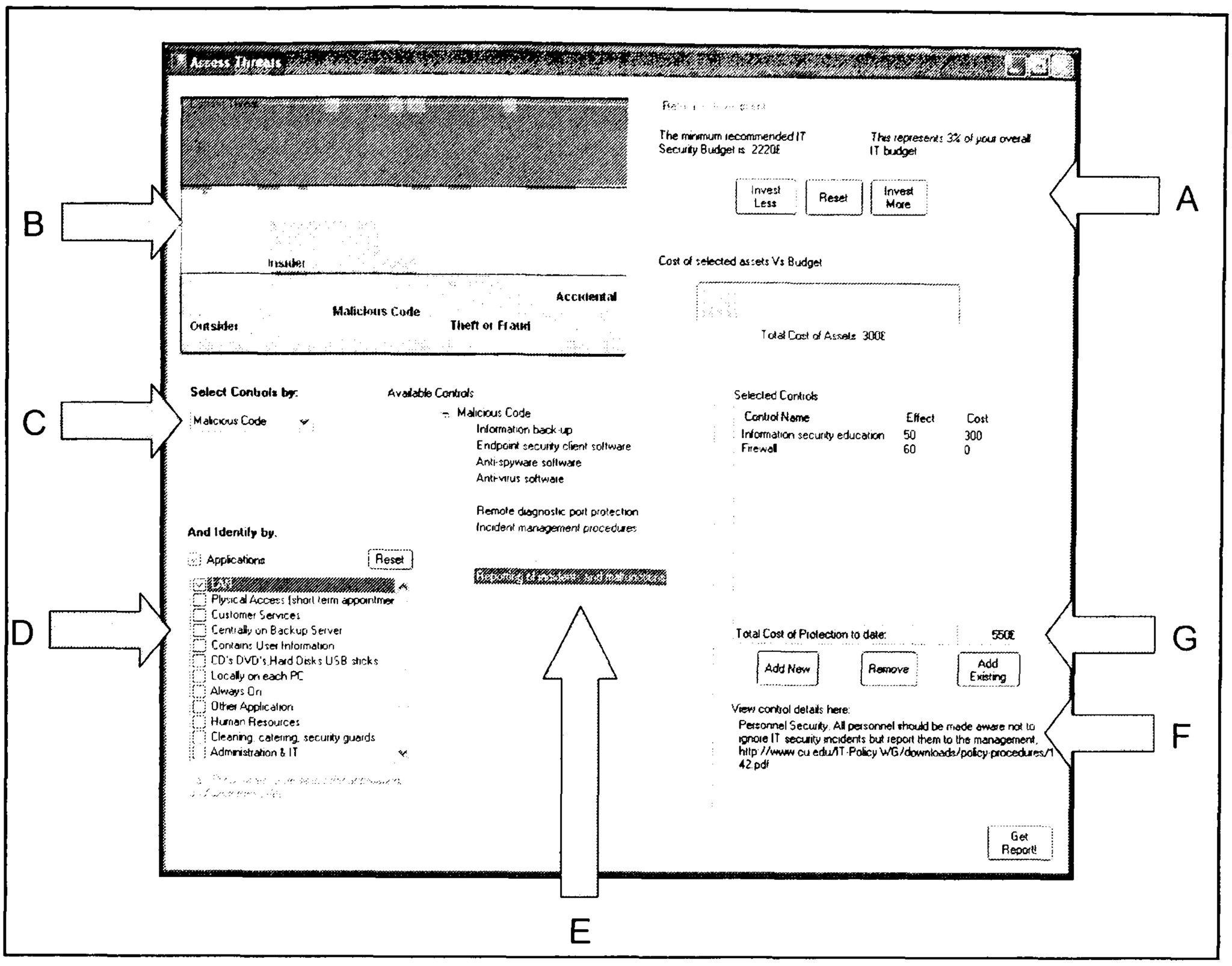


Figure 71: The Assessor GUI presents the assistance an SME user needs when selecting controls

6.4.4.1 The R.O.I. display

This display shows to the user what the minimum recommended security budget is and also presents it as a percentage of the overall security budget (Figure 71A). Here the user has the option to decide whether they want to invest more or less on security. When controls are selected a progress bar illustrates to the user what proportion of the selected I.T. security budget they have spent, if the entire selected by the user budget has been spent, the user is not allowed to selected any more controls unless they increase the selected budget by selecting 'invest more'.

A subroutine here considers the cost of controls in relation to the size of the organisation as specific prices for the controls are not being used, and because not all controls need to be applied for as many PCs the organisation has. For example if there are 50 computers, the antivirus control needs to be multiplied by 50. At the same time, controls like physical security, biometrics and hardware firewall will still need to be more than one in a home office but not as many as 50. Therefore a multiplication factor is used which will be roughly 5 for a small organisation, 10 for a medium and 25 for a large to illustrate differences in controls prices relevant to the organisation size. In a proper commercial working model of course with some altering of the database the controls can be distinguished in software, hardware and physical and then use this rough approximation for hardware and physical while multiply all the software controls with the number of pc's, while this will make the output a bit more specific, it will still not be 100% precise. Therefore for the prototypes purposes the approximate multiplier based on the number of employees is chosen to be used simply to illustrate to the user how the cost increases with the size of the organization.

A known vulnerability of the tool that has not been addressed here but is crucial to be tackled in a "full" version of PRAM is that the control selection process ignores possible overlaps or/and conflicts between different security measures.

One last issue for a full version of PRAM is the actual cost of the controls, and since it is not the purpose here to include actual brands and prices of countermeasures, the prices for a number of products from each control category could be gathered and averaged to

provide the input here. For the purposes of this prototype however, approximations were made according to the typical prices expected for each product category.

6.4.4.2 The Threat Display

This display (Figure 71B) is the first thing the user sees when the module loads, it graphically illustrates the threat scores for the organisation that, according to the user inputs, have been calculated in Excel. Another important feature of this display is that by clicking on any of the threat labels on the display, a pop-up presents the user with the 'threat profile' of this threat. The threat profile includes statistical and financial data which aims to assist the user with the selection of countermeasures. Particularly the financial data, as part of the tools ROI feature, calculates the ALE by each threat,

- ***ALE = Annual Frequency x Losses occurred***

As discussed earlier, the actual figures that make up the factors for this calculation have initially been devised from survey data, However as will be seen later in this chapter, if the user has used the feedback module they can return and re-evaluate the selection of cost-effective controls based on expected ALE, however this time with the numbers adapted to specific figures from the organisation.

Figure 72 illustrates how PRAM informs the user of these financial issues related with the threats the organisation faces as part of the assistance in raising awareness and paying appropriate attention to where the organisation is really at risk when selecting controls.

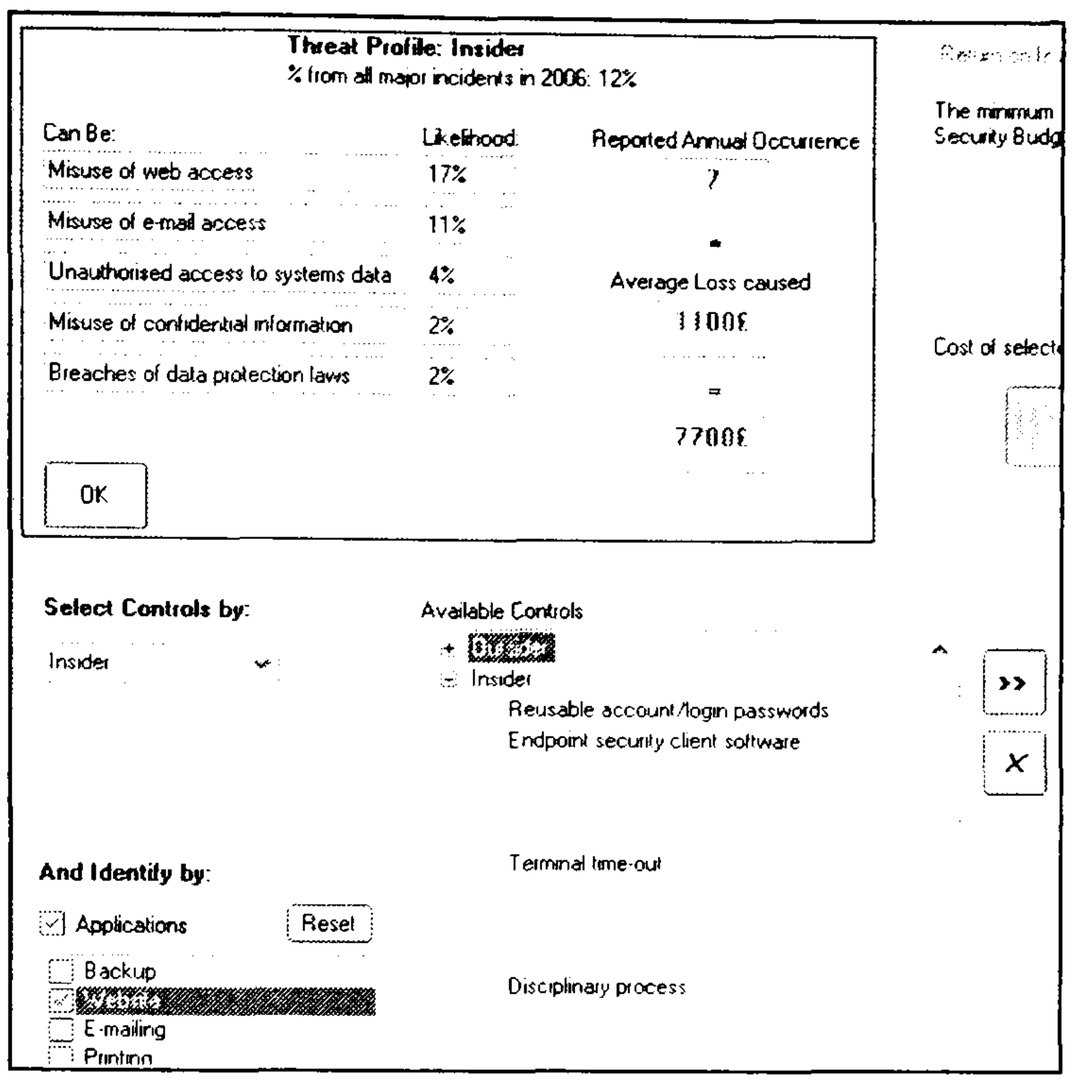


Figure 72 : PRAM assists the Cost-effective selection of controls

PRAM allows the user to view a threat that is undesirably high on the coloured display seen in previous figures, click on it to view what losses may result from this threat and then from the bottom display select the corresponding controls, even considering the application that requires more protection. When controls are added, their cost is added in the ROI display, and the user has the option to contrast the cost of controls against the estimated loss due to a threat and therefore select the most cost effective controls.

6.4.4.3 The Threats – Applications – Controls Display

This is the main display at the bottom of this module; it enables the user to select the controls which match more the threat and budget requirements of the organisation. To do this the user can look at the threat display and decide which threat they wish to decrement

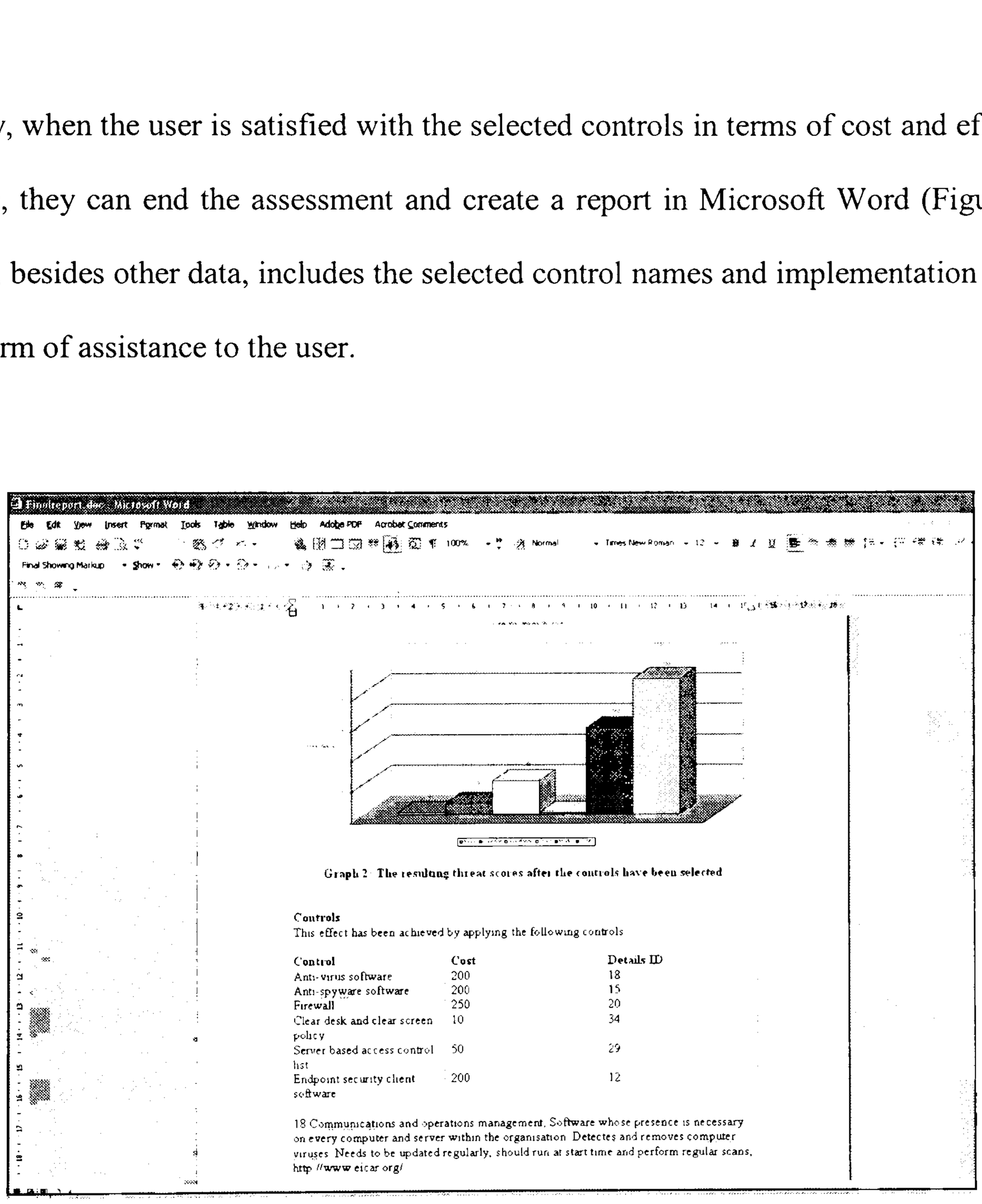
on the display. By selecting the name of that threat from a drop down list (Figure 71C) the tree-view control of the display is populated with the corresponding controls, then the user can populate a check-box display with all the applications that have been identified as existing within the organisation (sorted in terms of importance) (Figure 54D). By checking any of these applications the controls that correspond to it and that already exist in the tree-view under the threat's being assessed name are highlighted green (Figure 54E) to make the users choice of controls easier. Furthermore by clicking on a control once the system displays a short description and details of this control to assist the users with their selection (Figure 71F).

When a control is selected its cost is subtracted from the remaining budget and its effect upon the threats can be viewed in the threat display. If in the first module the user has selected 'productivity', the controls are listed in terms of intrusiveness but in an ascending order, otherwise they are listed in terms of effectiveness (i.e. security) they provide.

In addition, an option provided to the user here is to select certain controls as controls already been implemented within the organisation (Figure 54G). When the application is selected, its effect is illustrated on the 'Threat Display' without however its cost being reduced from the remaining suggested security budget (Its cost does however appear inside the 'Total Cost of Protection to Date' display). This feature enables the user performing the assessment to visually establish what effect the existing controls have on threats, add controls to supplement existing ones that have not eliminated a threat, even

remove existing controls and replace with more efficient potentially even at a better overall cost. This feature can therefore be described as a tool to evaluate the effectiveness of existing organisation security.

Finally, when the user is satisfied with the selected controls in terms of cost and effect on threats, they can end the assessment and create a report in Microsoft Word (Figure 73) which, besides other data, includes the selected control names and implementation details as a form of assistance to the user.



Finalreport.doc - Microsoft Word

File Edit View Insert Format Tools Table Window Help Adobe PDF Acrobat Comments

Final Showing Markup Show

Graph 2: The resulting threat scores after the controls have been selected

Controls

This effect has been achieved by applying the following controls

Control	Cost	Details ID
Anti-virus software	200	18
Anti-spyware software	200	15
Firewall	250	20
Clear desk and clear screen policy	10	34
Server based access control list	50	29
Endpoint security client software	200	12

18 Communications and operations management. Software whose presence is necessary on every computer and server within the organisation. Detectes and removes computer viruses. Needs to be updated regularly, should run at start time and perform regular scans, http://www.eicar.org/

Figure 73: A part of PRAM's output report

6.4.5 Feedback

This is the module which manages the efficiency of the suggested security plan and controls produced by the previous modules. To do this there are three displays used: the Control Box Display, the Threat Occurrence Display and the Handle Applications Display.

Having the information from each stage stored inside specific locations in Excel this allows us not to have to re-run the whole application from the beginning, but instead store all the new information from the feedback halfway through and therefore asking the user to re-run the RA application from the middle (or the appropriate point) in order to re-assess new threats or changes to applications

Therefore:

- If the user simply reports threat occurrences and the system suggests adding controls, then they only need to re-run the assessor module and select more controls for an application. The assessor will check whether this is after the feedback and if this is the case will open a database and highlight existing controls so that the user can select additional
- if the user removes applications the system deletes them from the database and their values from Excel and therefore the user again only needs to run the assessor only to remove controls (which however is not recommended)

- if the user adds applications they need to re-run the application from the asset handler so as to also score the newly added controls importance (or we could score the assets here and run it from the assessor again)

6.4.5.1 The Control Box Display

The control box display in this module provides with information initially on what the user is expected to do and subsequently, according to the users input, what actions should be taken after the feedback.

6.4.5.2 The Threat Occurrence Display

Figure 74 illustrates the display which enables the user to assess the effectiveness of the controls already implemented.

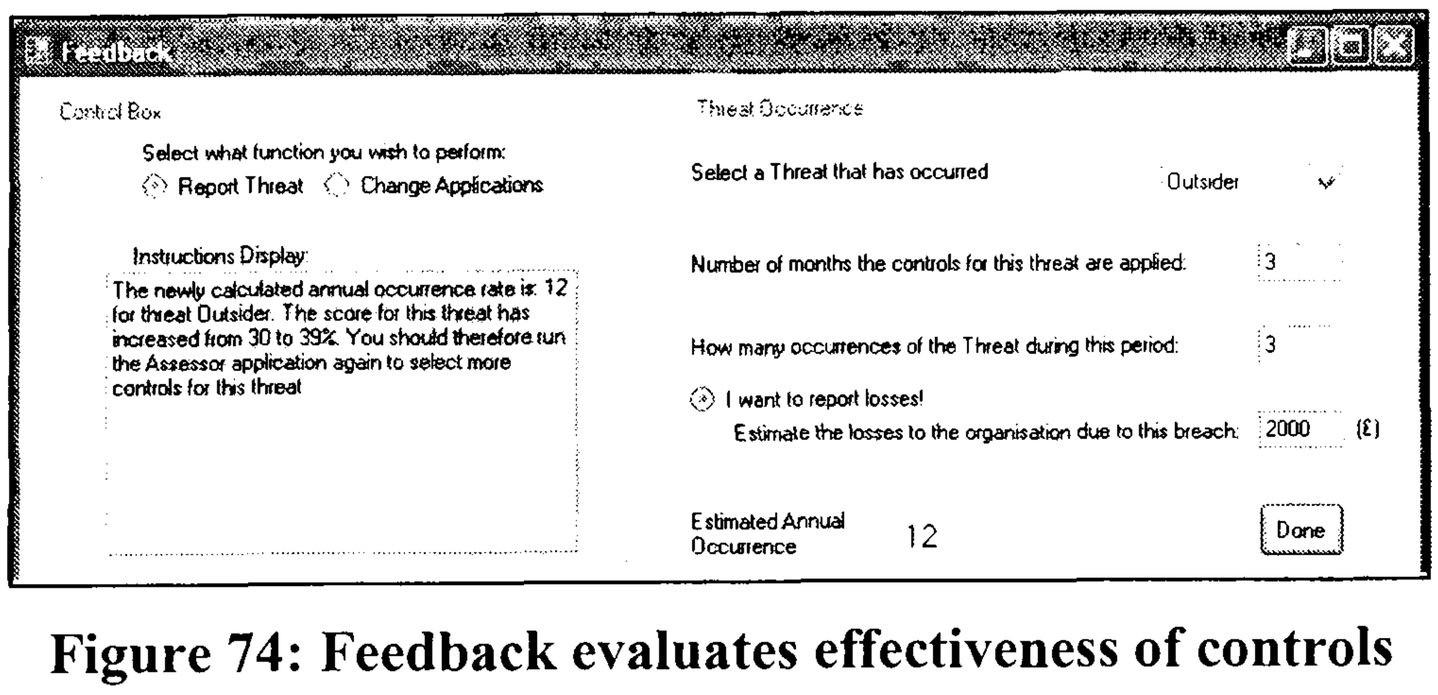


Figure 74: Feedback evaluates effectiveness of controls

The user is required to state the period the controls have been applied and the number of threats that have occurred during that period. This allows for the system to predict the annual occurrence of each threat. When controls were first suggested, survey data was

considered for estimating risks and therefore select appropriate controls. Through this module PRAM can establish whether that data was accurate or if the specific organisation has different needs. Before storing the new annual occurrence, the system grabs the old and compares it, if the new is larger, the system suggests that more controls should be applied for this threat, if it is smaller or zero no action is taken as it is better to consider that the applied control are successful than that the threat was overestimated and therefore controls are removed. Since the initial controls where considered for the threat occurring x number of times in a year if the newly calculated number of annual occurrences is smaller it means the controls are sufficient but since the threat still occurs the organization might benefit from trying to apply the controls better or configuring and updating them better. If however the new annual rate is larger it means that we need to apply more controls that are appropriate for this threat. The user can then re-run only the last part of the methodology (i.e. the assessor) and with new data this time on annual occurrence and losses due to threats re-consider security.

6.4.5.3 The Handle Applications Display

In the lower part of the interface the user can add or remove applications to or from the existing applications that were chosen during the assessment process. The user first selects which of the two actions they wish to perform. If the user selects to remove an application, first the system populates the list-view display in the interface with all the previously selected applications from the database. Then the user can select the application they wish to remove and the system first deletes the score of the application from the location it has been stored in Excel, then another query deletes the application

from the selected applications database. This way the threat scores are re-calculated according to the new situation and the user can assess the controls again.

Similarly the function that allows the user to add applications to the existing organisation profile, populates a list of all the available applications and the list of existing applications (Figure 75A). The user can move the desired application from the first list to the second. When adding applications the user can also score them (Figure 75B) and therefore avoid having to re-run the Handler module but instead proceed straight to the Assessor to select controls.

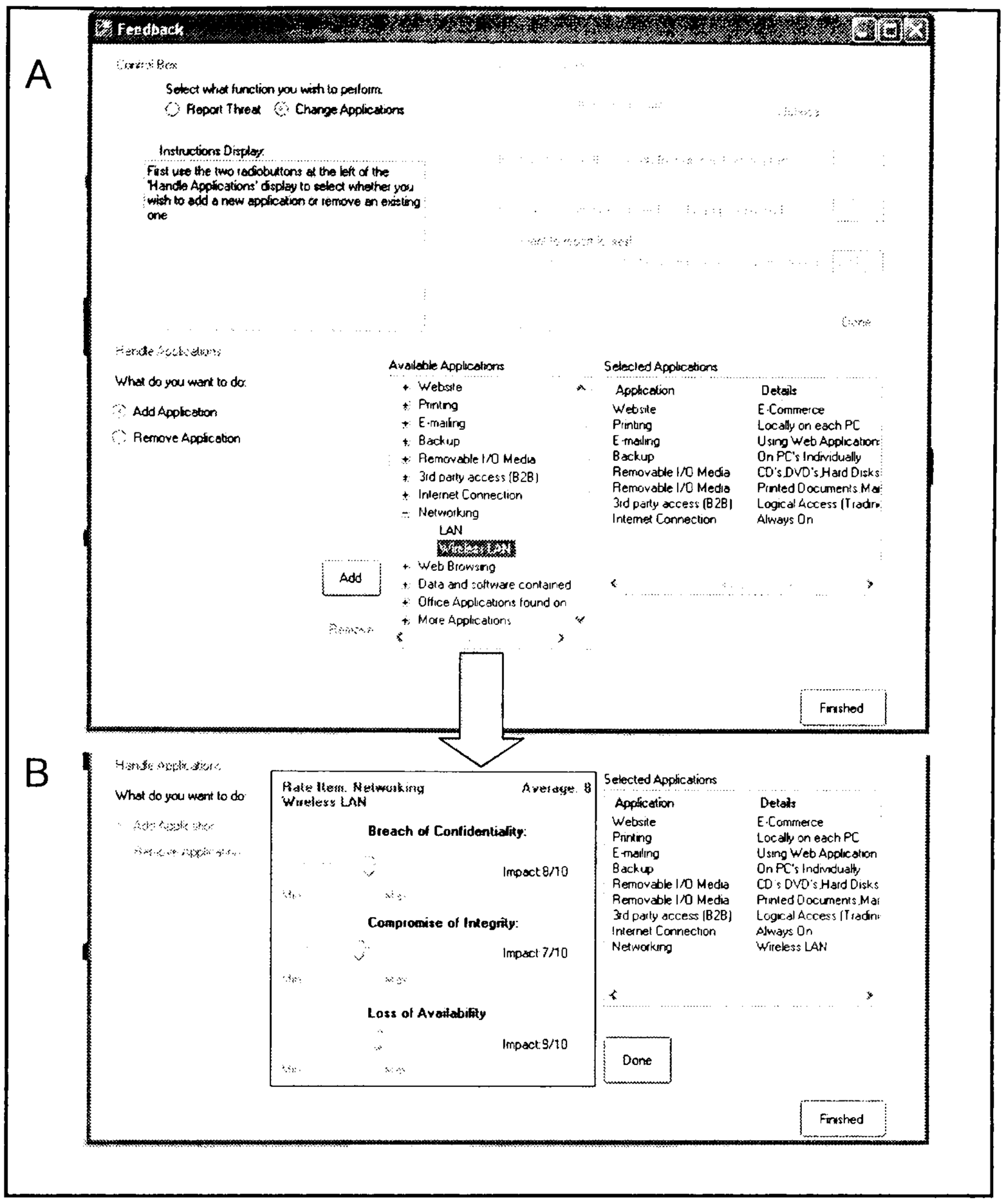


Figure 75: The Feedback module enables the update of the organisations profile

6.4.6 Administrative Update

The administrative update of the software is mainly based upon updating the applications and controls database, including descriptions and the links between tables and the threat scores in Excel when new survey data becomes available. The purpose of this part is to allow the easy update of the tool each time an application, threat or control is added or needs to be removed. This interface will simply update the database if we are updating

applications or controls, or updates the scores in Excel if we are modifying threat scores e.g. due to new survey data. This interface will allow the user to be able to update the tool themselves. As an example, if we are discussing a commercial application a designated user of the tool can be notified by email or even by text message of a control ID and delete it or of a new control together with an effect score and cost to add. For the purposes of this prototype this interface is not operational since there is no actual need to update the tool this way. It is however as a GUI to illustrate the concept.

6.5 Conclusions

To conclude this chapter, the requirements that have been assessed by this prototype of PRAM are:

- No use of questionnaires, but on the contrary a straightforward input of data by use of profiling i.e. similar assets are grouped together under the applications where they may be found and the threats that belong to the same category also grouped under their main threat group
- Easy selection of controls and assistance to selecting, both from a financial perspective as well as from what control matches what applications
- Simplistic (i.e. easy to understand and use) graphical display and 'tip' text-boxes
- Incorporation of financial elements: ALE, ROI
- Assistance on implementation by giving a few words and appropriate links in the report

- Active feedback which adapts the tool to the organisation more closely and also does not require running the whole application from the beginning (existing tools do not even have feedback anyway).
- Easy update of PRAM with new applications, threats and controls.

Therefore, in theory PRAM should eliminate the main setbacks associated with existing RA solutions. The following chapter investigates whether this is the case by comparing PRAM to the already evaluated existing RA tools for SMEs

7 Practical Evaluation of Prototype

Having designed and built a prototype approach to risk management which is suitable for SMEs, an evaluation is in order which will prove whether firstly, it surpasses the prohibiting characteristics of existing RA tools which should make it appropriate in theory, and secondly, evaluate it in practice by seeing whether it is actually suited for the needs of SMEs. This chapter presents the different ways in which the novel methodology was tested and evaluated. The evaluation is intended to confirm the suitability of the proposed approach above the current state of the art.

7.1 Methods of evaluation

There were two approaches to validating that PRAM does what it has been designed to do and addresses the requirements of SMEs from an RA perspective. The initial evaluation aimed to assess the operation of PRAM (how it copes with the characteristics the other RA tools have been evaluated upon in Chapter 4) and how the output it produces compares with that of the commercial tools (in terms of which is more appropriate for SMEs). A further evaluation aimed to investigate how 3rd party users perceived PRAM and its functionality (and therefore has it achieved the requirements for ease of use, assistance to user, requiring less time etc that PRAM has been designed for).

- In order to validate the performance of PRAM and ensure it appropriately addresses the requirements of SMEs, the PRAM prototype was evaluated upon the three SME test scenarios upon which the existing RA solutions were evaluated

were again used. The prototype was used to assess the risks and controls corresponding to the cases of the three SMEs in question which provided information that allowed comparison with the available solutions. More specifically, PRAM was evaluated in the exact same way as the existing RA tools were in Chapter 4, firstly the risk analysis and management processes are discussed; this time the feedback process is also discussed (an element not seen previously, as it was not existent in the other RA tools. Furthermore, in the case of PRAM, to initiate the evaluation against the other tools, instead of simply listing the advantages and disadvantages of the methodology, there is a comparison and discussion on these against those of the other tools. Then PRAM is evaluated upon the same characteristics that were used in Chapter 4, essentially those that were discovered to be necessary so as to cope with the identified requirements and distinctive environment of SMEs.

- What has also been judged appropriate was to have 3rd parties compare and contrast the existing RA tools and this prototype framework based on scenarios they devise, encouraging the subjects to consider and devise a realistic scenario of an organisation they have preferably been involved with, document this scenario and perform an analysis with all the available tools, then rate them on specific aspects that this research is interested in. Assessing the tools functionality and whether it fulfills the desired requirements by having a group of students evaluate it in the lab against the rest of the RA tools. The group of students belongs to an information security MSc which is annually being taught the concepts of risk

analysis and a demonstration of the existing RA tools as part of an MSc–level module on Information Security Management.

7.2 Practical evaluation of PRAM's performance

The performance of PRAM was validated in the same way that existing tools were evaluated in Chapter 4, in order to provide results which are comparable with the ones on that chapter. Using the same scenarios and evaluation criteria as with the commercial tools allowed to successfully evaluate the usability of the system relative to the other solutions claiming to target SMEs. The scenario-based evaluation of PRAM is the decisive evaluation method which aims to prove that the developed methodology addresses the identified problems of existing solutions and suits the needs of SMEs for which it was designed.

7.2.1 PRAM Operation

PRAM has been evaluated using the same 3 test scenarios that were used in Chapter 4 with the existing RA tools. The analysis, management processes and the advantages and disadvantages of the prototype are then discussed before scoring PRAM on the same criteria as in Chapter 4.

7.2.1.1 Risk Analysis

Performing the risk analysis using PRAM is similar for all three scenarios, in the first part the user is firstly required to input the general information on the organisation including

the applications/business functions/types of data existing in the organisations. Then the user is required to score the importance of these to the organisation by considering the impact of breach/loss of confidentiality, integrity and availability to the organisation. This concludes the risk analysis part of the module by estimating the levels of risk the particular organisation is according to its characteristics and operation (as Figure 76 illustrates for the organisation in scenario 1).

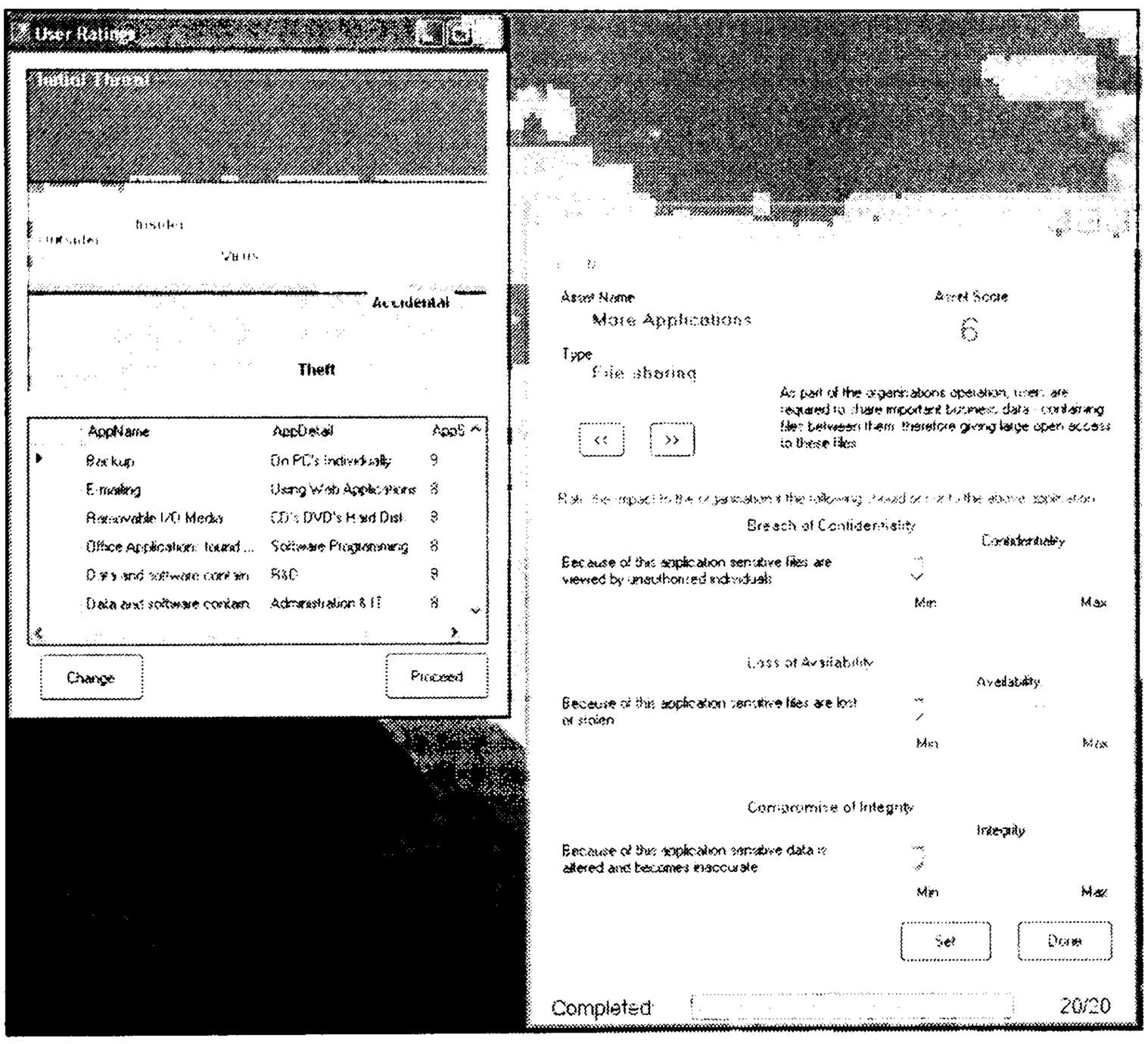


Figure 76: The Risk Analysis output

7.2.1.2 Risk Management

When using PRAM to manage the risks an organisation faces, firstly the user is provided with the capability, by clicking on threats on the coloured display, to graphically see what potential losses each threat might cause (Figure 77), this should help in choosing which threats should be given more attention to, judging by the likelihood/threat score (the

position of the threat on the coloured display) and the potential costs to the organisation of the threats' occurrence.

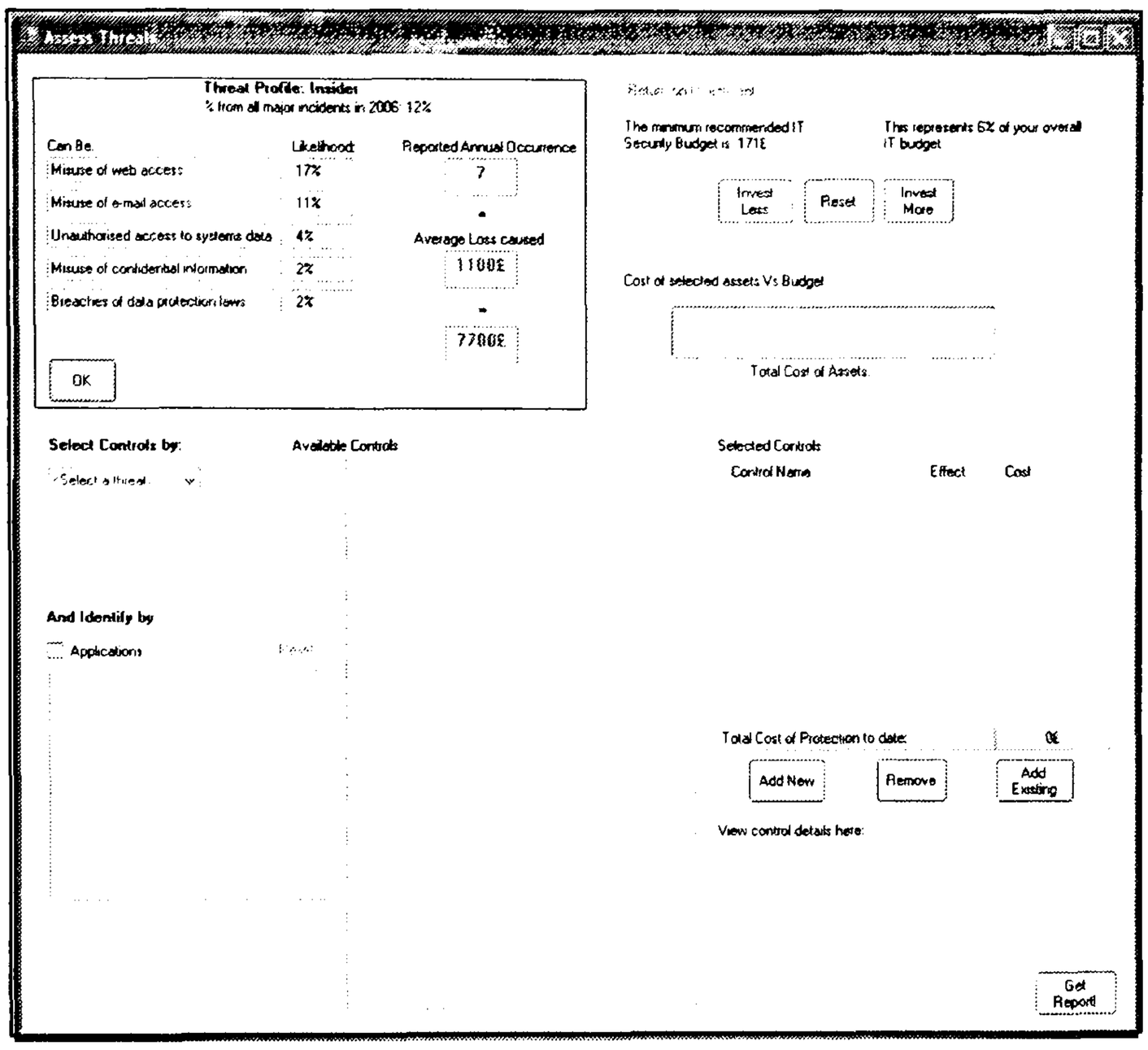


Figure 77: PRAM demonstrates ALE because of Insider Misuse

Having established the importance of each risk, the user can then proceed to the selection of controls, as discussed previously, the system recommends what the minimum budget devoted to security should be. Based on the threat the user wants to address and the application needing to protect the most (judging by the importance ratings in the previous part), the user is presented a list of all the controls that will decrease each threat with the corresponding ones to the selected applications highlighted. In the case of organisations with existing security controls that want to assess their security (which is the most likely case), the user can select what controls have already been implemented by the organisation and can visually judge which threats are still high and need more controls implemented (Figure 78). By selecting additional controls, the user can reduce all threats

to minimum levels while at the same time ensure that they remain within the desired budget (Figure 79). By contrasting Figure 76 and Figure 78, one can see how the initial threat levels the organisation faces are being reduced with the existing solutions, but leaving a couple of risks still at notable levels. These are then minimised by the addition of new controls, without however surpassing the recommended budget. This process is how PRAM will ideally operate in all scenarios. Among the benefits of using the PRAM graphical countermeasure selection approach the user can even remove controls that already exist from the organisations profile/security plan and add others which are more appropriate to reducing the existing threats and to the I.S. budget of the organisation.

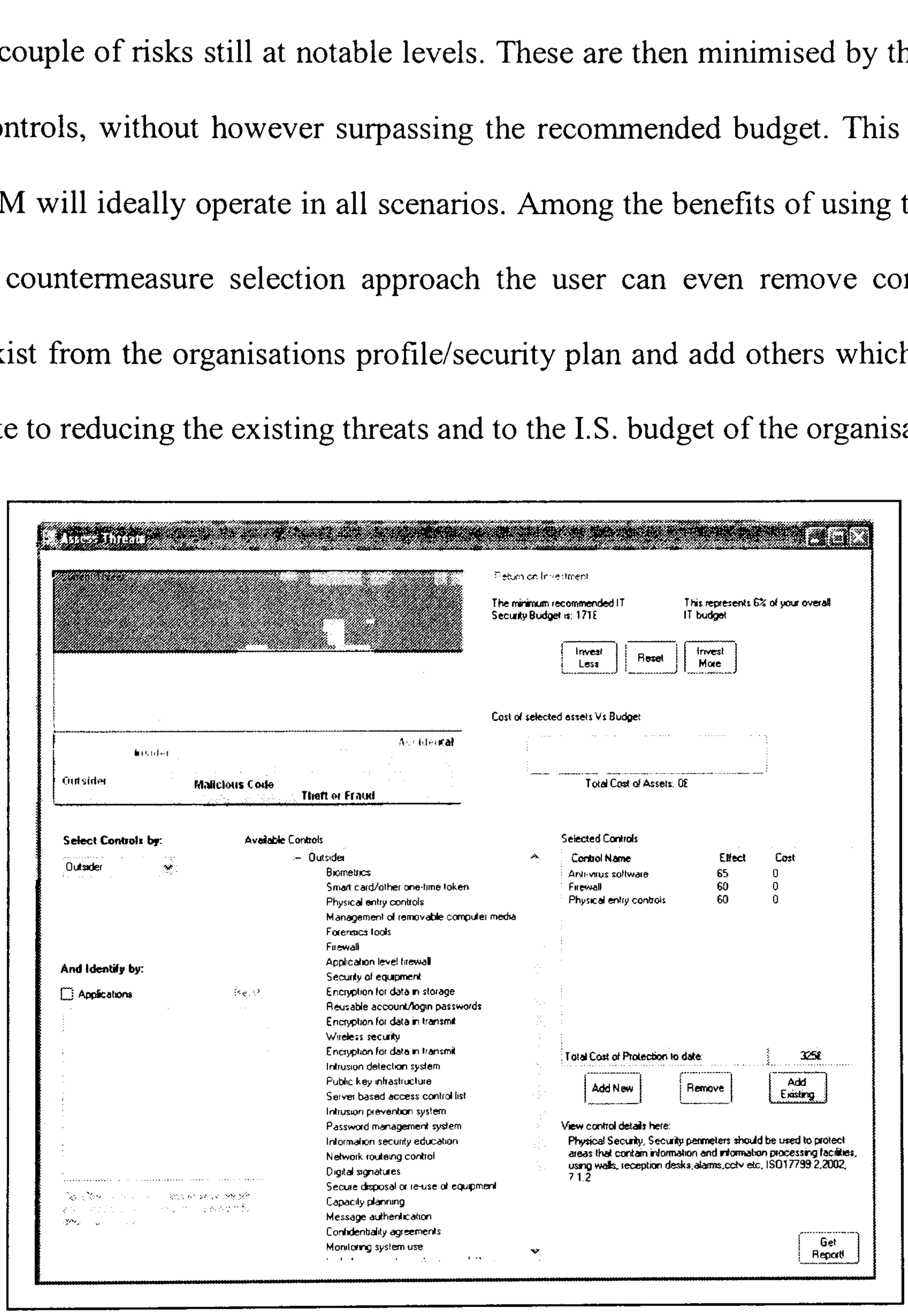


Figure 78: The main controls selection process – A

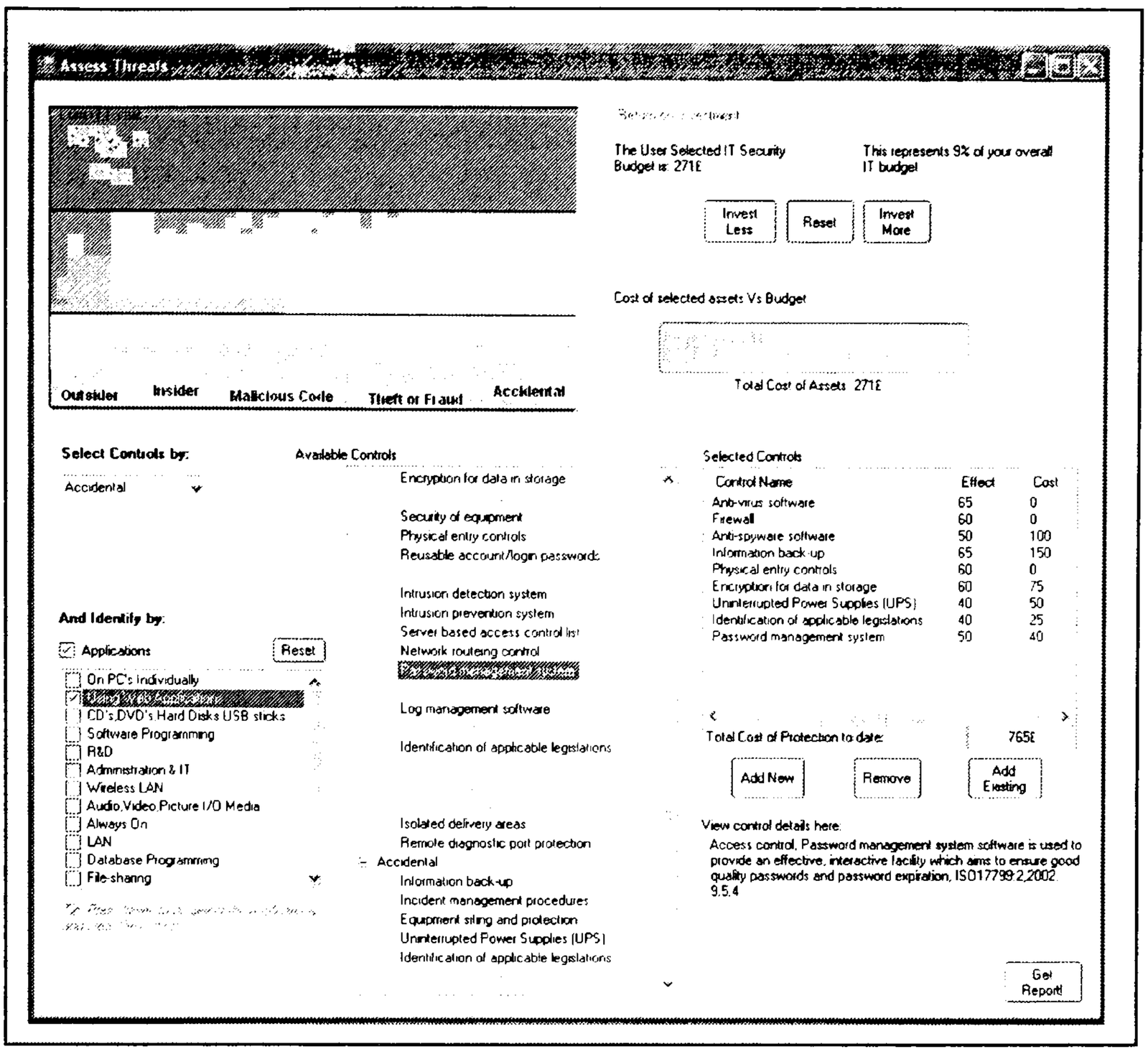


Figure 79: The main controls selection process - B

The difference that the diversity in size and sector of the organisations makes is visible in PRAM during the risk management process. Firstly in the risk levels which are partly equivalent to the sector, and subsequently in the recommended I.S. budget and cost of countermeasures that both consider organisation size. By looking at the coloured threat displays in Figure 80 (A for the small research organisation and B for the medium healthcare), the diversity of results according to the size, sector and organisational characteristics in PRAM is obvious.

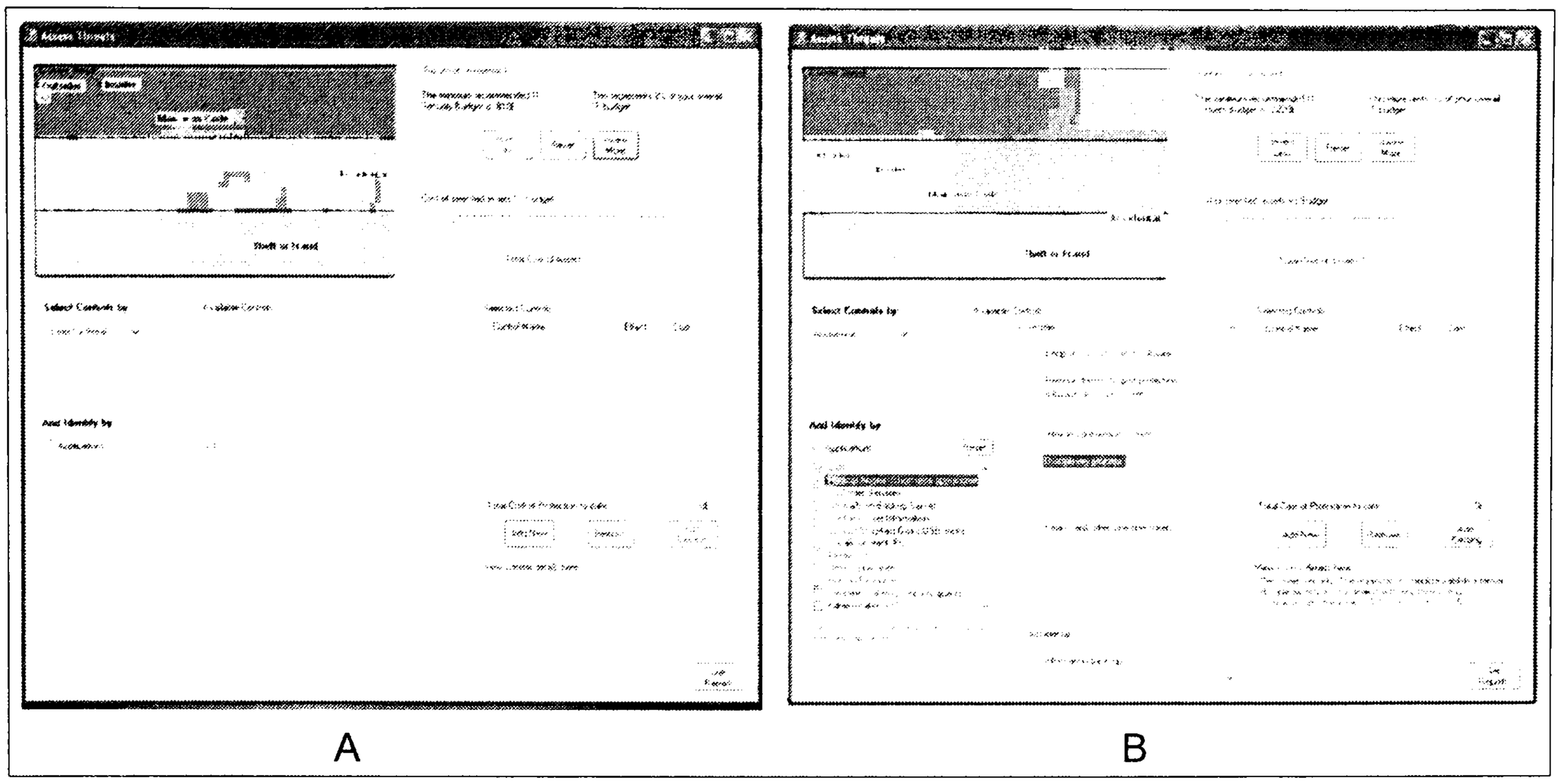


Figure 80: In PRAM threats vary for different organisations

Finally, by comparing Figure 81 and Figure 82, it is apparent that for the three different organisations, that have different security requirements, even though the essential countermeasures (such as the antivirus and firewall) remain the same, PRAM makes a clear differentiation on the required spending for I.S. countermeasures and to the required countermeasures themselves.

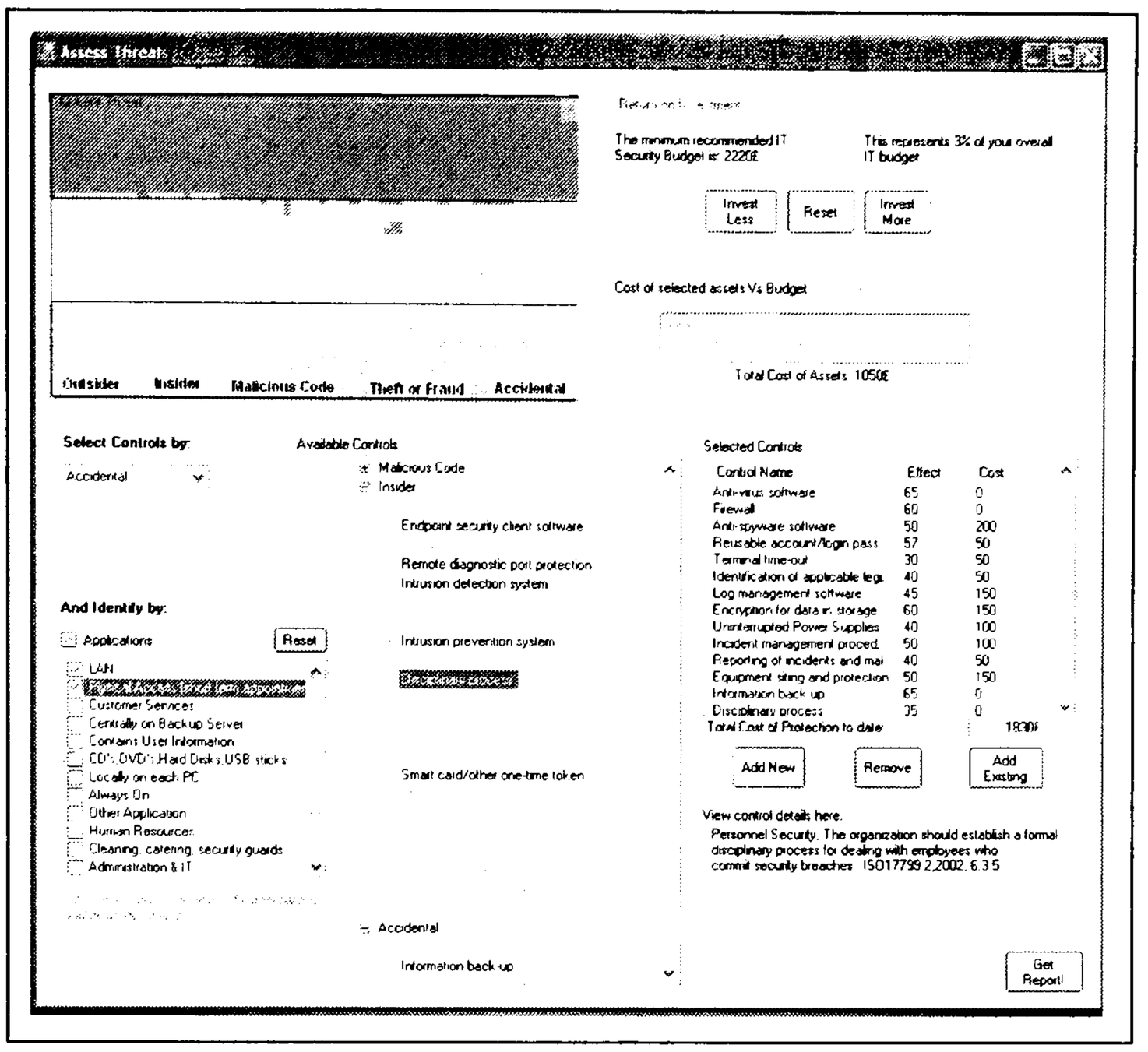


Figure 81: Variation of required controls for different scenarios - A

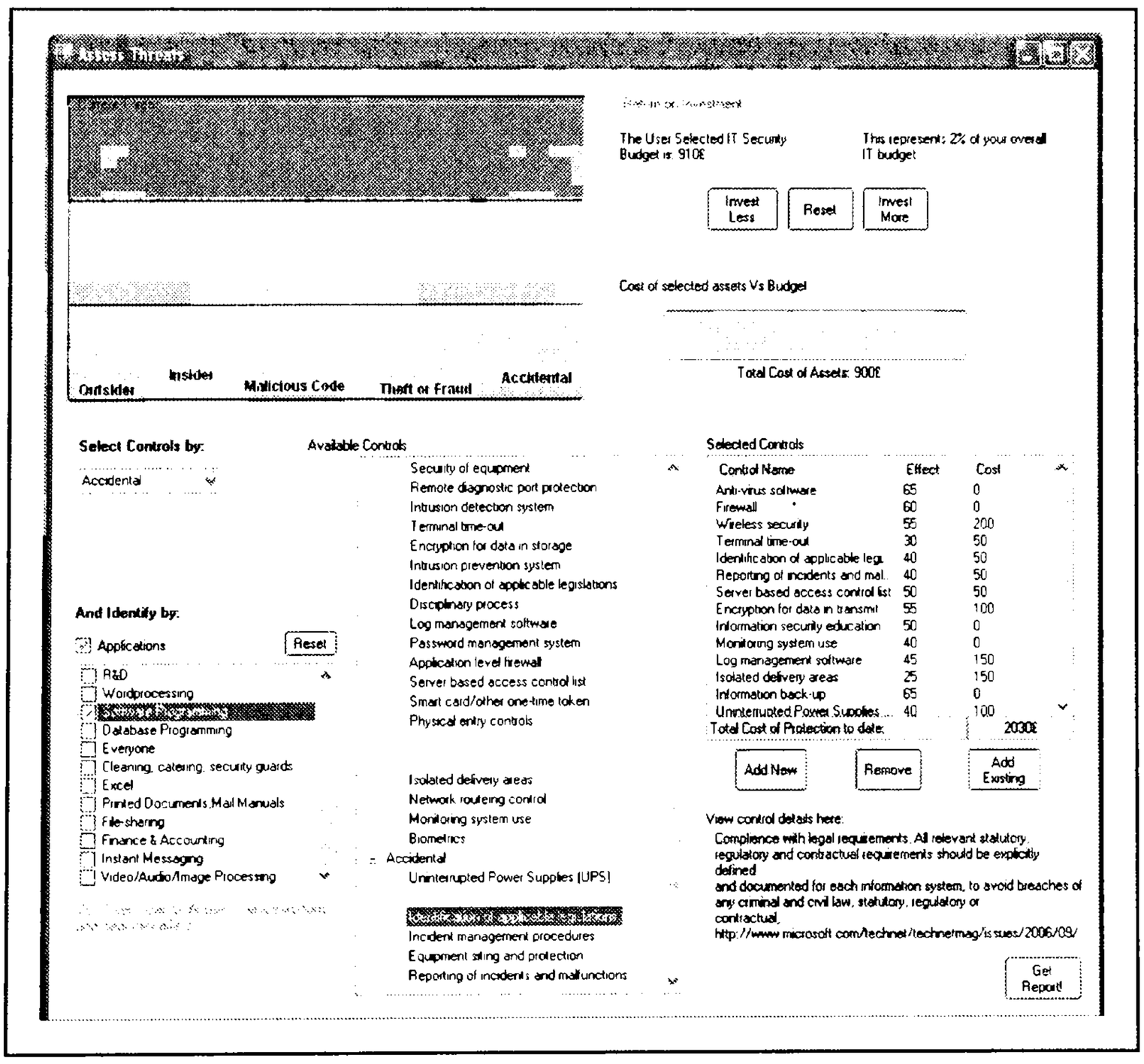


Figure 82: Variation of required controls for different scenarios - B

7.2.1.3 Feedback

As described in the previous chapters, the feedback module is essentially a progression of the Risk Management, acting as a dynamic I.S. support module to the SME. Even though none of the evaluated tools performs this function, it is considered to be one of the most useful features of PRAM. For the purposes of evaluating PRAM, the feedback module was used for fictitious scenarios of threats occurring to the selected organisations causing losses. As expected, when the losses and annual occurrence rates of threats were higher than the ones considered when first assessing the organisation's security' the tool suggested reconsidering security controls, this time having more realistic (to the specific organisation) figures.

Figure 83A illustrates how the third scenario of the medium sized healthcare organisation was reassessed to produce different threat levels and selected controls after reconsidering the case with the new data illustrated in Table 11.

Organisation Scenario 3: Medium sized healthcare organisation				
Threat	**Occurrence**	**Period controls have been implemented**	**Cost per incident**	**PRAM recommendation**
Malicious Code	3	5 months	500	Reinforce security
Theft or Fraud	2	6 months	2000	Reinforce security
Insider	1	7 months	500	No action required
Accidental	2	12 months	3000	Reinforce security

Table 11: Information input during feedback

By reporting these and re-running the assessor module, when selecting the existing controls, this time threats of accidental, theft or fraud and malicious code are not eliminated therefore as Figure 83B illustrates certain additional controls are required

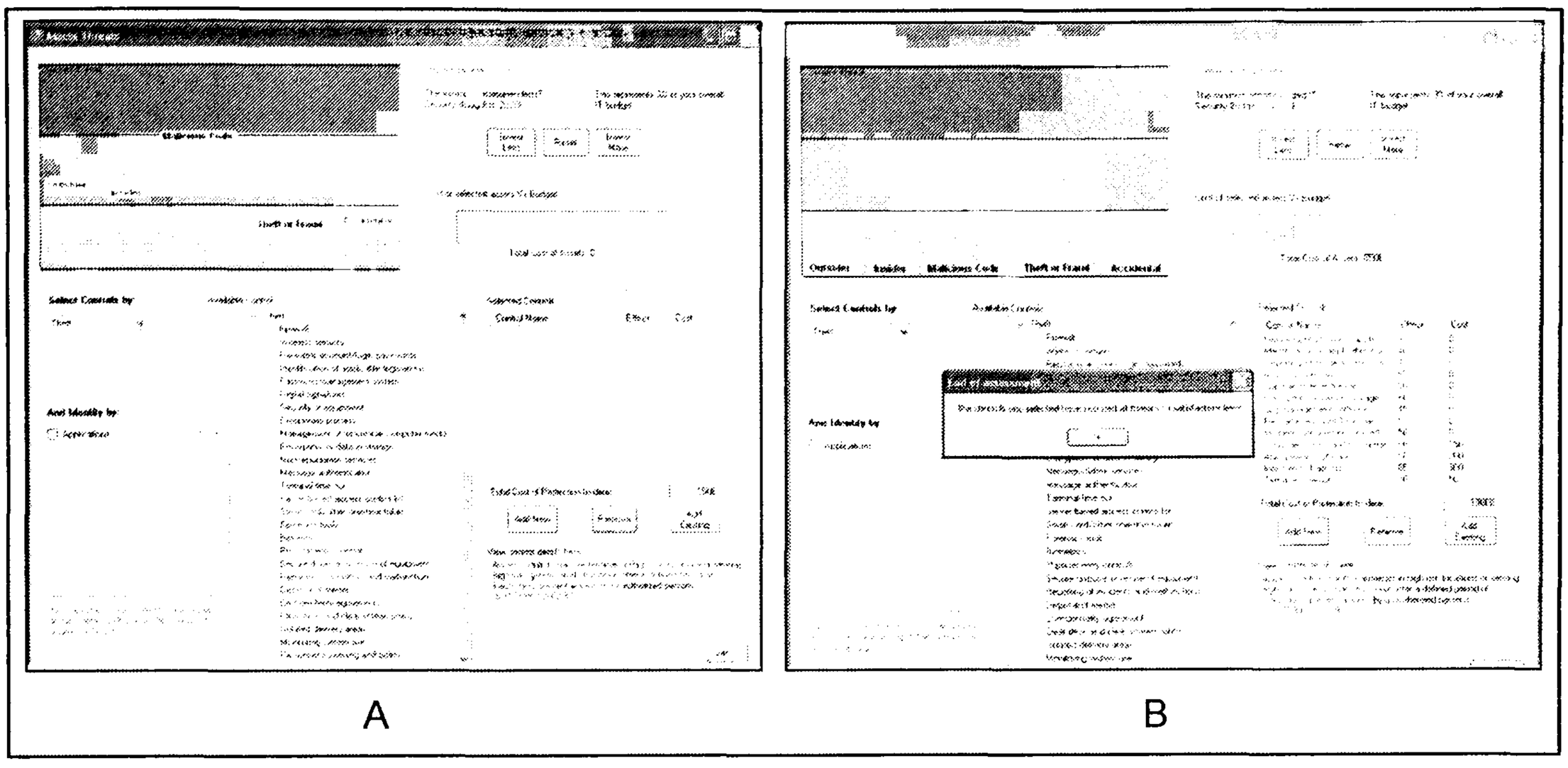


Figure 83: Assessing the threats after having reported flows in the existing security

This is illustrated as in Figure 83B, the addition of 4 new controls was required (the ones which add extra cost to the 'overall security to date') in order to minimise the threat that was reported in the Feedback as one that kept occurring and only after this addition did the system notify the user that the organisation is now safe.

Most importantly, as Figure 84 illustrates, this time the ALE is adapted to the specific numbers for the organisation.

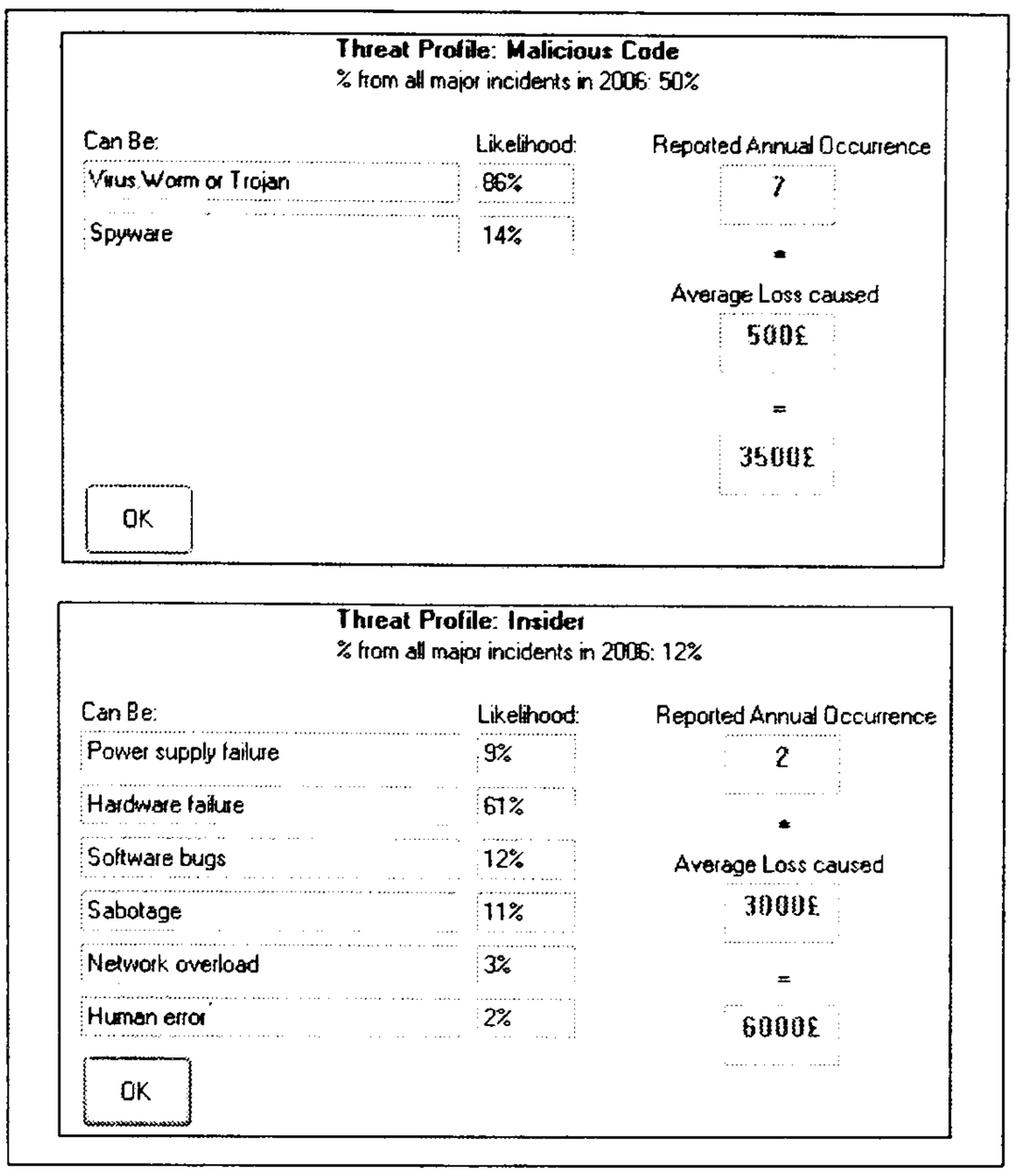


Figure 84: After feedback the threat ALE display is 'fitted' to the organisation

As discussed earlier the feedback module also provides the option to update applications however, apart from the already discussed benefits of this feature, this would not contribute anything to this evaluation so is not discussed here.

7.2.1.4 Advantages - Disadvantages against the existing tools.

- Advantages: By using the applications profiles, the analysis process is made notably shorter, eliminating the setbacks associated with the questionnaire based approaches other RA methodologies use. The analysis process concludes with a useful graphical illustration of the risks and risk levels the organisation is facing, raising the user awareness towards this issue which is the main purpose of a risk analysis but which the evaluated tools fail to address. PRAM offers addressing of the existing security practices, implemented controls and cost of security to date,

elements that other tools do not consider but simply address what controls are in place and recommend those that are missing from lists of all possible controls. Furthermore the existing tools do not recommend controls based on the specific organisations needs and budget. PRAM provides the option for dynamic feedback on the effectiveness of recommended controls, a feature which satisfies the requirement for complete management of the risks and which other tools do not address at all. PRAM offers the functionality for the user to build security from scratch or assess existing security, either by only complementing it or by also changing the existing measures

- Disadvantages: Using profiles shortens and simplifies the RA process; however it has an effect on the level of detail upon which the organisation is 'described'. However, since the requirement was not to produce a detailed RA methodology but a framework which lies between this and the baseline guidelines, this disadvantage has a minor effect upon the operation and ability of PRAM to perform what it was designed to (i.e. inform, guide, assist and raise the awareness of SMEs).

7.2.1.5 Evaluating PRAM's technical characteristics

During the evaluation of PRAM, no technical issues occurred, the prototype was tested in several computers both desktops and laptops (all Window-based) and there were no programming or interoperability issues recorded. Both the Visual Basic interface as well as the data interactions with MS Word, Excel and Access did not present any problems.

Finally, the software is small in size and does not occupy much space on the target hard-drive, installation is simple and short and there are no additional software or hardware elements required to be purchased or present for PRAM to operate apart from the MS Office components previously mentioned.

7.2.2 Discussion on the characteristics of PRAM

In this section PRAM will be evaluated on the same characteristics the other RA tools addressing SMEs were judged upon in Chapter 4. These characteristics represent the requirements of SMEs from an RA tool therefore will indicate if the PRAM framework is suitable for the purposes it was designed for.

7.2.2.1 Characteristics evaluation

Table 12 presents the scores achieved by PRAM after evaluating it on the same criteria as the RA tools in Chapter 4, together with a justification of why these scores were assigned to each feature of the framework. Considering these criteria constitute teh identified needs of SMEs from a RA tool, the following results aim to illustrate how appropriate PRAM is for these organisations and how it addresses the purposes it has been designed for.

Requirement	Score	Justification
Cost	3	PRAM is not a commercial product
Ease of use	2.5	Virtually anyone who has been involved in the organisation enough to know very basic information on the applications found within can use it.
Length of Process	3	The assessment can be completed in approximately one hour.

Assistance to user	3	The prototype is accompanied by a user guide including a worked example, there is also adequate assistance within the tool.
Risk Impact Analysis	.5	PRAM suggests controls based on the organisations requirements for security vs productivity, on the importance of the applications and also on the threats the organisation is under, demonstrating elements such as the ALE to the user. Does not get full marks since initially (before running the feedback) the outputs and recommendations are based on survey data therefore might not be 100% appropriate to the organisation in question.
Assistance in choosing controls	3	The controls are listed in order of priority in terms of price, intrusiveness or effect according to the organisations needs. Furthermore controls are filtered and recommended to the user based on the identified threats the organisation is under and the existing applications.
Cost – Effective Controls	2	Cost of controls, increased costs due to size of the organisation is considered and ALE to assets because of threats occurring is considered, the user is then required to make the decision.
Comprehensive output	3	The tool presents the user with a comprehensive report illustrating only the required data to understand and face the problem.
Deployment assistance	2.5	PRAM provides details on threats and how they have been decreased, information on what the controls are and carefully selected links to more information on implementation and configuration issues. Does not get full marks since it is provided via external links
Length of Report	3	The tool presents the user with a comprehensive report illustrating only the required data to understand and handle the problem.
Dynamic Feedback	3	There is none provided, no consideration on the effectiveness of the solutions, can rerun the tool and select the newly implemented control as existent, however, there will still be no consideration of threats that occurred or losses
Dynamic Update	2	The dynamic update requires the users input which might introduce errors and disruptions. However if update performed by the programmer, it is quite straightforward since no changes in the tool are needed, only changes to the database which can easily be located and replaced by the user if provided with the updated version

Table 12: The evaluation characteristics of PRAM

7.2.2.2 PRAM's output and how it compares to that of existing tools

Section 7.3.1 has described how PRAM's output differentiates according to the different organisational characteristics such as size, sector, budget and applications. Before proceeding to the discussion on the scores PRAM has achieved against the other tools on the evaluation, a brief comparison of the prototype's output with that of the existing tools will be discussed. PRAM's outputs for each of the three scenarios are also included in Appendix E. Comparing the output of PRAM with that of MRSAT, the Microsoft tool provides a longer and more detailed report, however PRAM's output simply illustrates the elements that needs to be included and a working version could easily be updated with more descriptions and additional links to information. What is most important here is that PRAM includes much more justification on why the controls should be implemented and what they will offer, being more useful to justify such investments to the management. Compared with Cobra's report, the layout of the report gives a more 'professional' impression and allowing the user to select the elements they wish to be included in the report is a useful addition to avoid lengthy reports. However, the quality of the recommendations is not appropriate for SME's requirements as identified and therefore PRAM, at least naming the countermeasures required and providing some information on what they are and how to implement them, does provide a more useful output to the SME user. Finally, the automatically generated countermeasure list in the Buddy System is a good element, however the automatic suggestions are not necessarily always correct and furthermore as discussed in Chapter 4 the recommendations are too

vague and in a similar way as with Cobra, PRAM's output is again more useful to the SME user.

7.2.2.3 Characteristics comparison table and discussion against the other tools

As means of comparing the appropriateness of PRAM for SME use, and Table 13 illustrates the marks achieved by PRAM when evaluated against those in Chapter 4.

Category	Criteria	MRSAT	Cobra	Buddy	PRAM
General	Cost	3	2	2	3
	Ease of use	2.5	2.5	2	2.5
	Length of process	2	1.5	1.5	3
Process	Assistance to user	3	2	2	3
	Risk Impact Analysis	1	1	2	2.5
	Assistance in choosing controls	2	1	3	3
	Cost – Effective Controls	1	1	1	2
Output	Comprehensive output	3	2	1.5	3
	Deployment assistance	2	1	1	2.5
	Length of Report	2.5	3	2	3
After	Dynamic Feedback	1.5	2	2	3
	Dynamic Update	2	2	2	2
Overall	Category: General	7.5/9	6/9	5.5/9	8.5/9
	Category: Process	7/12	5/12	8/12	10.5/12
	Category: Output	7.5/9	6/9	4.5/9	8.5/9
	Category: After	3.5/6	4/6	4/6	5/6
	Total (out of 36):	**25.5**	**21**	**22**	**32.5**

Table 13: PRAM scores against the commercial tools

This result illustrates the appropriateness of PRAM for addressing SME information security assessment and planning needs. The final score as well as the individual scores were expected to fair better from those of the existing tools, since the factors upon which

the tools were evaluated are the requirements of the SMEs from an RA tool and therefore the requirements that this methodology were designed to address.

7.3 User evaluation of PRAM

Following the evaluation of PRAM in a similar way as with the previous tool, further testing was conducted to investigate whether the goals for ease of use, assistance to the user etc that PRAM was designed to address have been successful. Thus this evaluation needed to be performed by objective users.

7.3.1 Background

This section provides information on the background of the evaluation, such as, the users attended and the methodology of the evaluation.

7.3.1.1 The users

The practical evaluation of PRAM was performed under 'controlled conditions' within the University of Plymouth in a laboratory were the MSc Information Systems Security students were asked to attend. These students were asked to attend since they had been presented with the basic concepts of RA in the past and as part of their course material they had been demonstrated the use of Symantec's INFORM method. They therefore had some understanding of RA and an organisations requirement for planned security, without however being security experts. Invitations were issued to approximately 30 potential participants, overall 9 users participated in this evaluation:

- The users were aged between 22 and 27 years old.
- 6 of them had been employed by an organisation before, out of which 4 were in I.T. related positions.
- 6 stated they have some information security knowledge, only 2 had used RA in the past.

These fulfil the overall goal that the participating users are sufficiently informed on how an organisation operates and on basic security issues and also have some understanding of how organisations operate. The participants were not I.S. experts since they were only in the second month of their MSc education, they do however have some basic understanding of risk and certainly because of the area they chose to study they have the motivation to consider and study the RA tools offered to them for this evaluation in a mature and careful manner. Ideally it would have been preferable for SME members to have participated in the evaluation of PRAMM against the commercial RA tools; this however was not possible due to two reasons. The main reason had to do with time constraints associated with this project and the second with the likely unwillingness of SMEs to participate in such an evaluation, justified by the previously identified characteristic of SMEs that they cannot afford disruption to operations but also in the identified reluctance of SMEs to even participate in the SME security survey that was conducted by the author, a procedure much less time consuming than this evaluation. The MSc students are not comparable to the sort of people likely to be using such a system within an SME, they were however judged to have the appropriate knowledge so as to

evaluate whether these RA tools are user-friendly and easy to use which is the purpose of this second evaluation.

7.3.1.2 Methodology

The process the users were required to go through during this evaluation is described in detail in Appendix C, which includes the handout they were given. The two-hour lab session for evaluating PRAM required the users to select one of the three commercial SME RA tools available to them (essentially because of the time limit of two hours it was decided that it would be preferable for the users to perform a thorough RA using one of the commercial tools and PRAM, devoting an hour for each, rather than briefly going through all the solutions). Then they were asked to devise a scenario of an organisation they would assess the risks of, similar to the three scenarios used in the author's evaluation (this option was mainly intended for those that had industry experience; those that did not could use the existing scenarios). Following that, the users were required to assess the risks of this organisation using firstly one of the commercial tools and then using PRAM on the same scenario. Finally the users were asked to complete a questionnaire (a copy of which can be found in Appendix C) provided which investigated the issues this evaluation is concerned in. More specifically, after collecting information on the user and their background, the following issues were investigated:

- The 'Use of the tool' (ease of use, interface, better approach for analysing the organisation), to address what the users perceived of the operation of the tools.

- The 'Output' (assistance with implementation of controls, which would be more useful to the management), to address the user's opinion of the appropriateness of the tools on the requirements of SMEs.
- The user's opinion on the Feedback feature, to investigate whether this is a useful addition to the RA process.
- Finally the questionnaire considered adoption of RA issues such as whether the users would use such a practice in their organisation, which and why or what would deter them from the adoption of RA, in order to consider whether PRAM has achieved what it was designed for and therefore the new approach to RA is more appropriate for use than the existing tools.

7.3.2 Findings of the evaluation

This section presents a discussion and an analysis of the evaluation results. In the graphs provided, the results are illustrated according to the commercial tools the users have evaluated against PRAM, before presenting the overall outcome in each issue investigated.

7.3.2.1 Use of Tool

This investigation began by considering the users perception of the ease of use of the tools, all 9 users stated that PRAM was easier to use than the commercial products they evaluated. Figure 85 illustrates the users view of the user friendliness of the RA tools

interface, as the results illustrate the majority preferred PRAM's GUI while a user also favoured the MRSAT interface.

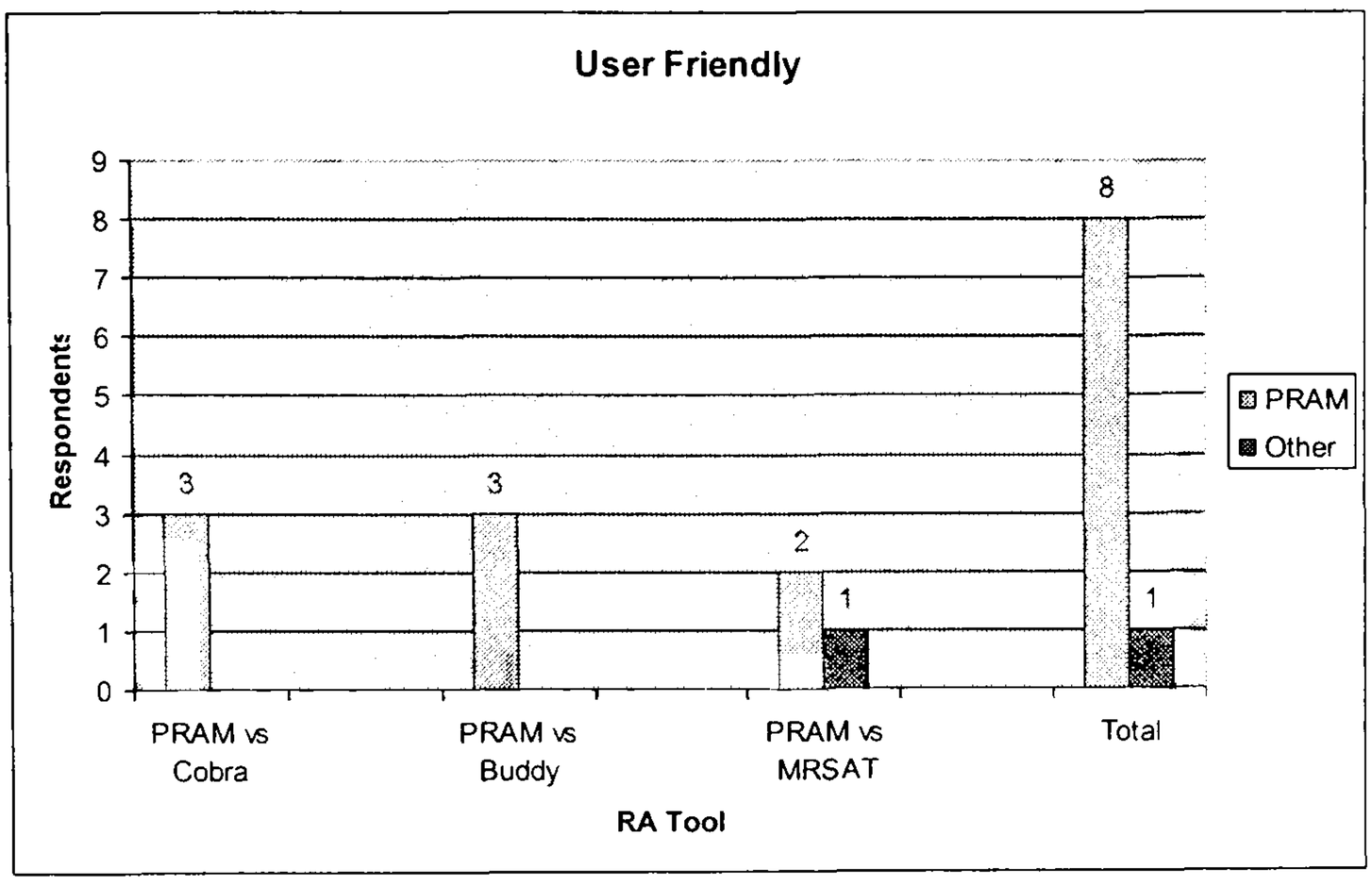


Figure 85: The user's views of the RA tools interface

Figure 86 illustrates the users view on which tools provide the better assistance to the user performing the RA. According to this, the majority of the respondents (8) judged PRAM provides the user with more assistance while the Buddy System came second with one preference.

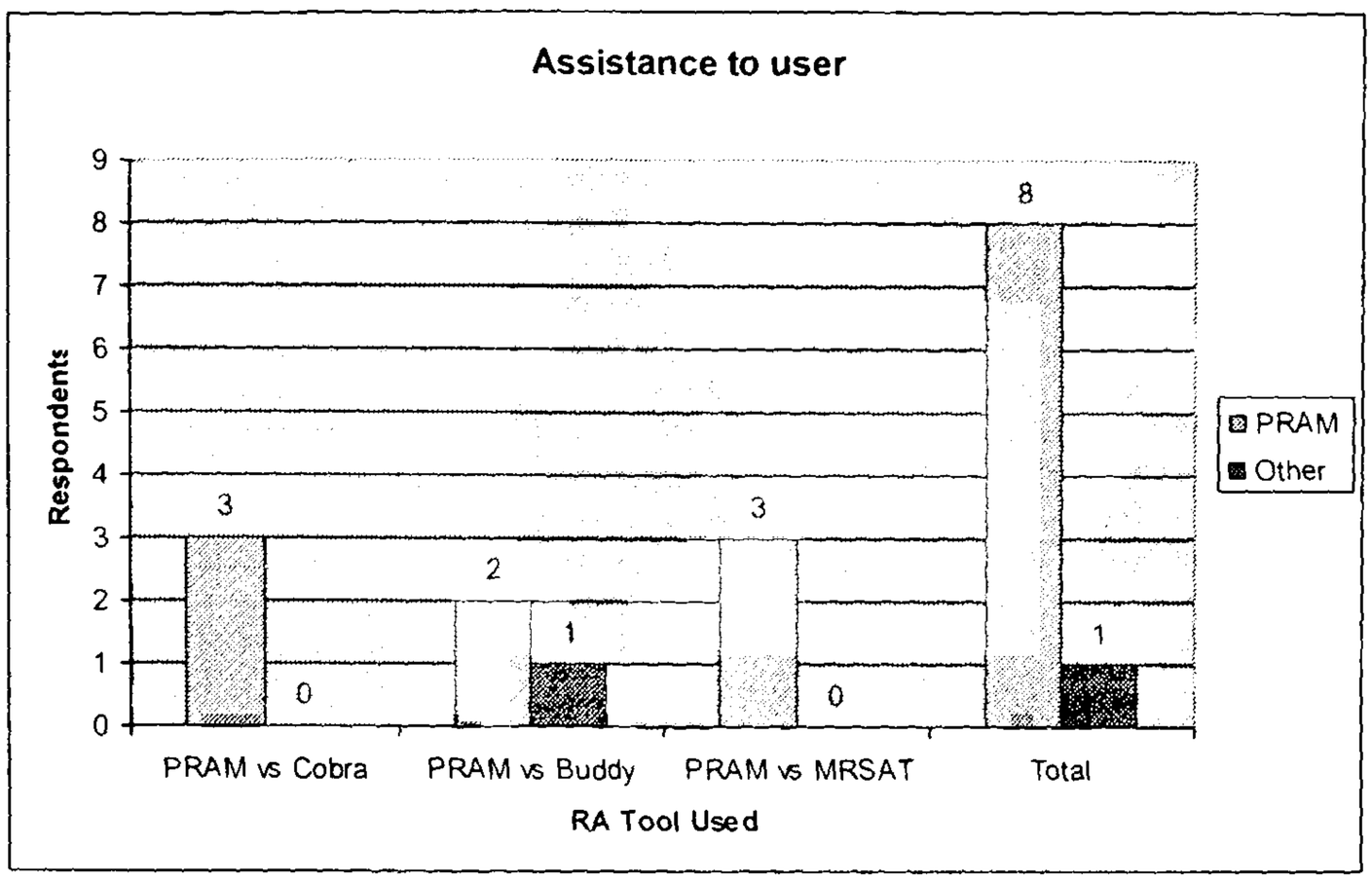


Figure 86: Which of the tools provided more assistance to the user

The users also favoured the use of profiling compared to questionnaires for analysing the organisation and its assets (Figure 87). It is characteristic that many of the users were dissatisfied with the amount of time required by the commercial tools and commented upon this negatively (as can be seen in the quoted comments in Appendix D) while on the other hand the majority of the users stated they preferred profiling because of its ease of use and much shorter period required to complete the process.

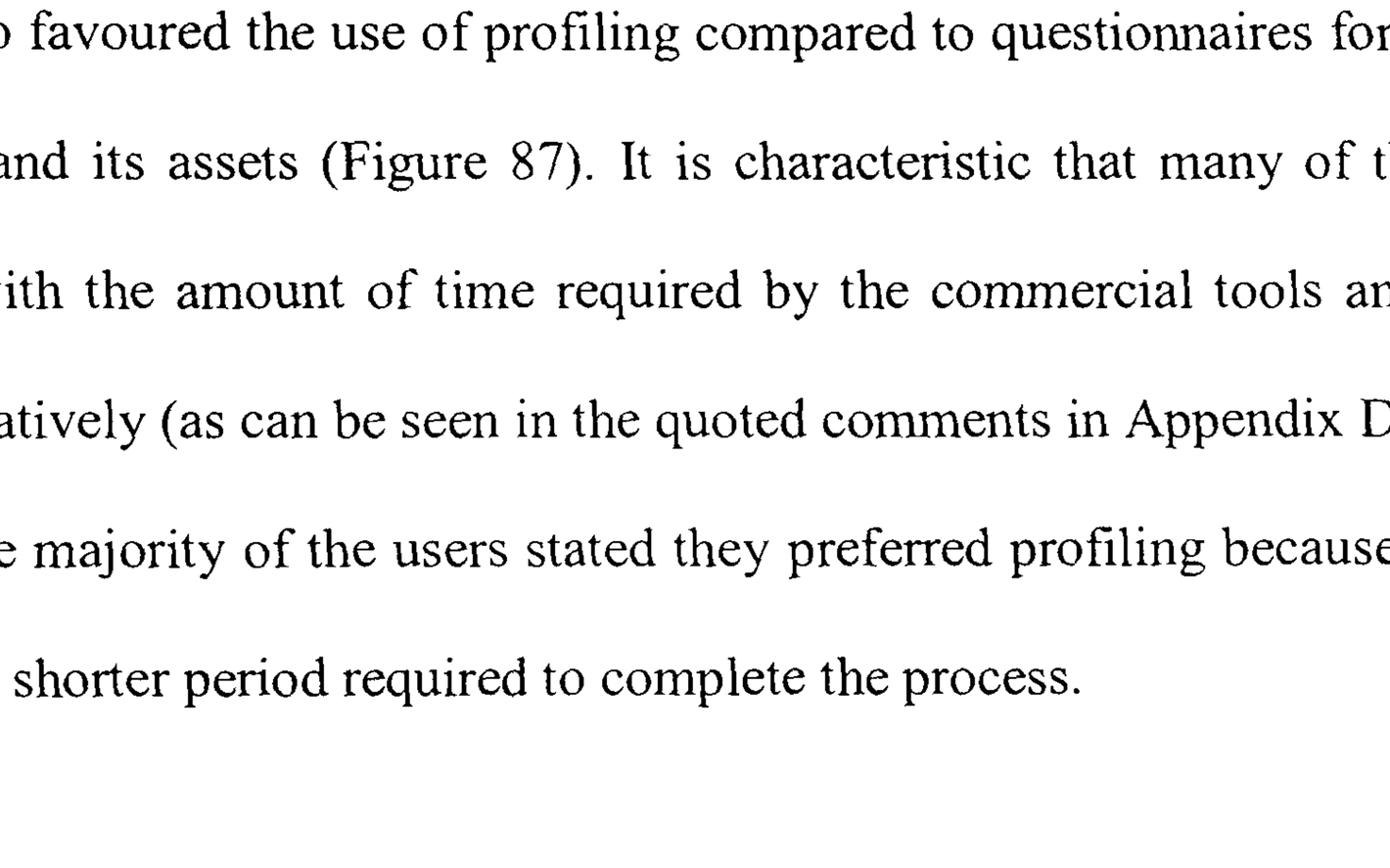


Figure 87: Preferred method for the analysis of assets

Finally, one of the elements that do not exist in the evaluated tools but is a novel feature of PRAM, the financial considerations of ROI of security solutions and the illustration to the user of the ALE because of the threats the organisation faces, were also perceived as a good addition by the majority of the users (Figure 88).

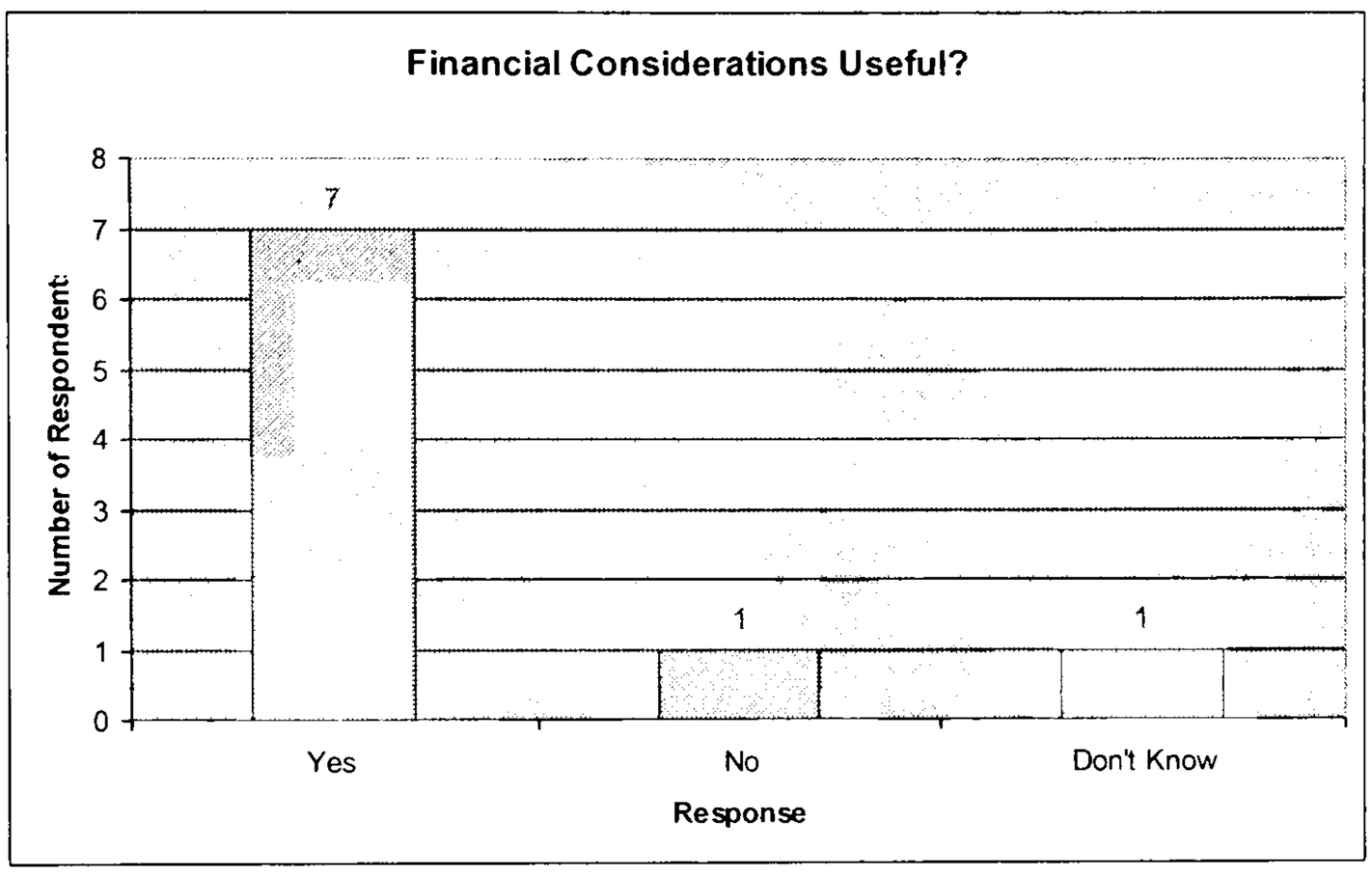


Figure 88: Users perception of the financial considerations in RA

7.3.2.2 Output

This part of the evaluation aimed at gathering user opinions on the appropriateness and usefulness of the output reports provided by the RA tools used. As Figure 89 illustrates, the users were first asked to state which, in general terms, output they found to be more useful. PRAM's output was judged to be better than Buddy's, slightly better than MRSAT's but not as good as Cobra's report.

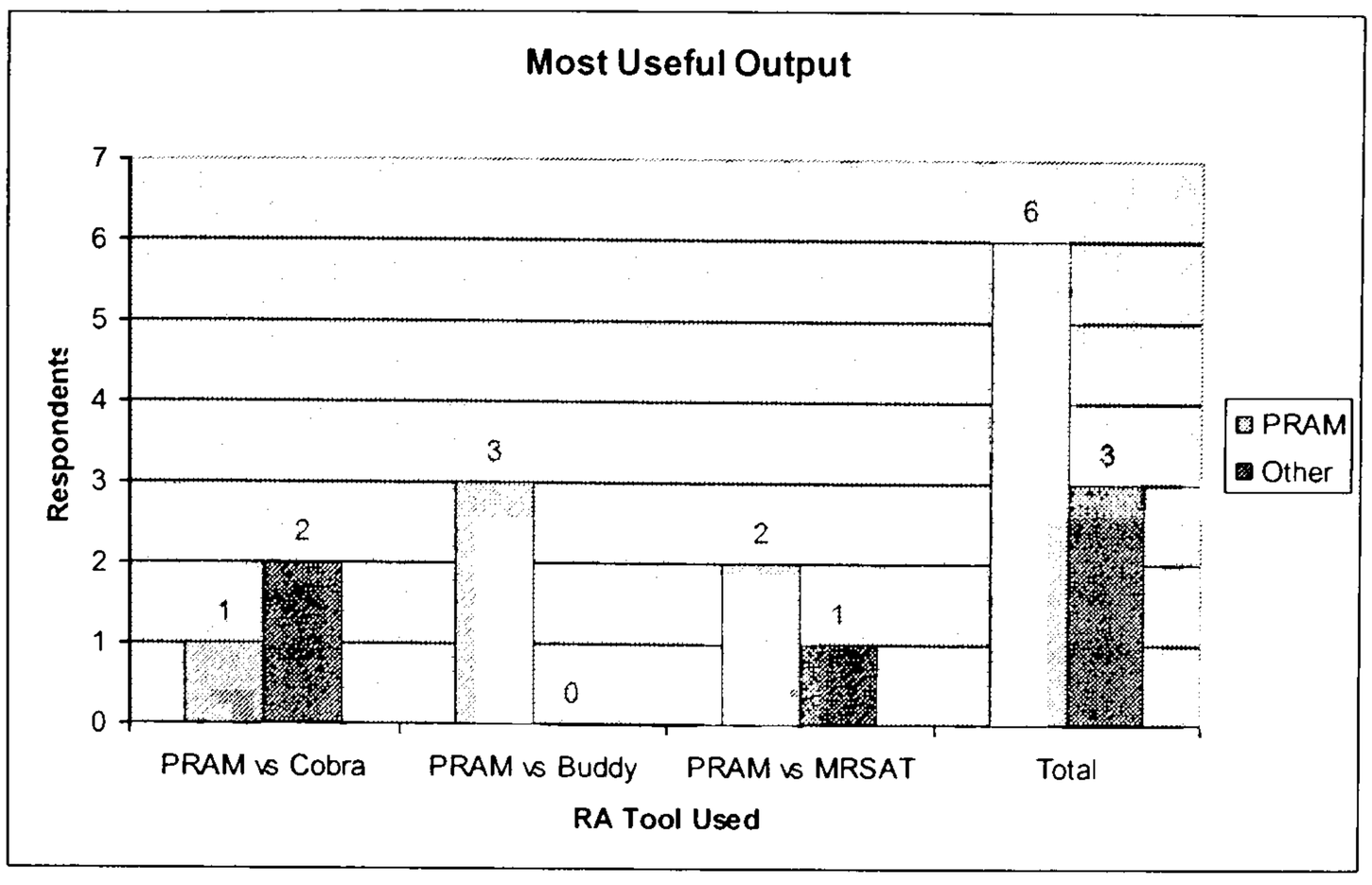


Figure 89: Which output was most useful

When queried the users which output they judge as to contain the better information on issues about the implementation of the suggested countermeasures, PRAM's approach of providing external links to information was perceived as somewhat more appropriate that that of the other tools (Figure 90).

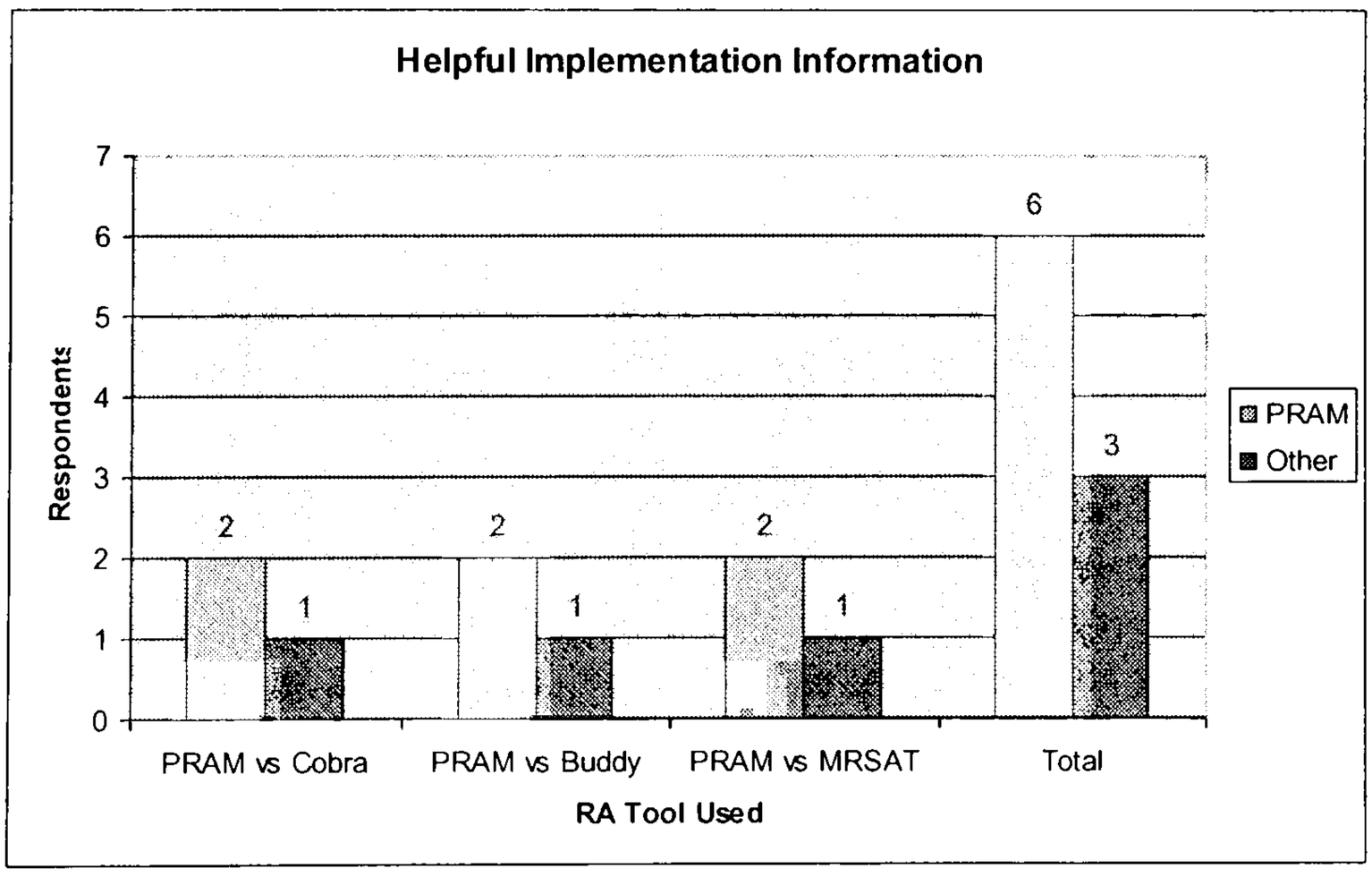


Figure 90: Users view of the offered guidance to implementing controls

However, when the users were required to state their view on which output was more useful to illustrate to the management, all 9 of the respondents favoured PRAM confirming this way that the required objective of creating a methodology whose output can raise managerial awareness on security issues and justify security spending has been achieved.

7.3.2.3 Feedback

This section of the evaluation basically addressed how the feature of feedback and subsequent threat management, which was conceived as an essential part of an RA tool for SMEs, is viewed by the users. The results illustrated in Figure 91 were satisfactory as none of the respondents found this addition unnecessary. Most users (7) considered the feature useful, and one regarded it as imperative for RA tools.

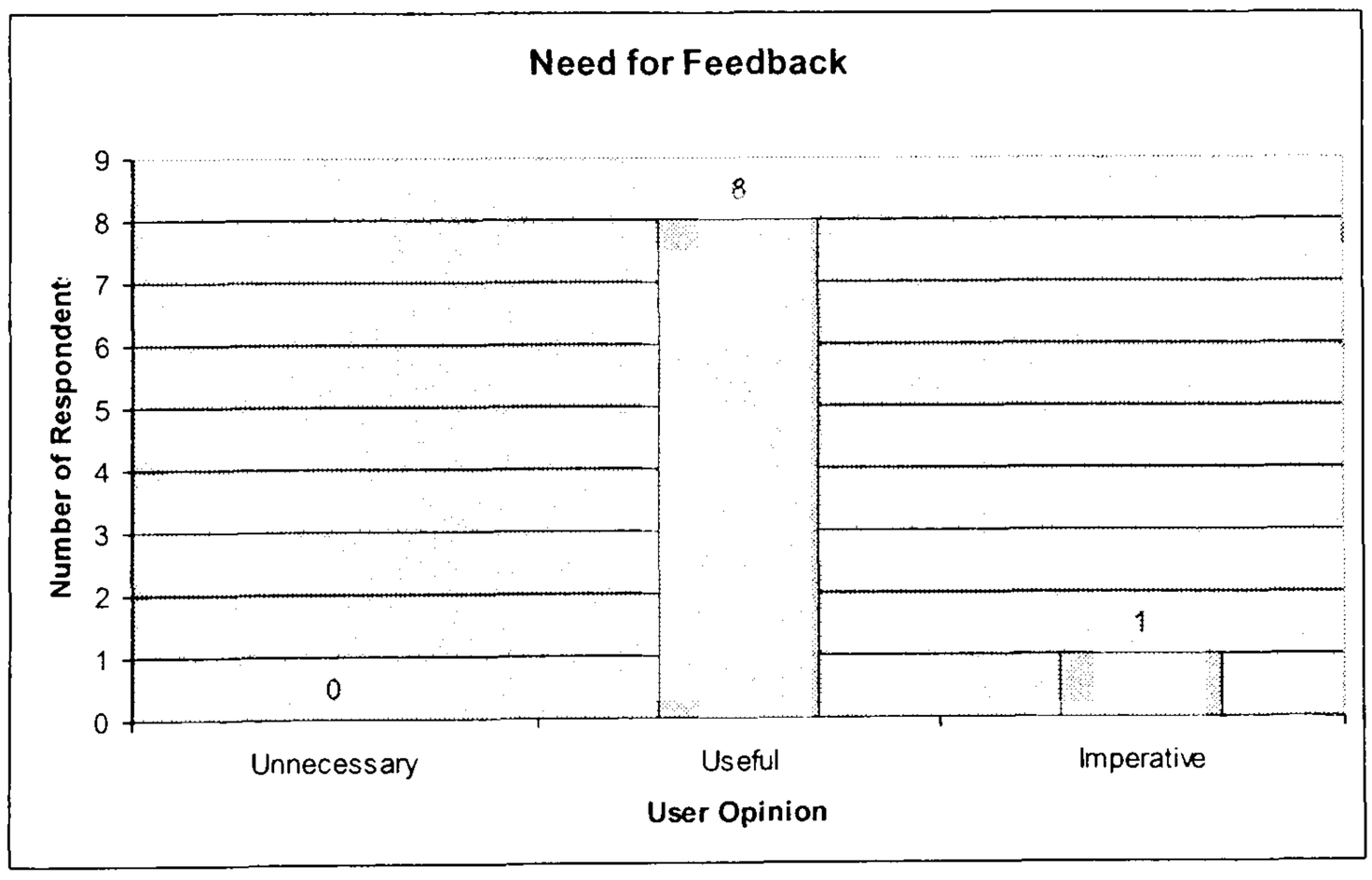


Figure 91: User opinion of the feature of feedback included in RA

7.3.2.4 Final Thoughts

Concluding this evaluation, this final part investigated what final impression the RA tools and PRAM have left with the users. Overall, as Figure 92 illustrates, the users were positive both in the appropriateness of PRAM for use by an SME as it was favoured by 8 of them. The number of users that stated they would use a fully working version PRAM over the other RA tools in real life was 7, which is also a positive outcome.

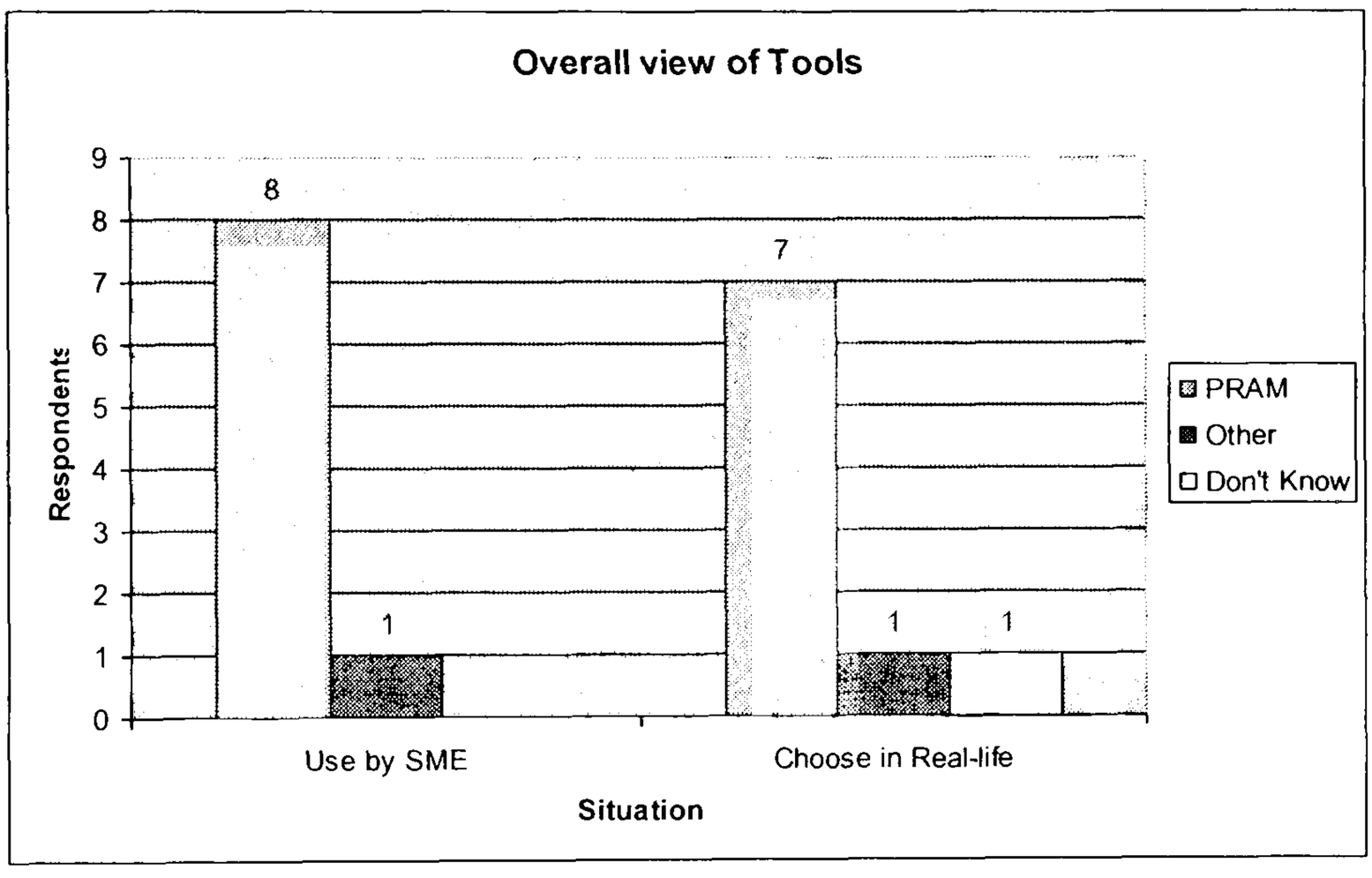


Figure 92: Overall opinion of RA and PRAM

Finally, having used the RA tools, the users were asked to state what characteristics they perceive as deterring for the widespread adoption of RA tools. As illustrated in Figure 93 most of the users selected the ease of use as a deciding factor and the time needed to perform the RA as major reasons. One user stated that cost might be a deterring factor.

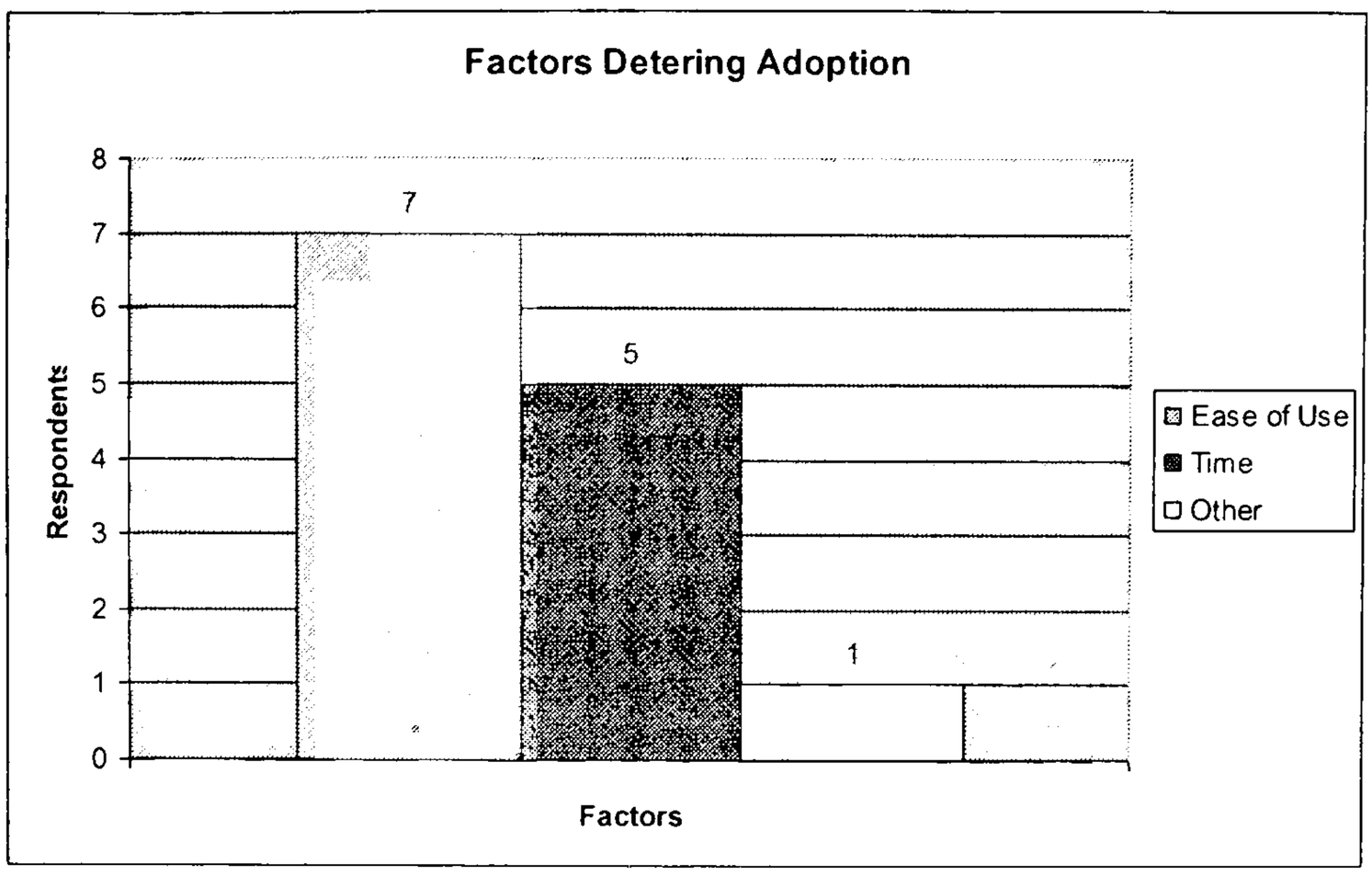


Figure 93: Factors which might deter the adoption of RA by SMEs

It is worth noting that, as also confirmed by the user quotes in the Appendix, the users were mainly disenchanted by the commercial tools complicated approach and long period of time required to perform the assessment. As also stated by the users these issues are not valid to the case of PRAM.

7.4 Discussion on the evaluation results

Overall, the greatest concern with the users evaluating the tools was ease of use, time required to complete the process and the difficulties faced by the questionnaire-based approaches that the users perceived negatively. One can say that as students cannot afford to devote enormous period of time to perform such an assessment, similarly an SME manager (or even employee) cannot afford such a disruption to their everyday tasks. Overall PRAM was preferred, with only minor hesitations on the output, which however, is simply illustrative of what it should include. In terms of ease of use, and all the additional features of PRAM compared to the other tools, like feedback, profiling and

ROI were received very positively and gave PRAM a clear advantage from the users that evaluated the tools.

Interestingly, (as can be seen in the user quotes section in Appendix D) some of the users that stated they would use PRAM in real life also stated they would use PRAM for an SME and one of the other tools for a large organisation or that they would use PRAM as an introductory RA tool and then use one of the rest for a more detailed assessment. This is not a negative for PRAM, as firstly, as has been largely discussed throughout this thesis, PRAM has been designed not to be a thorough RA methodology but a progression of guidelines raising SME awareness and providing as much simplicity and assistance as possible instead. Secondly, it has also been made clear that this prototype version of PRAM is not as detailed as a fully functional version but aims to demonstrate the novel features and the functionality of the approach. Therefore these comments simply illustrate that PRAM has achieved the purposes it was designed for.

7.5 Conclusions

The evaluation of PRAM established it has achieved the aims and objectives upon which it was designed. The first evaluation proved the PRAM process and output surpass those of the existing RA tools on the issues SME's are mainly concerned with and have been deterring such organisations from adopting RA. During that first stage of the evaluation PRAM has shown to be good at assessing different scenarios of organisations and provided adequate results according to the size, sector and assets compared to the tools evaluated in Chapter 4. Furthermore the second, practical, part of the evaluation of

PRAM has illustrated that it has surpassed the issues SME's are concerned with when it comes to RA. With the attention to ease of use, assistance to user and user-friendly interface, having profiled assets behind applications thus allowing the simple analysis of the organisation, and allowing subsequent management of threats, the users that evaluated PRAM have shown a significant preference to this prototype over the existing tools. Their responses illustrate that this approach would be preferable for adoption by an SME.

8 Conclusions and Future work

To conclude this thesis, this chapter summarises the achievements of the research, then proceeds to discuss the limitations that were faced during the study and ends by discussing the areas of RA for SME that require further development in the future.

8.1 Achievements of the research

This research has achieved all the aims and objectives specified in Chapter 1. Specifically, this research has:

1. Established the importance of RA for organisations, and particularly to those of small and medium size which do not tend to employ trained security specialists to handle the task of securing the network, The research has identified that SMEs tend not to follow either the path of RA or other solutions available to them, with the consequence that they face avoidable security issues.

2. Analysed current solutions (e.g. outsourcing, guidelines, and their automated progressions) and established that they inappropriate for use by SMEs. These solutions are simply a guide through all the available controls and security practices without either any assistance in selecting countermeasures or implementation details of controls. By contrast, SMEs require a solution that can be used and interpreted by, as well as provide useful assistance with selecting controls and a comprehensive output to, the non-trained SME user.

3. Identified the requirements for RA methods in SME scenarios. By examining survey findings and conducting a practical evaluation of existing RA solutions (focusing upon those that are designed for use by SMEs), the current limiting factors were identified. This led to the identification of those elements that a novel RA solution should include in order to successfully address the requirements of SMEs.

4. Specified a novel RA methodology based upon the aforementioned requirements. A progression of the traditional RA process has been designed and the Profile-based Risk Analysis and Management (PRAM) architecture created. The main characteristics of this architecture are the use of Protection Profiles, inclusion of financial elements, and a comprehensive user interface and output.

5. Implemented a proof-of-concept prototype which illustrates how the previously conceived features have been implemented in practice. The resulting RA tool consists of four different modules: the Organisation Profiler which assists the user in inputting the organisations details to the system, the Application Handler which assists the user with valuing the importance of the identified assets, the Assessor module provides the SME user with all the required details to select appropriate countermeasures and the Feedback module which provides the subsequent risk management.

6. Evaluation of this prototype against the existing solutions, establishing that PRAM surpasses the characteristics of existing SME RA solutions, leading to the conclusion that such an approach is suitable for use by this type of organisations.

The importance of RA to SMEs and the concepts behind PRAM's architecture (such as the PP's, the necessity of included financial elements and the need for a more comprehensive output to the user) have been presented in a number of academic conference papers (listed in Appendix F). These concepts have received a number of positive comments from reviewers therefore it is believed that a significant contribution to the areas of I.T. security and RA have been made by this research.

8.2 Limitations of the research

This section analyses what limitations occurred during the research into, and the implementation of the prototype.

- As far as practical limitations are concerned this prototype was developed only for windows based systems which might not be a problem in most cases but would still deter a small number of organisations from adopting it.

- There has been insufficient data from existing surveys on SME characteristics in terms of specifically discussing SME I.S. practices and needs, surveys focus on large organizations. Most major and credible surveys do make a differentiation between large organisations and the overall sample of respondents which gives an idea of the SME side of the story. However, there is none dedicated to SME characteristics, needs and practices to provide with appropriate data for this investigation.

- Appropriate testing on organisations was not performed due to time constraints, selecting contacting and awaiting results from a number of appropriate organisations from each sector would significantly delay the completion of this research. Furthermore judging by the degree of participation from the MSc Students, who should have a somewhat large interest in the issue, in this evaluation it is likely that SMEs would be even harder to persuade to participate. Unfortunately the group of students was relatively small for such an evaluation, but the results were nonetheless indicative. Furthermore, since the functionality and outputs of PRAM were primarily evaluated in the scenario-based evaluation against the commercial RA tools, it has been shown practically in this thesis that the developed RA methodology surpasses the existing ones.

8.3 Suggestions and future work

In this section suggestions are made as to what future work should be done on PRAM to allow the conversion of this framework to a full-product which will effectively address the requirements of SMEs in the area of I.S. management and RA.

- A more detailed database and realistic figures on controls effect, intrusiveness and cost is required. For the first two perform a survey among a number of security educated individuals who can rate these elements and the average rating can be used in the prototypes database. To complement this database of controls, a further consideration of what controls may be overlapping or contradicting with

each other is necessary, so as to alter the PRAM software and avoid the selection of such controls being possible by the user.

- In a commercial version of PRAM, the association of "Threats" to "Applications" (and therefore assets) should continue to be automatic but it should also allow for "user interventions" (e.g. add a Threat). In this way peculiarities of the application environment (context) can be taken into account.

- Add the underlying assets under the applications in the Profiler engine and adapt the 'sub-threats' under threat profiles to these assets on the rest of the modules as described in Chapter 5.

- Further assistance to the user is required; PRAM includes a list of links to useful and selected websites on each of the controls. Nevertheless it would be useful to include details on the selected controls, assisting the user with appreciating, acquiring and implementing them, within the report. This sort of information would still be collected from external sources but it would save the user from making the effort to collect all this information from the recommended websites.

- Having performed these revisions to the prototype, perform a wider practical implementation and testing of the resulting prototype with SMEs participants to strengthen the general usability of the work. The evaluation subjects should include both organisations that have not implemented RA before to evaluate

PRAMs appropriateness as well as organisations that have performed one in the past so as to compare results.

- Another issue which was not addressed in the evaluation of PRAM due to time constraints and should therefore be considered in future work on this project is that the actual results (security measures) produced by the proposed methodology should be compared with the respective results of a conventional RA methodology as an supplementary way to assess their appropriateness.

- In the prototype was chosen for the user to have the capacity to select controls. However when PRAM is updated with more realistic figures on controls costs and effects, the option can be added that, if the user wishes, the system can suggest certain countermeasures for them. That could simply be based on the number of controls the organisation can approximately purchase according to the I.S. budget combined with the levels of threats. Therefore if the budget approximately allows for the purchase of 7 controls, two controls can be chosen for the two largest threats, then one control for each of the other threats. The user should then be able to add, remove or modify as desired. This would offer some further assistance to the user, however the selection of controls would simply be based on which controls come first on the list of controls for each threat according to their effect or intrusiveness (relevant to the users earlier selections) and would not overcome most problems related with traditional RA. The current approach was preffered for the prototype since human intelligence, when presented with the appropriate

information of threat scores, effect of controls on threat, ALE and budgeting issues, would produce more suitable selections of controls. These two approaches should be practically evaluated to establish which produces more suitable results but this would ideally involve implementing the suggested controls, by both the automated and the human – based approaches, within existing organisations and identifying which would produce the better results ie in time reduce threat occurrence. This process would require significant resources and time.

- Having performed the appropriate testing to ensure the PRAM prototype, with these additions, is suitable for the requirements of SMEs, transform it to an online application so as not to require any modifications or data stored on users' individual computers, provide with additional assistance and allow more proper updating of the tool and its databases. By having the tool online, it enables updating databases with new threats controls etc, leading to automatic re-assessment of the situation organisations are under and then notify the organisations that they are in need to re-assess their security as new threats occurred. Furthermore, by allowing users to come online and perform feedback will lead to database with more informed data on SMEs. Finally among the benefits of having it online is that it is not dependant on the characteristics, the O.S. and the software residing on the organisations computers.

8.4 The future of RA in the SME sector

As identified from the survey data in Chapter 2, SMEs constitute a very large percentage of the overall number of organisations worldwide; therefore they are also a major part of the economy and require sufficient and appropriate protection. RA is an essential part of organising and implementing effectual and cost-effective I.T. security. As this research established, SMEs are more in need of such practices than other organisations particularly as their majority does not employ any full-time I.S. security specialists to analyse risks, implement and manage security countermeasures. It is unlikely that organisations will stop facing I.S. threats, and therefore SMEs will always be in need of such a practice. However, as long as the solutions face the setbacks discussed in this thesis they will continue not to be adopted by SMEs. The methodology discussed in this thesis embraces those characteristics that an SME would require from such a solution. With the additions discussed in the 'future work' section, a fully operational RA solution can be produced which can be widely adopted by SMEs leading to improved 'full-time' security, with significant savings both from the selection of cost-effective controls as well as from thoroughly addressing the specific threats an organisation faces.

REFERENCES

1. ACCSS 2006, (2006), "Computer Crime and Security Survey", ISBN: 1-86499-849-0

2. Amatayakul M. (2003) "*Security Risk Analysis and Management: an Overview (AHIMA Practice Brief).*" Journal of AHIMA 74, no.9 October 2003 http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_021089.html, Accessed 10 September 2006

3. Allard J., (2003), "Risk Management For IT Auditors", ISACA, 20 September 2003. URL: http://www.isaca.be/Presentations/Risk_Management_For_IT_Auditors.pdf., Accessed 17 November 2006

4. Alred D., (2001), "Awareness, A Never Ending Struggle", SANS Security Essentials July 18, 2001 URL: http://www.sans.org/reading_room/whitepapers/awareness/391.php, Accessed 25-11-2006

5. Alberts C.J., Dorofee A. J., (2001),"OCTAVESM Criteria, Version 2.0", December 2001, http://www.cert.org/archive/pdf/01tr016.pdf

6. Arreola (2005), "Research Design, Measurement & Evaluation Supplementary Materials". URL: http://www.utmem.edu/~rarreola/researchdesign.html#guttmanscale, Accessed 10 September 2006

7. Baker and Mckenzie (2004), European Union: Security Legislation and Regulations, URL: http://www.bakernet.com/ecommerce/eu-s.htm, Accessed 23-11-2006

8. BBC. (2004) "Small firms fail security checks", BBC News Online, 30 March 2004, URL http://news.bbc.co.uk/2/hi/technology/3580105.stm, Accessed 5 August 2004.

9. Berinato S. (2005), The 2005 Global State of Information Security Survey, CIO magazine, URL: http://www.cio.com/archive/091505/global.html, Accessed 10 September 2006

10. Briere D., (2003), "Wireless Home Networking For Dummies" , Wiley & Sons inc pp184, ISBN 0-7645-3910-8

11. BSI (2006), "RA2, Art of Risk", URL: http://www.bsi-global.com/ICT/Security/bip0022.xalter, Accessed 24-11-2006

12. BSI (2002), "*Information security management systems — Specification with guidance for use*", British Standards Institution BS 17799:2002. 5 February 2002, ISBN: 0 580 40250 9

13. Buchanan W., (1999) "Mastering Networks", Macmillan Press LTD, ISBN 0-333-74804-2 pp352-374

14. Burke T., (2003), "U.S. Government IT Security Laws: A Guide to IT Security Legislation and Contractor Responsibilities", September 2003, URL: http://www.sans.org/reading_room/whitepapers/legal/1306.php, Accessed 23-11-2006

15. Buszta K., (2003)., "Security Management", CRC Press Information Security Management Handbook, pp 1080 - 1099 ISBN: 0-8493-1997-8

16. Camp L. J., (2006) "The State of Economics of Information Security", Information Security journal, Volume 2 Issue 2 URL: http://www.is-journal.org/V02I02/2ISJLP189-Camp.pdf., Accessed 23-11-2006

17. Chong C. K. (2003) *Managing Information Security for SMEs. May 2003*, Information Technology Standards Committee, URL www.itsc.org.sg/standards_news/2002-05/kinchong-security.ppt, Accessed 10 July 2006.

18. Churchill C.N., Lewis L. V., (2006) "The five stages of small business growth", Harvard Business review, 28 October 2006

19. Cisco (2006), "Designing Network Security", Cisco Press URL: http://www.ciscopress.com/content/images/1587051176/samplechapter/1587051176content.pdf , Accessed 24-11-2006 p241

20. Cisco Systems. (2001) *The Return on Investment for Network Security*, URL: http://www.cisco.com/warp/public/cc/so/neso/sqso/roi4_wp.pdf, Accessed 17 November 2006

21. Commoncriteria (1999), "Common Criteria for Information Technology Security Evaluation User Guide" URL: http://www.commoncriteriaportal.org/public/files/ccusersguide.pdf, Accessed 17 November 2006

22. Corby M., (2003), "Considerations for Outsourcing Security", CRC Press Information Security Management Handbook, pp 1595 ISBN: 0-8493-1997-8

23. CRAMM (2006), "*The History of CRAMM*", Insight Consulting 2006, URL: www.cramm.com/overview/history.htm, Accessed 20 July 2006.

24. CRAMM b (2006), "Overview: How it works", Insight Consulting 2006, URL: http://www.cramm.com/overview/howitworks.htm, Accessed 17 November 2006

25. Deloitte, (2005), 'The 2005 Global Security Survey', 2005 Global Security Survey URL:

http://www.deloitte.com/dtt/cda/doc/content/dtt_financialservices_2005GlobalSecurit ySurvey_2005-07-21.pdf Accessed 5-9-2006

26. Diamond B., (2004), Why Small Businesses Need to Secure Their Computers (and How to Do it!), URL: http://www.securitydocs.com/library/2106, Accessed 25-11-2006

27. Dimopoulos V. Furnell S.M. Jennex M. Kritharas I., (2004a), "Approaches to I.T. Security in Small and Medium Enterprises", , Proceedings of the 2nd Australian Information Security Management Conference 2004, Perth, Australia, 26 November 2004, pp73-82, 2004

28. Dimopoulos V. Furnell S.M. Barlow I. Lines B.L., (2004b), *"Factors affecting the adoption of IT risk analysis"*, The 3rd European Conference on Information Warfare and Security Royal Holloway, University of London, UK, 28-29 June 2004

29. Dimopoulos V. Furnell S.M. Barlow I. Lines B.L., (2004c), "Using protection profiles to simplify risk management", The Security Conference, April 14/15, Las Vegas, USA, 2004

30. DTI 2006, (2006) *"Information Security Breaches Survey 2006"*, Department of Trade and Industry, April 2006, http://www.security-survey.gov.uk/

31. DTI 2005 (2005), Information security: Protecting Your Business Assets

32. Endorf F. C., (2003), "Measuring ROI on security", CRC Press Information Security Management Handbook, pp 1056 - 1059 ISBN: 0-8493-1997-8

33. Ernst & Young,(2005),'Global Information Survey 2005, Report on the widening gap', www.ey.com

34. European Commission (2005), "The new SME definition, User guide and model declaration" , URL: http://ec.europa.eu/enterprise/enterprise_policy/sme_definition/sme_user_guide.pdf, Accessed 9 September 2006

35. European Commission (2007), "Enterprise and Industry, SME Definition", March 2007, URL: http://ec.europa.eu/enterprise/enterprise_policy/sme_definition/index_en.htm, Accessed 14 April 2007

36. FDIC, Federal Deposit Insurance Corporation, (1999), " Risk Assessment Tools and Practices for Information System Security", URL: http://www.fdic.gov/news/news/financial/1999/ FIL9968a.HTML Accessed 3-9-2006

37. Federal Aviation Administration. (2001) *Executing The Risk Management Process*, Nasdocs, URL http://nasdocs.faa.gov/nasiHTML/risk-mgmt/vol1/5_chapt.html, Accessed 9 July 2003.

38. GAO, United States General Accounting Office, (1999),"Information Security Risk Assessment Practices of Leading Organizations", August 1999, http://www.gao.gov/special.pubs/ai99139.pdf Accessed 3-9-2006

39. GAO (1999), "Information Security Risk Assessment Practices of Leading Organizations", United States General Accounting Office

40. GAO (2001), "Management Planning Guide for Information Systems Security Auditing", 10 December 2001, URL: http://www.gao.gov/special.pubs/mgmtpln.pdf, Accessed 15 December 2006

41. Garfinkel S., (1997), "Web Security & Commerce", O'Reilly, June 1997, ISBN: 1-56592-269-7

42. Garrett C., (2004), "Developing a Security-Awareness Culture –Improving Security Decision Making", SANS Institute, 23 July 2004, URL: http://www.sans.org/reading_room/whitepapers/awareness/1526.php, Accessed 21-11-2006

43. Gordon A. L., Loeb P. M., Lucyshyn W. and Richardson R., (2006), CSI/FBI *Computer Crime and Security Survey*. Computer Security Institute, URL http://www.gocsi.com, Accessed 26 July 2006

44. Granger S., (2001), "Social Engineering Fundamentals, Part I: Hacker Tactics", Security Focus, 18 December 2001, http://www.securityfocus.com/infocus/1527, Accessed 28-11-2006

45. Gray B., (2005) "The Role of the Security Analyst in the Systems Development Life Cycle", SANS Institute, 12 January 2005, URL: http://www.sans.org/reading_room/whitepapers/awareness/1601.php, Accessed 26-11-2006

46. GSSL, (1997) *A Practitioner's View of CRAMM,* Gamma Secure Systems Limited, URL http://www.gammassl.co.uk/topics/hot5.html

47. C.S.E., (1996), "A Guide to Security Risk Management for Information Technology Systems", Communications Security Establishment, January 1996, URL: http://www.cse-cst.gc.ca/documents/publications/gov-pubs/itsg/mg2.pdf

48. Hamilton C., (2003), *"The Integration of Information and Physical Security as an Element of Homeland Security"*, Computer Security Journal, March 2003

49. Hamilton C., (2002) *"Risk Management and Security"*, RiskWatch, Inc., July 2002 URL: http://www.riskwatch.com/Whitepapers/Risk_Management_and_Security_11-07-02.pdf, Accessed 15 May 2006

50. Hall J., (2003), "Selling Security To Management", SANS Institute, 31 October 2003, URL: http://www.sans.org/reading_room/whitepapers/awareness/393.php, Accessed 25-11-2006

51. HKCERT (2005), "Information security guide for small business" URL: https://www.hkcert.org/secguide/eng/sme_guideline_e.pdf, Accessed 24-7-2006

52. Hoo S. J. K., (2000) *How Much Is Enough? A Risk-Management Approach to Computer Security,* June 2000, Consortium for Research on Information Security and Policy, http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/06.doc, Accessed 14 March 2006.

53. INFORM (2005), *"The Symantec Information Assurrance Risk Model"*, URL: https://www.informplan.com/inform, Accessed 16 November 2006

54. INTOSAI EDP Committee (1997), "I.T. audit training I.T. Security Student Notes", October 1997, www.intosaiitaudit.org

55. ISACA (2000), "COBIT 3rd Edition Control Objectives", July 2000, www.isaca.org ISBN: 1-893209-17-2

56. ISO (2006), "ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management", International Organization for Standardization, 7 October 2006, URL: http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html, Accessed 12 April 2007

57. ISO17799 (2005), British Standards Institution. '*Information technology. Code of practice for information security management*. BS I.S.O/IEC 17799:2005. 16 June 2005. ISBN 0 580 46262 5.

58. ISO 27001 (2005), British Standards Institution. *'Information technology — Security techniques — Information security management systems — Requirements'*, BS ISO/IEC 27001:2005, 18 October 2005, ISBN 0 580 46781 3

59. ISO Standards Bookshop (2002), "What is a Standard?", URL: http://www.iso-standards-international.com/what.htm

60. Jennex, M.E. and Addo T. (2004) "SMEs and Knowledge Requirements for Operating Hacker and Security Tools". *IRMA 2004 Conference*, New Orleans, Louisiana, 23-26 May 2004, URL: http://www.irma-international.org/conferences/2004/, Accessed 25-11-2006

61. Labuschagne L., (1999), *Risk Analysis Generations - The evolution of Risk*, August 1999, http://csweb.rau.ac.za/staff/labuschagne/research/articles/ra_generations.pdf, Accessed 30 July 2003

62. Labuschagne L., Eloff J.H..P., (2000), "Electronic commerce: The information-security challenge"

63. Langue C., Furnell S.M. Dowland P.S., (2005), "Approaches to Establishing IT Security Culture", Advances in Network and Communications Engineering 2 ISBN 1-84102-140-7, pp 46

64. Lawlor B., Vu L., (2003), "A Survey of Techniques for Security Architecture Analysis", Information Networks Division Information Sciences Laboratory, May 2003

65. Lloyd I. (2002) *Step by step to safety. September 2002*, British Computer Society Computer Bulletin, p18, URL http://www.bcs.org.uk/publicat/ebull/sept02/step.htm, Accessed 30 July 2003.

66. May M., (2004), "Federal Computer Crime Laws", URL: http://www.sans.org/reading_room/whitepapers/legal/1446.php, Accessed 23-10-2006

67. McAfee (2006), *"McAfee Proven Security Planner for Small Business"*, URL: http://www.mcafee.com/us/provensecurityplanner, Accessed 16 November 2006

68. Meritt W. J., (1998) "Risk Management", Proceedings of the 1998 National Information Systems Security Conference (NISSC), URL: http://csrc.nist.gov/nissc/1998/proceedings/paperE5.pdf, Accessed 16 December 2006

69. Microsoft (2006), "Safeguard Your Business in 7 Steps" URL: http://www.microsoft.com/smallbusiness/support/computer-security.mspx, Accessed 15 November 2006

70. Morgan Research, (2001) "Privacy and Business", Office of the Federal Privacy Commissioner, 31 July 2001, URL: http://www.privacy.gov.au/publications/rbusiness.html, Accessed 28-11-2006

71. Munley M., (2004), "Moving from Consciousness to Culture: Creating an Environment of Security Awareness", SANS Institute, 10 April 2004, http://www.sans.org/reading_room/whitepapers/awareness/1439.php, Accessed 25-11-2006

72. Muller J. N., (2003), "Network Manager's Handbook", McGraw-Hill, ISBN:0071405674, pp 503-527

73. Nanavati S., (2002), "Biometrics, identity verification in a networked world", John Wiley & Sons inc, ISBN 0471-09945-7 pp 15-20

74. National Institute of Standards and Technology (1995), "An Introduction to Computer Security:The N.I.S.T. Handbook, Special Publication 800-12", October 1995 http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

75. Network Working Group (1997) *Site Security Handbook.* RFC 2196, September 1997, URL: http://www.faqs.org/rfcs/rfc2196.html, Accessed 19 December 2006

76. Noakes K., (2003) Risk Analysis Software: Perspective, Gartner, Inc., February 2003 www.njcu.edu/assoc/njcuitma/documents/addendums/Risk_Analysis_Software_2.4.03.pdf, Accessed 17 November 2006

77. O'Connor T., (2004), "Scales and Indexes", June 2004, URL: http://faculty.ncwc.edu/toconnor/308/308lect05.htm, Accessed 17 September 2006

78. Paraskevas A. Buhalis D. (2002) *Hosted application provision for small and medium sized Tourism Enterprises*, Paper presented at ENTER2002 Conference, Innsbruck Austria, URL: http://www.eyefortravel.com/ papers/ASpsSMTEs.pdf, Accessed 12 July 2003.

79. Parker D. B., (1998) *"Fighting Computer Crime: A New Framework for Protecting Information"*, John Wiley & Sons, p. 240.

80. Pfleeger P. C., (2006), "Security in Computing, Fourth Edition" , Prentice Hall, ISBN: 0-13-239077-9

81. Robins G. (2001) *E-government, Information Warfare and Risks Management: an Australia Case Study*, Paper presented at the Second Australian Information Warfare and Security Conference 2001, URL: http://wwwbusiness.ecu.edu.au/profile/schools/mis/media/pdf/0029.pdf, Accessed 14 July 2003.

82. Schneier B., (2000), "Secret and Lies: Digital Security in a Networked World", Wiley Computer Publishing, 2000. ISBN: 0-4714538-03

83. Shaurette M., (2003), "The Building Blocks of Information Security", CRC Press Information Security Management Handbook, pp 1080 - 1099 ISBN: 0-8493-1997-8

84. Spinellis D. Kokolakis S. Gritzalis S., (1999) *Security Requirements, Risks, and Recommendations for Small Enterprise and Home-office Environments"*, URL: http://www.dmst.aueb.gr/dds/pubs/jrnl/1999-IMCS-Soft-Risk/html/soho.html, Accessed 5 July 2003.

85. Stoneburner G., Goguem A., Feringai A., (2002) "N.I.S.T. Special Publication 800-30: Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology", National Institute of Standards and Technology, July 2002, URL:

http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, Accessed 10 September 2006

86. Sustaita D., (2001), "Security Awareness Training Quiz - Finding the WEAKEST link!", SANS Institute, 13 August 2001. http://www.sans.org/reading_room/whitepapers/awareness/396.php, Accessed 25 November 2006

87. Symantec, (2006), Symantec Internet Security Threat Report, March 2006, www.symantec.com

88. Tanenbaum A., (1988) "Computer Networks second edition", Prentice-Hall, ISBN: 0-13-162959-X, page 254

89. Thompson K. L., Solms v. R., (2003), "Integrating Information Security into corporate governance", Proceedings of the IFIP TC11 18thh International Conference on Information Security, Kluwer Academic Publishers, pp169 – 179, ISBN 1-4020-7449-2

90. Tipton H. F., (2003) "Types of Information Security Controls", CRC Press Information Security Management Handbook, pp 120 - 125 ISBN: 0-8493-1997-8

91. Trochim W. (2006),"Guttman Scaling", Web Center for Social Research Methods URL: http://www.socialresearchmethods.net/kb/scalgutt.htm, Accessed 12 April 2007

92. Upfold et al. (2005), " An investigation of information security in small and medium enterprises in the eastern cape" , URL: http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/082_Article.pdf, Accessed 24-11-2006

93. Yazar Z., (2002), "A qualitative risk analysis and management tool – CRAMM", SANS institute

94. Wallhoff J., (2002), "*Security Management Practices*", The CISSP and SSCP free study portal, April 2002 http://www.cccure.org/Documents/CISSP_Summary_2002/page57.html

95. Whitman M., Mattord H., (2003), "Principles of Information Security, 1st Edition", Thomson Learning, Course Technology, Boston, Massachusetts. ISBN: 0-6190-6318-1, pp15

Appendix A: Test Scenarios

About the scenarios

Three different organization profiles chosen, wanted to cover, firstly all cases (sizes) of SMEs. The second criterion was to deal with diverse organizational requirements. Firstly the industry sectors and secondly the physical environments are appropriately diverse. Secondly the focus of the organization from a security perspective is diverse. The first is primarily concerned with accidental loss of data on the computers, the second with modification of data and downtime of hosted applications and the third with confidentiality of customer data and physical theft of equipment.

Scenario 1: Home office

My Home Office: Software Programming & website development

Sector:	IT
Organization Size:	2 (1 Programmer, 1 Admin)
IT Size:	1 Pc, I Laptop, 1 print server
Applications:	Office, programming, IM, Video, image, audio processing
Internet Connection:	DSL
IT Budget (per year):	2000
Organization Budget (per year):	15000 (3 projects of 5000 profit per year)
Networking	LAN, Wireless LAN
Who created the IT infrastructure?	Organisation owner

Security Requirements

The organization considers itself low risk

Consists of a single room home office including wireless LAN and 2 computers both connected to the internet.

2 people personnel with full access to all data, access to anyone else is highly controlled since it is a home.

Main security concerns:

The organization is mainly concerned for availability and integrity of backed-up material and information within computers not as much for website, print servers etc. second main concern is availability of email and applications within computers.

Delays in project completion etc due to loss of availability, loss of prototype software etc either accidental or theft.

Loss of customer confidence, since small organization cannot afford this

Scenario 2: Small organization

The Network Research Group

Education on the area of networking

Due to specialty on the sector occasionally handles web hosting other small commercial projects on the area.

Sector:	Education
Organization Size:	20 (14 researchers, 6 Admin)
IT Size:	20 Pc, 4 Laptop, mail server, web server, backup server,4 pdas
Applications:	Office, programming, IM, Video, image, audio processing, database applications, web browsing
Internet Connection:	DSL
IT Budget (per year):	7000
Organization Budget (per year):	30000 (through university, conferences, independent projects)
Networking	LAN, Wireless LAN
Website	With personal information (staff login and contact details)
Who created the IT infrastructure?	Organisation staff

Security Requirements
Small office consisting of 3-4 rooms with somewhat controlled access, within a large open area with students and staff roaming around.

Accessible to cleaning and security personnel who are employed by the building (ie for many offices) not specifically by the office.

Can have explicit security to the organization areas etc however is preferable not to have it limit legitimate user access.

Since the organization is concerned with IT and security reputation is very important and also it is highly targeted, however on the pluses, staff is quite security aware.

Main concerns:
Breach of confidentiality of commercial projects and hosted websites can lead to damaged reputation which the organization is concerned about.

Loss of availability of research data, a small concern for theft, mainly accidental loss however would have great impact on work progress cause delays misses of project submissions etc

Integrity of Student data is of medium importance and a bit likely to be targeted by disenchanted students.

Scenario 3: Medium organization

Medium- sized Medical Center

Sector:	Healthcare
Organization Size:	60
IT Size:	60Pc,10laptops, 10 pdas
Applications:	Office, web, databases
Internet Connection:	DSL
IT Budget (per year):	15000
Organization Budget (per year):	500000 (through services to patients)
Networking	LAN
Website	Transactional (Displays information only)
Who created the IT infrastructure?	External Provider

Security Requirements

Organization spans over a small building with about 30 rooms, access to the building is fairly controlled. However patients/emergencies can be overlooked there is high degree of people in and out.

The organization does not consider themselves to eb at a great IT security risk, however unlikely, any breach could have dear consequences since customer (patient) records is highly confidential and protected by a number of legislations. It is highly confidential information

It is however imperative that this information is highly available at any time especially to key hospital staff.

Even though information is highly confidential, security cannot be 'intrusive' since authorized people require easy access both to the building as well as the information and because of high numbers of customers in and out.

Main concerns:

Availability of information at any time is crucial

Breach of confidentiality could cause high fines i.e. financial losses

Breach of Integrity may prove crucial patient records should never be unauthorized tempered with

Theft of expensive equipment

After the assessment

Since SMEs need support and proper management of risks instead of simple controls selection, after the assessment there needs to be a check on how the tools evaluate the selected controls effectiveness and appropriateness.

Appendix B: SME Security Survey

US IT Security Survey

Mark the title that describes your job function: □ Owner/CEO/President □ Manager □ IT Specialist □ other:_____

Is your company connected to the Internet? □ Yes □ No

What operating systems do you use? (mark all that apply)
□ Novell Netware □ Microsoft Windows □ Linux □ Unix □ Macintosh □ Other:_____ □ Don't know

How many people does your organization employ? □ 0-4 □ 5-20 □ 21-250 □ 251-500 □ 500+

Choose the industry that best describes your organization (choose only one): □ Accounting □ Computers/IS/IT □ Professional
□ Construction/Real Estate □ Education □ Entertainment □ Financial □ Healthcare □ Marketing
□ Manufacturing □ Food Service □ Retail □ Telecommunications
□ Misc Services □ Wholesaler □ Non-profit

Does your company have a documented security plan or policy? □Yes □No □ Don't know

Is there a specific person responsible for security at your organization? □ Yes □ No □ Don't know

Is the company's security plan reviewed, modified, or updated at least once a year?
□ Yes □ No □ Don't know

Are employees trained on the security plan? □ Yes □ No □ Don't know

Are there consequences for not following the security plan and are employees trained on them? □ Yes □ No □ Don't know

Has an inventory of assets been conducted (data, confidential info, servers, anything that needs protection)? □ Yes □ No □ Don't know

Has a threat analysis been conducted to identify internal or external threats to company assets? □ Yes □ No □ Don't know

How often is data backup done (check all that apply)? □ Daily □ Weekly
□ Monthly □ Don't know

Are data backups stored at a location other than company premises? □ Yes □ No
□ Don't know

Are backups tested periodically to ensure operability (i.e. test restoring files)? □ Yes
□ No □ Don't know

Are user accounts deleted/disabled immediately following an employee resignation/termination? □ Yes □ No □ Don't know

Please indicate if the following activities are implemented:

Security Item	Implemented?
Physical security (i.e. access badges, keys to secure areas or server rooms)	□ Yes □ No □ Don't know
Firewalls (software or hardware) are installed on all external network connections	□ Yes □ No □ Don't know
Intrusion Detection System or other forms of network level protection	□ Yes □ No □ Don't know
Anti-Virus software for servers and workstations installed and periodically updated	□ Yes □ No □ Don't know
Operating System Patches and Updates are checked and installed periodically	□ Yes □ No □ Don't know
Password Policies requiring minimum lengths and periodic changes are in place and enforced	□ Yes □ No □ Don't know
Network user accounts to control access to network resources	□ Yes □ No □ Don't know
Uninterruptible Power Supplies for critical IT equipment are installed and tested	□ Yes □ No □ Don't know
Wireless security (ex: WEP) is in place* *□ Mark here if no wireless technology used	□ Yes □ No □ Don't know
Disaster recovery plan in place and tested	□ Yes □ No □ Don't know

Please indicate the degree to which you agree with the following statements

Item	Agree	Somewhat Agree	Neither Agree/Disagree	Somewhat Disagree	Disagree
I am comfortable our security plan protects our critical data					
We have adequate knowledge about IS security					
I am confident my company won't have a IS security problem					
We rely on one or two key people to manage our IS security					
Our security rules are a burden to follow					
I stay awake nights worrying about my company's data and networks (I worry a great deal about our security)					

Any additional comments you wish to make:

European IT Risk Analysis survey

Section 1: General

1. **Please indicate the size of your organization:**
   - ☐ 1-4 employees
   - ☐ 5-20 employees
   - ☐ 21-250 employees
   - ☐ 251-500 employees
   - ☐ 500+ employees

2. **Mark the title that describes your job function:**
   - ☐ Owner/CEO/President
   - ☐ Manager

☐ IT Specialist

☐ Other (Please specify):

3. Choose the industry that best describes your organization:

☐ Accounting
☐ Computers/IS/IT
☐ Professional
☐ Construction/Real Estate
☐ Education
☐ Manufacturing
☐ Non-profit
☐ Misc Services
☐ Other (Please specify):

☐ Entertainment
☐ Financial
☐ Healthcare
☐ Marketing
☐ Retail
☐ Telecommunications
☐ Food Service
☐ Wholesaler

4. Is your company connected to the Internet?

☐ Yes ☐ No

If yes, what type is your Internet connection?

☐ 56kbps ☐ DSL
☐ ISDN ☐ Cable modem
☐ Other (Please specify):

5. Please indicate the dependence of your company on the information technology systems:

☐ Not at all dependant
☐ Somewhat dependant
☐ Totally dependant

6. What operating systems do you use? (Mark all that apply)

☐ Microsoft Windows 9x, Me
☐ Microsoft Windows NT, 2000, XP
☐ Linux

☐ UNIX

☐ Macintosh

☐ Novell Netware

☐ Don't know

☐ Other (Please specify):

7. How many Information Technology (IT) administrators does your company employ?

☐ None

☐ 1

☐ 2

☐ 3+

8. Who is responsible for the IT security at your company?

☐ IT administrator

☐ Security officer

☐ Other (Please specify):

Does this person have any formal IT security qualifications?

☐ Yes ☐ No

9. Does your organisation have a dedicated IT security budget that is separate from the overall IT budget?

☐ Yes ☐ No

Section 2: Security

10. Does your company have a documented security plan or policy?

☐ Yes ☐ No ☐ Don't know

11. How are the members of staff made aware of the contents of the IT security plan? ***(only relevant if your answer to Question 10 was "Yes")***

- ☐ Via a staff handbook
- ☐ Specific document distributed to staff
- ☐ Contract or letter of employment
- ☐ On joining or during induction
- ☐ Through ongoing training
- ☐ Employees are not made aware of any security plan
- ☐ Other (Please specify):

12. Please indicate if the following activities are implemented:

Security Item	**Implemented?**
Physical security (i.e. access badges, keys to secure areas or server rooms)	☐Yes ☐No ☐Don't know
Firewalls (software or hardware) are installed on all external network connections	☐Yes ☐No ☐Don't know
Intrusion Detection System or other forms of network level protection	☐Yes ☐No ☐Don't know
Anti-Virus software for servers and workstations installed and periodically updated	☐Yes ☐No ☐Don't know
Operating System Patches and Updates are checked and installed periodically	☐Yes ☐No ☐Don't know
Password Policies requiring minimum lengths and periodic changes are in place and enforced	☐Yes ☐No ☐Don't know
Network user accounts to control access to network resources	☐Yes ☐No ☐Don't know
Uninterruptible Power Supplies for critical IT equipment are installed and tested	☐Yes ☐No ☐Don't know
Wireless security (ex: WEP) is in place* *☐ Mark here if no wireless technology used	☐Yes ☐No ☐Don't know
Disaster recovery plan in place and tested	☐Yes ☐No ☐Don't know

13. How confident are you of your security?

- ☐ Not at all
- ☐ A bit worried
- ☐ Confident
- ☐ Extremely Confident

Section 3: Risk Analysis

14. Has an inventory of assets been conducted (data, confidential info, servers, anything that needs protection)?

- ☐ Yes
- ☐ No
- ☐ Don't know

15. Has a threat analysis been conducted to identify internal or external threats to company assets?

- ☐ Yes
- ☐ Internal threats only
- ☐ External threats only
- ☐ No
- ☐ Don't know

16. Does your organization perform IT risk management? (i.e. identifying assets - threats and subsequently securing them).

☐ Yes ☐ No

If yes, how often?

- ☐ Once a year
- ☐ Once every 2-3 years
- ☐ Other (Please specify):

17. If you carry out IT risk analysis, is it provided in-house or by a third-party?

☐ In-house ☐ Third-party

18. If you conduct in-house risk analysis, who is responsible for this task?

19. Do you use any risk analysis software tool?

☐ Yes ☐ No

If not, do you use any other method like BS7799/ISO 17799 to secure company assets?

20. In case you do not perform IT risk analysis, please state the reasons why not.

- ☐ Lack of budget
- ☐ Lack of expertise
- ☐ Lack of awareness
- ☐ Disruption
- ☐ Other (Please specify):

21. If you had the option, what would you upgrade as far as your organization's IT security is concerned? (please select only 1)

- ☐ Security Administrator
- ☐ Risk Analysis
- ☐ More Security technologies / countermeasures
- ☐ Employ security training / awareness

22. If you were convinced that risk analysis is a necessary procedure in order to successfully secure your organisation's network, how much would you be prepared to spend on appropriate tools to assist the task?

- ☐ £0 – £100
- ☐ £101 - £1000
- ☐ £1001 - £3000
- ☐ More than £3000

23. Please use this space to provide us with any additional comments you may have:

Appendix C: PRAM evaluation lab

Section 1: The Lab

You have been handed a CD containing 4 RA tools, 3 commercial and 1 under development

In this lab you are required to perform the following steps:

1. Devise a scenario of a small or medium sized organization you are supposedly managing.
2. Select one of the three commercial RA tools and perform a RA on your organization, then do the same for PRAM, the RA tool under development
3. Answer the questionnaire provided therefore evaluate the suitability of the tools for SMEs

For any questions during the progress of this lab please ask the lab supervisors

Step 1: Devise a scenario

Place yourself in the position of a manager or someone significantly involved in the operation of a SME. Ideally, select an organization that you have worked for in the past and you know its purpose, functions and IS requirements.

Write the scenario down; describe the organization and its IT assets as well as the security requirements, in a way similar to the example scenario in Appendix 1. Please use the space provided to you in Appendix 1 to write down your scenario.

If you are unsure, and only then, you may use the scenario provided to you in the Appendix.

Step 2: Perform the RA

Bearing in mind that you are in a position within your organization where the task of analyzing the IT security risks faced, selecting the appropriate controls and implementing them to safeguard your IT assets is a task which falls to you and only.

Select one of the commercial RA tools provided that you wish to use, that may be either the Buddy System, Cobra or MRSAT. Then install it on your system, run it and perform an assessment based on the scenario you devised in section 1.

During the process of the RA keep notes (using the sheet provided to you in Appendix 2) of elements you find positive in this approach to RA and other elements that you consider negative and which might deter you from using such a tool.

After you complete the assessment and before proceeding to use the PRAM prototype, make sure you have a good look at the results provided to you at the end by the tool you have selected and used. Install the prototype version of PRAM on your system, then use it to perform an RA on the same scenario you used previously. Again you are encouraged to use the sheet provided to you in Appendix 2

When using PRAM keep in mind that it is a prototype and not a fully operational commercially available product like the previous you used. Therefore PRAM's database is not as complete as that of the previous.

However, the purpose of this lab is for you to consider the usability, functionality and effectiveness of the two approaches you have used and which one would be more suitable for use by an SME manager or user with no IT security expertise, and maybe no significant IT knowledge at all. Therefore what you are required to consider here is which process is more suitable for this user:

- Easier to use
- Faster
- Provides more assistance in understanding what controls are more appropriate for your organization and why
- Assists with the selection of controls
- Assists with the implementation of these controls
- Provides support to the user in responding to events and re-evaluating effectiveness of the implemented security

Important: Feedback

Some period of time after the initial RA, you decide to upgrade your organizations IT, you therefore add some applications, remove some others and you also need to address a threat that keeps occurring even with the controls you have implemented. You need to:

- For the RA tool you have used consider how this update can be reported and addressed

- Consider what functionality your RA tool provides in re-assessing the selected controls that are judged to be insufficient since this threat keeps occurring.

Step 3: Complete the evaluation questionnaire provided to you

Answer the questionnaire provided to you on the following section.

Thank you for your participation in this evaluation

Section 2: Evaluation Questionnaire

Part 1: User Information

1. Please state your age:

2. Have you been employed by an organization before?

☐ Yes
☐ No

Was your position (Please tick as appropriate):

☐ IT related?
☐ Management/Owner
☐ Other

3. Do you have practical Information security experience?

4. Have you used RA tools before? If yes, please state which.

Part 2: The Risk Assessment Tools

Use of tool

5. Which of the commercial RA tools have you chosen to use?

6. Which was easier to use by a non-trained (in RA) user?

☐ PRAM
☐ Other

7. Which had the most 'user friendly' interface?

☐ PRAM
☐ Other

8. Which approach did you prefer - profiling or the other you used (questionnaire)?

☐ Profiling of assets (PRAM)
☐ Questionnaire-based

Why?

9. Which approach provided more assistance in judging which controls are more appropriate for your organization and what controls you should select if you could not afford all of them?

☐ PRAM
☐ Other

10. Did you find the ALE and ROI financial considerations important to be included in a RA tool?

☐ Yes
☐ No

Output

11. Which provided with the most useful output to the user?

☐ PRAM
☐ Other

12. Which gave the most helpful information on how controls should be implemented?

☐ PRAM
☐ Other

13. Which output would be more useful to illustrate the threat and justify security-related expenditure to the management?

☐ PRAM
☐ Other

Feedback

14. What do you think of the provision of feedback and assistance after the end of the RA?

☐ Unnecessary
☐ Useful
☐ Imperative

Final thoughts

15. Overall which tool did you find more appropriate and helpful for use by an SME, i.e. an organization with limited budget to deploy countermeasures and limited IT security expertise within?

☐ PRAM
☐ Other

16. Which of the tools you evaluated would you actually use in a real life situation?

☐ PRAM
☐ Other

Why? (State below):

17. If you were managing your organization would you use such a tool to identify threats and select controls?

☐ Yes
☐ No

Which? (State below):

18. What would potentially deter you from adopting such a tool?

☐ Ease of use
☐ Time it takes to perform
☐ Other (State which):

APPENDIX 1: EXAMPLE SCENARIO

Medium-sized organization

Medium- sized Medical Center

Sector:	Healthcare
Organization Size:	60
IT Size:	60Pc,10laptops, 10 pdas
Applications:	Office, web, databases
Internet Connection:	DSL
IT Budget (per year):	15000
Organization Budget (per year):	500000 (through services to patients)
Networking	LAN
Website	Transactional (Displays information only)

Security Requirements

Organization spans over a small building with about 30 rooms, access to the building is fairly controlled. However patients/emergencies can be overlooked there is high degree of people in and out.

The organization does not consider themselves to eb at a great IT security risk, however unlikely, any breach could have dear consequences since customer (patient) records is highly confidential and protected by a number of legislations. It is highly confidential information

It is however imperative that this information is highly available at any time especially to key hospital staff.

Even though information is highly confidential, security cannot be 'intrusive' since authorized people require easy access both to the building as well as the information and because of high numbers of customers in and out.

Main concerns:

Availability of information at any time is crucial

Breach of confidentiality could cause high fines i.e. financial losses

Breach of Integrity may prove crucial patient records should never be unauthorized tempered with

Theft of expensive equipment

YOUR TEST SCENARIO:

(Please use the space bellow to write down the scenario you will be using)

APPENDIX 2: YOUR VIEW OF THE RA TOOLS YOU USED

Commercial RA tool used (Please state which bellow):

- Advantages

- Disadvantages

- Comments

PRAM RA prototype:

- Advantages

- Disadvantages

- Comments

Appendix D: Participants Quotations from their responses to the lab questions (Complete List)

MRSAT

- **Advantages**
  "Comprehensive report"
  "Help service provided explaining terms"
  "Fairly all-encompassing"
  "Graphical output"
  "More suited for business in terms of paperwork"

- **Disadvantages**
  "Too many questions been asked"
  "No progress bar showing the process status"
  "Laborious and heavy to use"
  "Would confuse those without a clear picture of their environment"
  "Too many confusing questions"
  "Requires in depth technical knowledge to be able to answer most of the questions"
  "Report was vague and almost useless"

Cobra

- **Advantages**
  "Provides the option to the user to set the level of security"
  "Easy to use"
  "Can provide parts of the report"

- **Disadvantages**
  "Not enough information/help given"
  "Does not mention cost/expenditure to deploy the controls"
  "It is difficult to understand what could be achieved by the tool"
  "Takes long time to complete the questions"
  "Report presentation (Graph) is not quoted with captions properly"
  "Advise too short, no links to get further information"

Buddy System

- **Advantages**
  "Lots of Information"

- **Disadvantages**
  "All the threats are not mentioned"
  "Too complicated"
  "Ugly design"

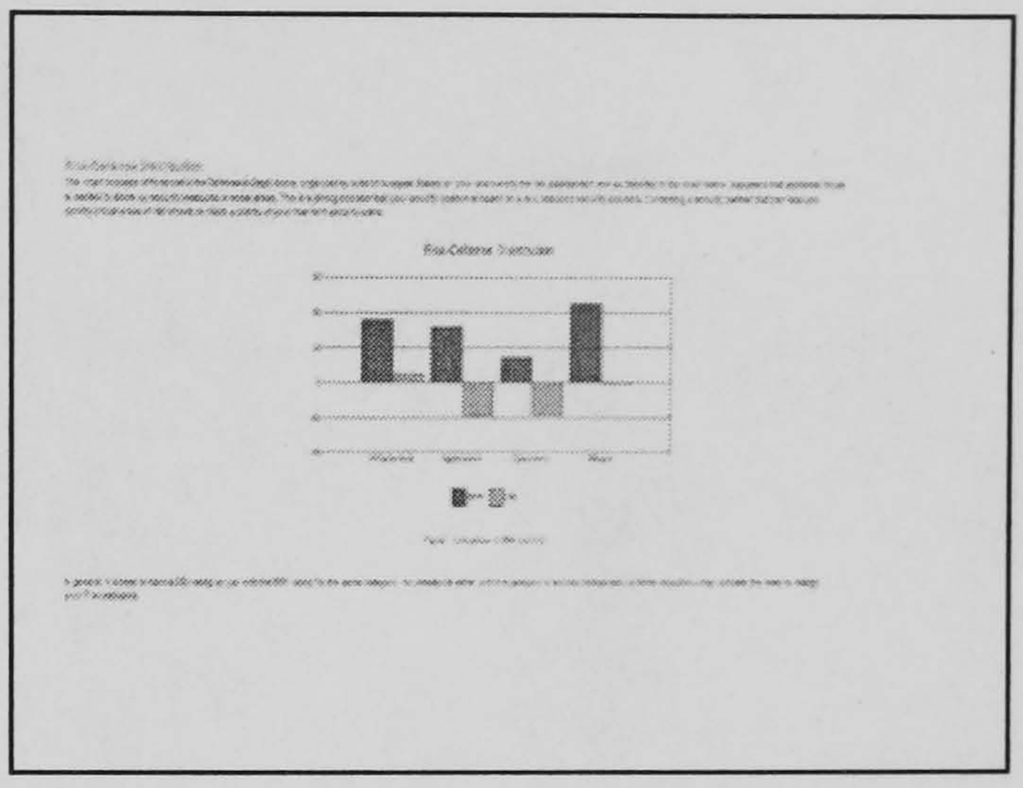
PRAM

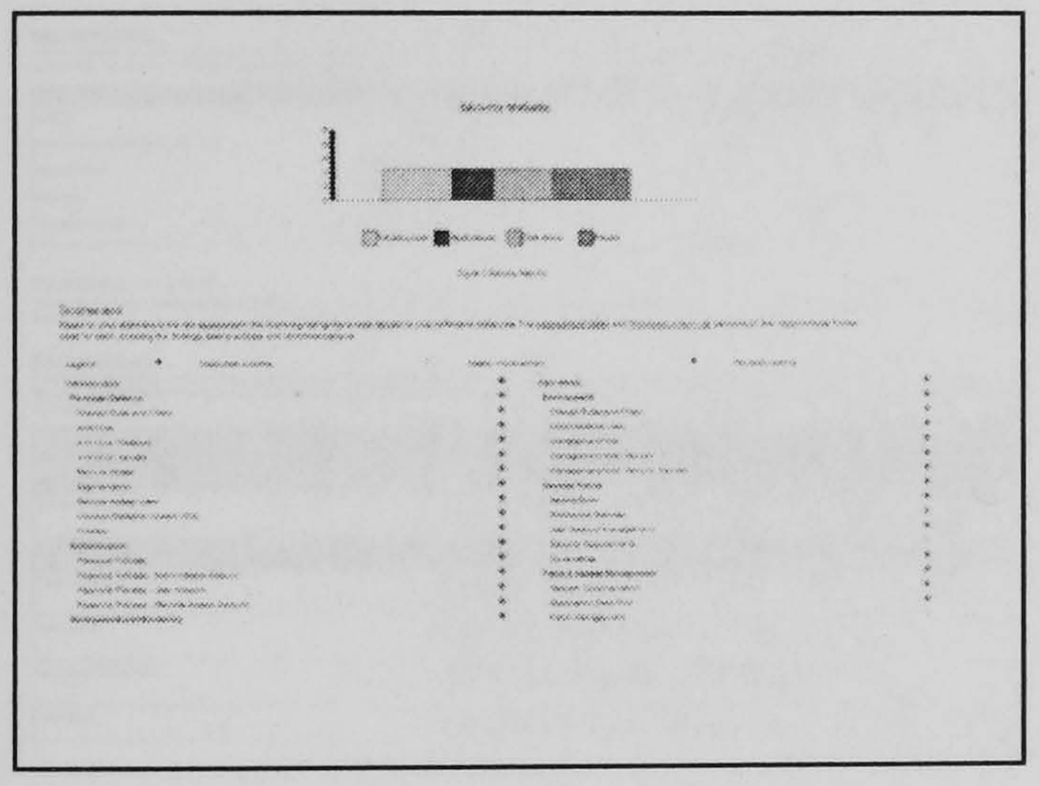
- **Advantages**
  "Easier to be completed since it doesn't take long time"
  "More user friendly (Not boring!)"
  "The risk measurement planning"
  "Profiling technique gives an idea especially to the non-trained user about the applications in the organisation that require attention"
  "Estimated costs very useful for financial planning"
  "User interface is good"
  "Scalability, less time to complete"
  "Ease of use"
  "Design"
  "Good description of the controls"
  "Easy to use, easy to ammend"
  "Easy to see the response to input values"
  "It is clear to follow step by step"
  "Box message: good point to advise the user "
  "Good content, up to date example with new threats"
  "Liked a lot the profiler, very easy to use, I think it can match the needs of SME"
  "The score module is clean and easy to run"
  "Overall simplicity"
  "User friendly, self-explanatory"

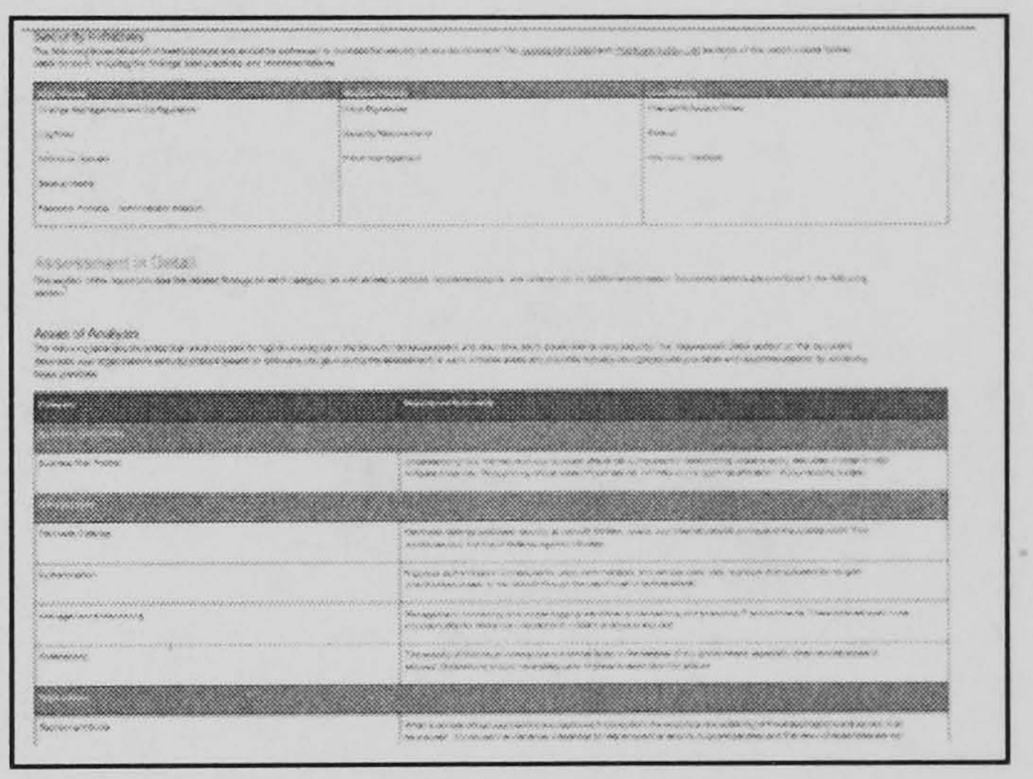
- **Disadvantages**
  "Not enough help function provided"
  "Too many functions in one window"
  "Perhaps not listing too many controls"
  "Output doc lacks supporting graphs and justification"
  "It may be hard to find quickly the solutions in the Assess threats module"

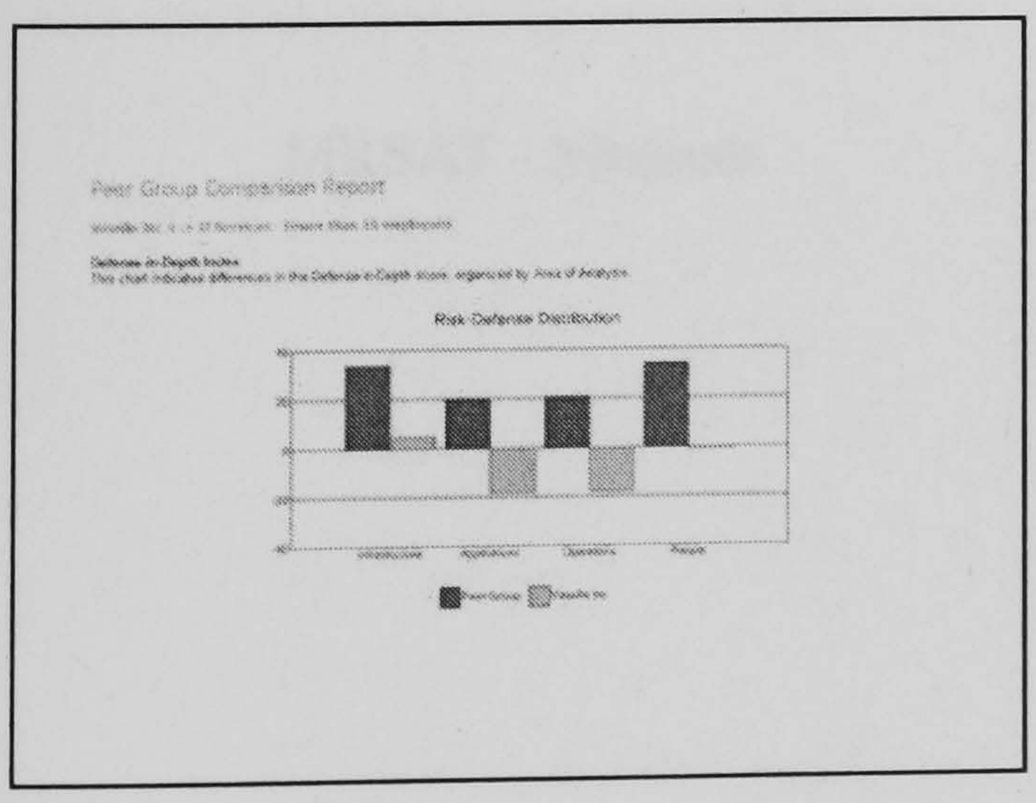
Appendix E: Outputs of the RA Tools

Mrsat - soho



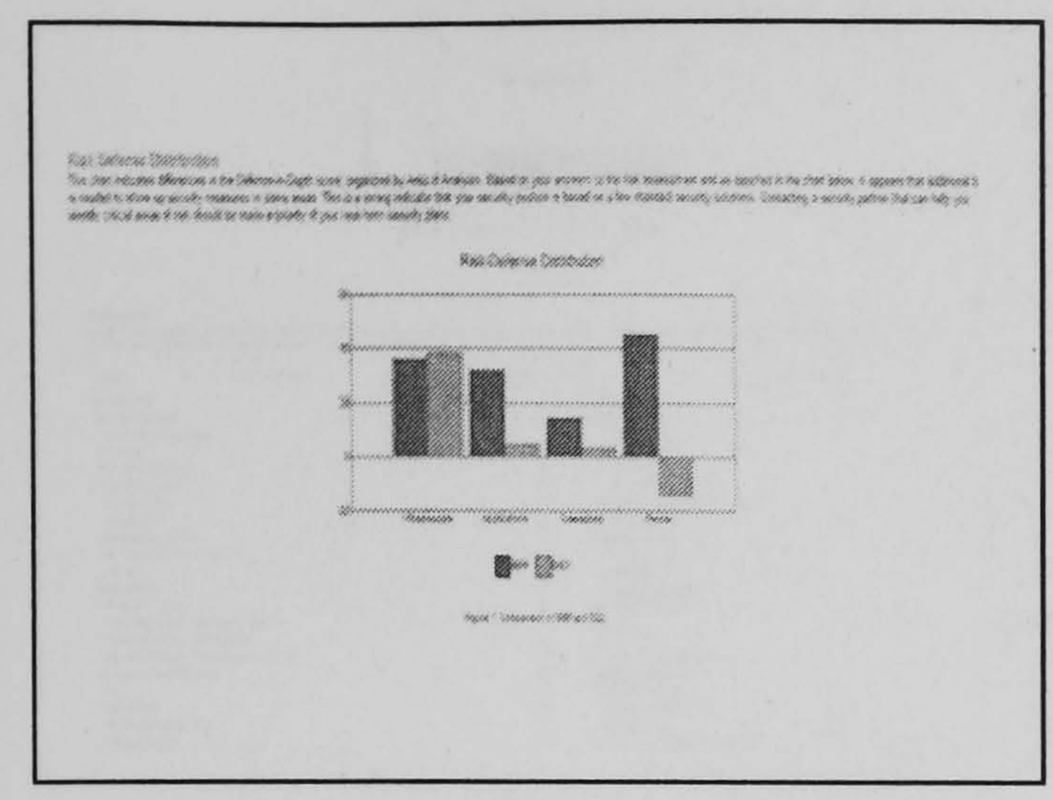


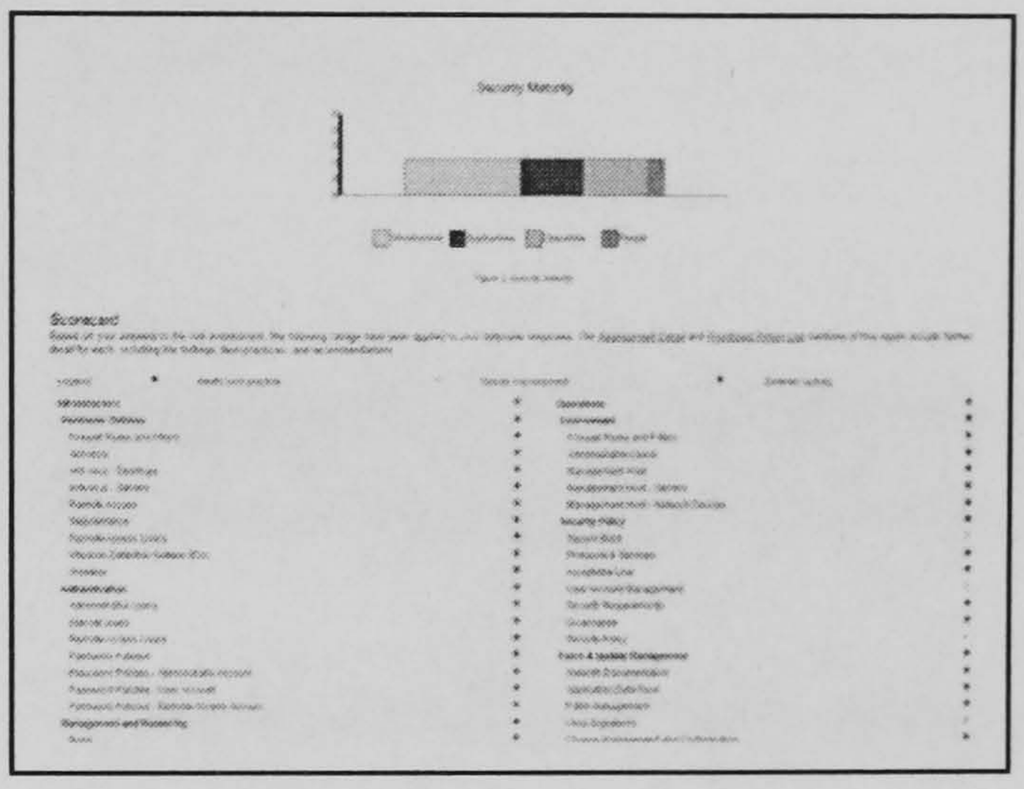


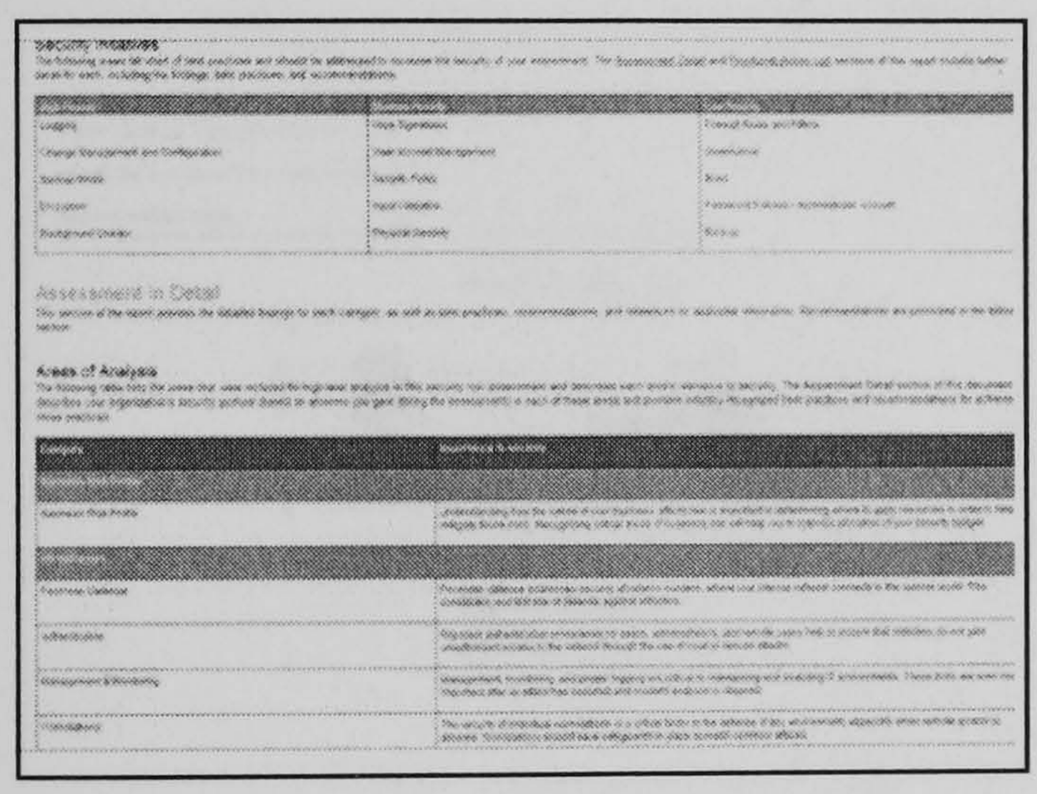


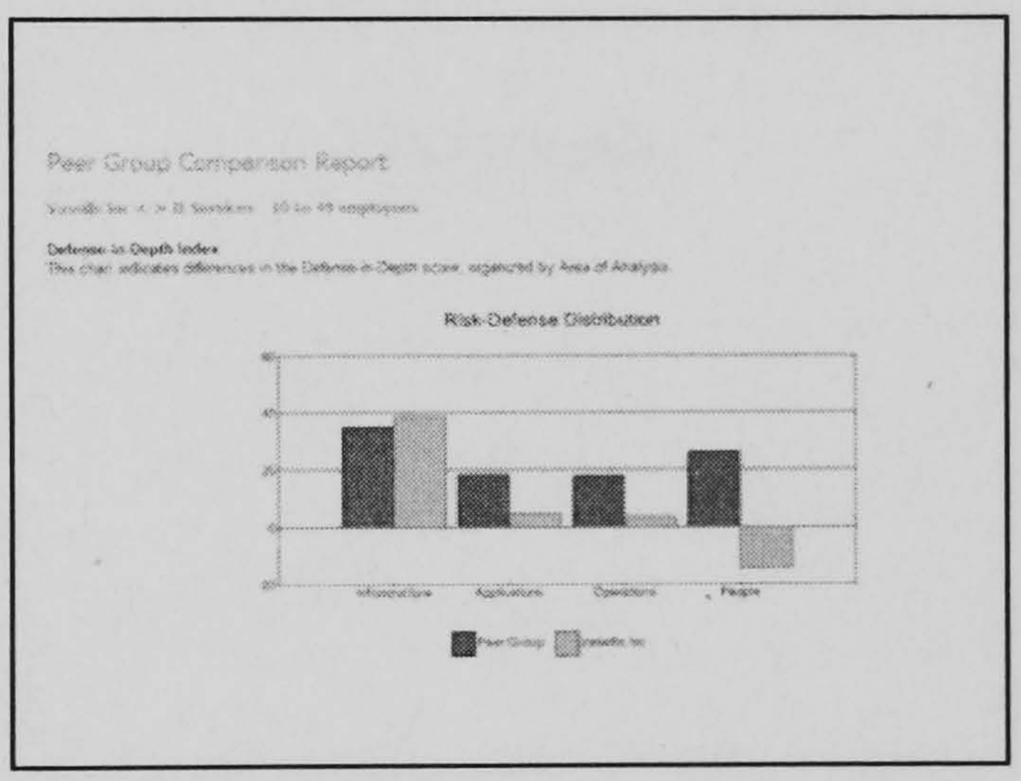
Mrsat -small

Appendix E: Outputs of the RA Tools

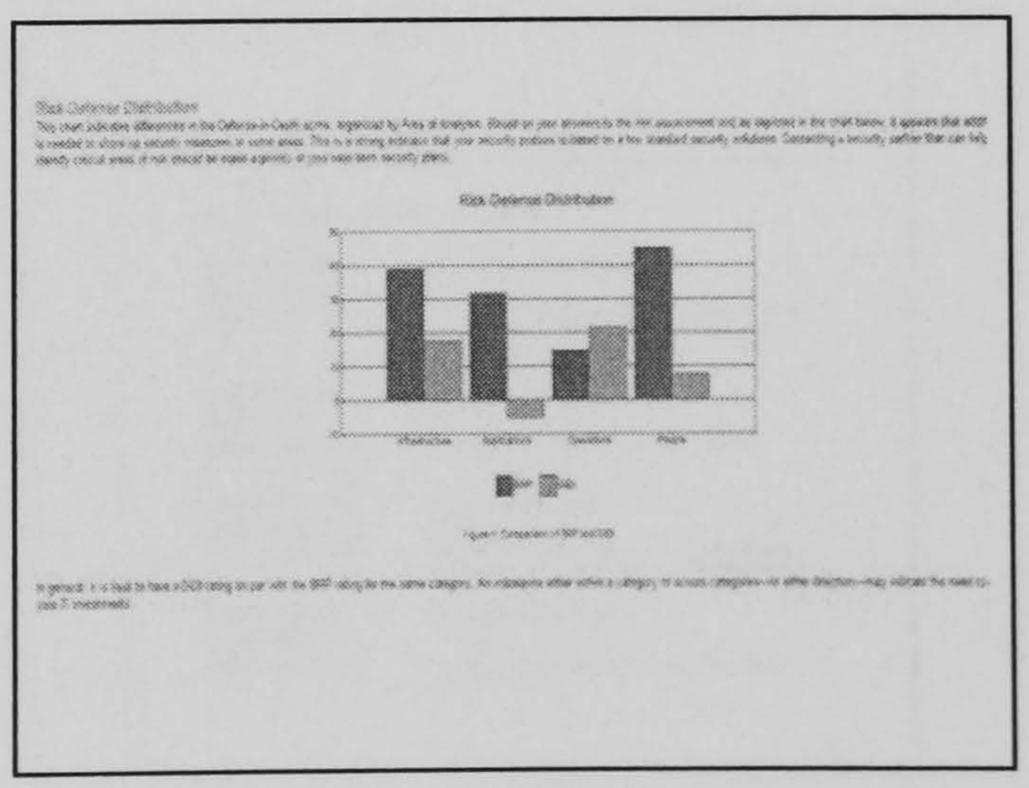




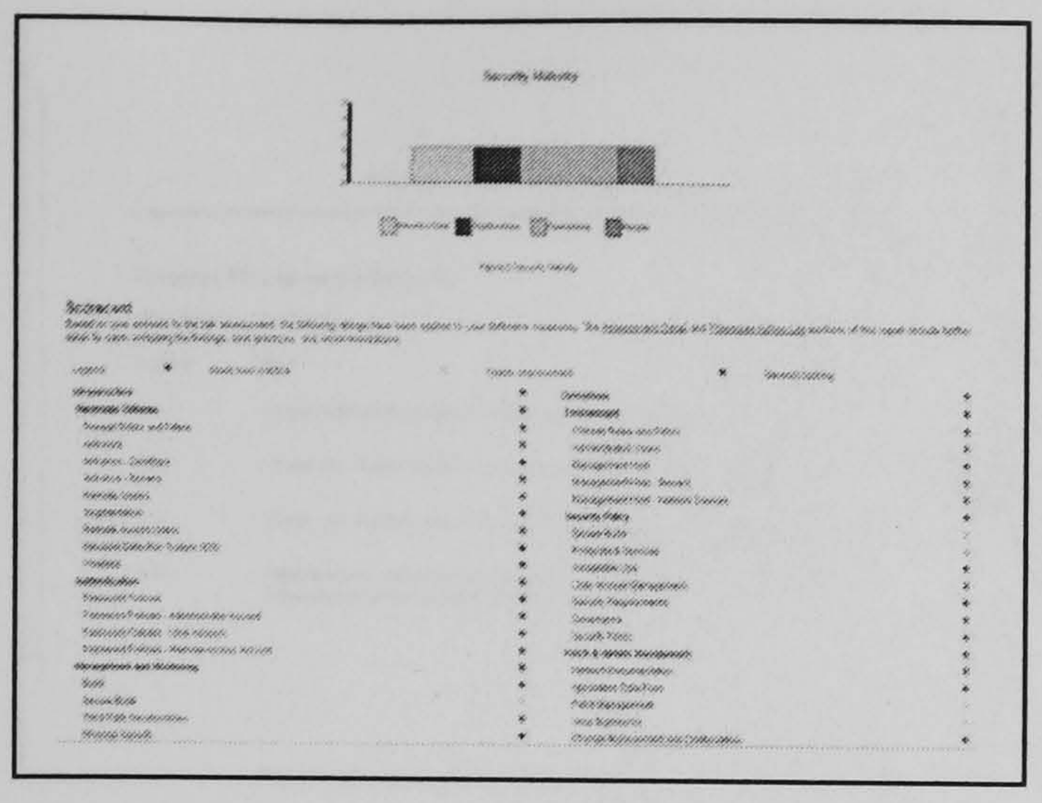


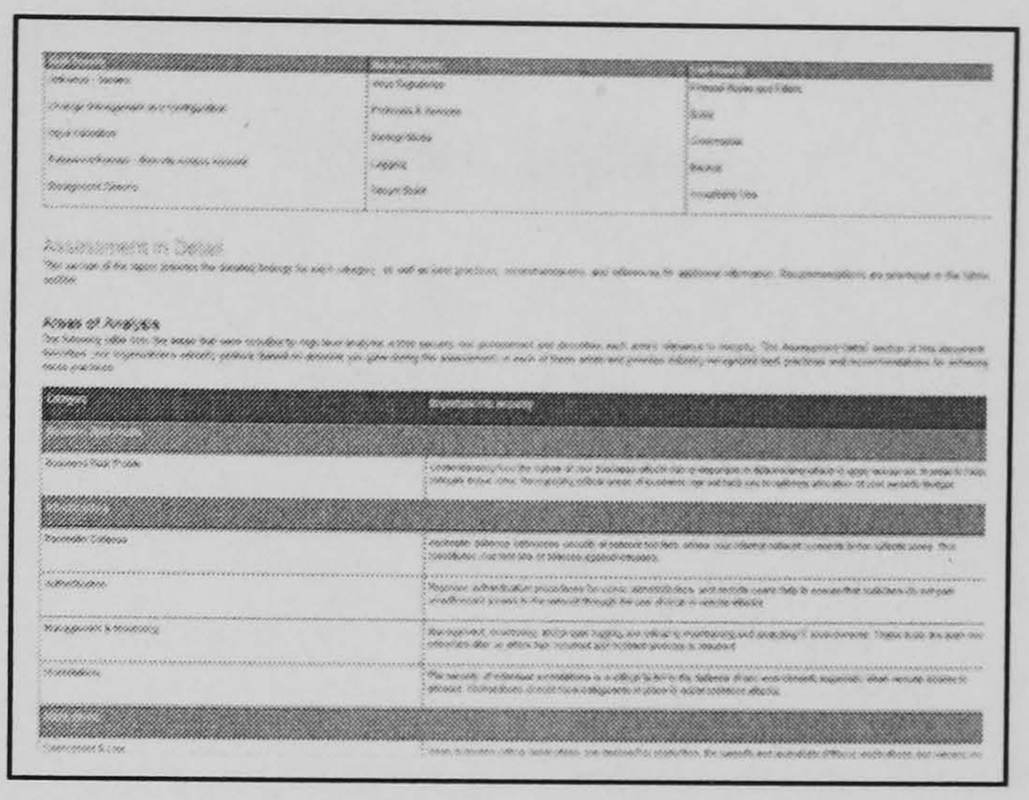


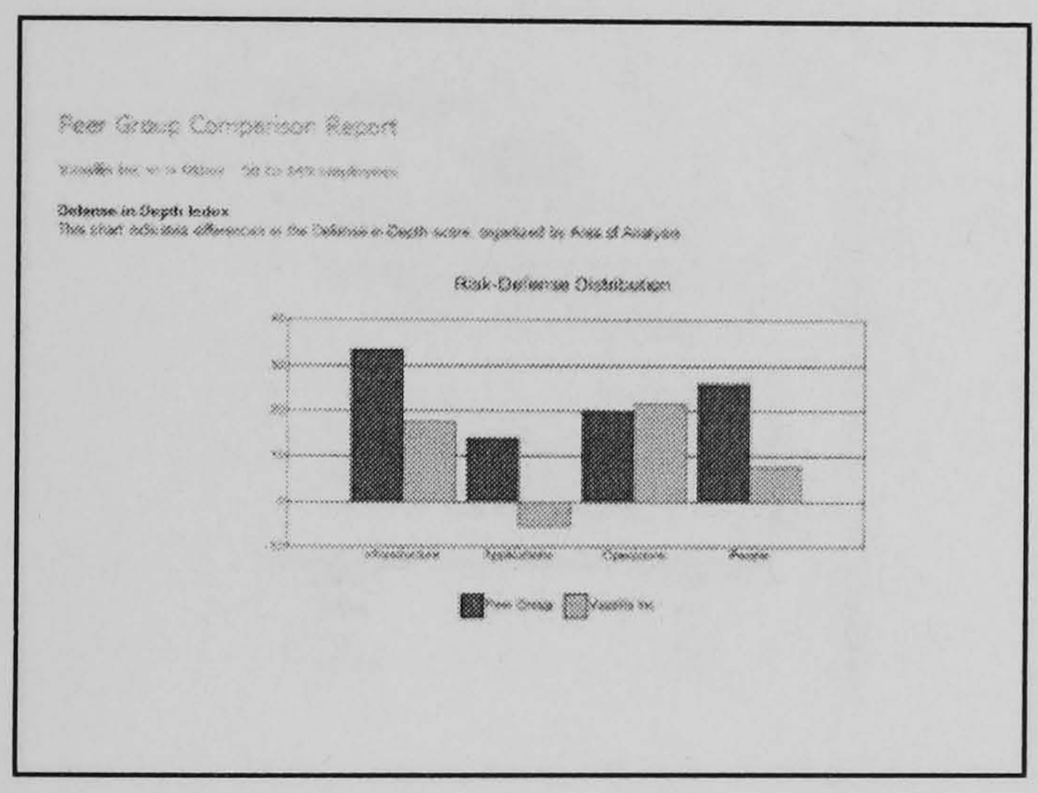
MRSAT - Medium



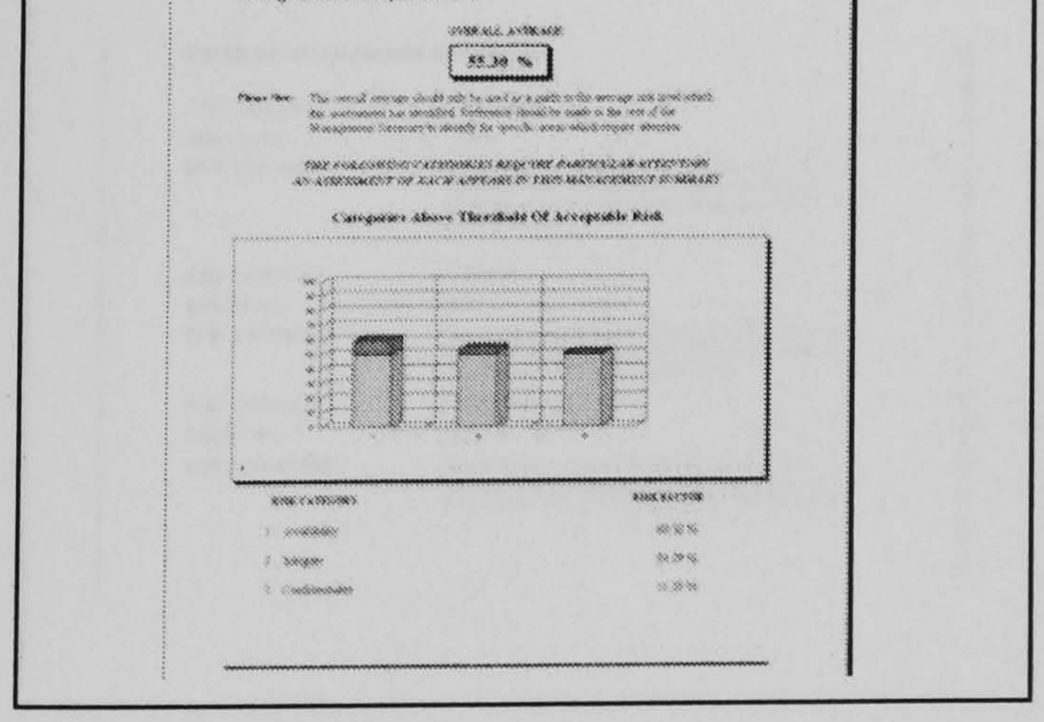
Appendix E: Outputs of the RA Tools

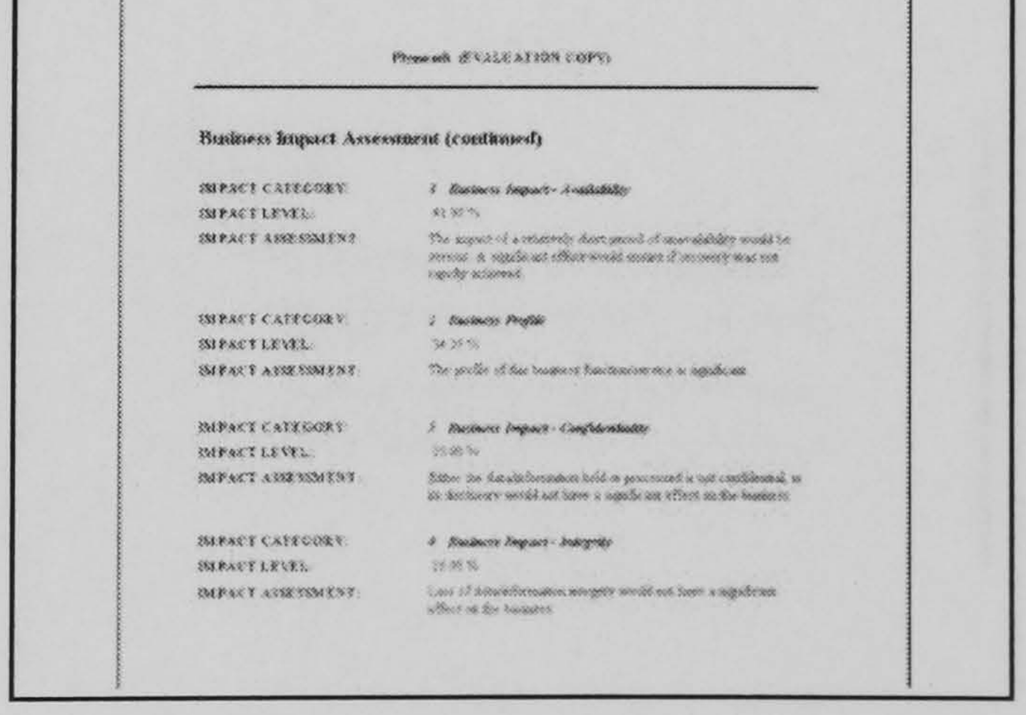






Cobra-small





Appendix E: Outputs of the RA Tools

(EVALUATION COPY)

Counter Measures (continued)

Risk Category: ***Availability***

NUMBER	TEXT
6112	Urgent steps should be taken to reduce exposure to Hacking/Electronic Sabotage
6114	Urgent steps should be taken to reduce exposure from the loss of third Party Service
6116	Urgent steps should be taken to reduce exposure from Operator Error/Sabotage
6120	Physical access controls/practices for those areas that may hold sensitive/confidential information should be reviewed and strengthened.

Cobra - medium

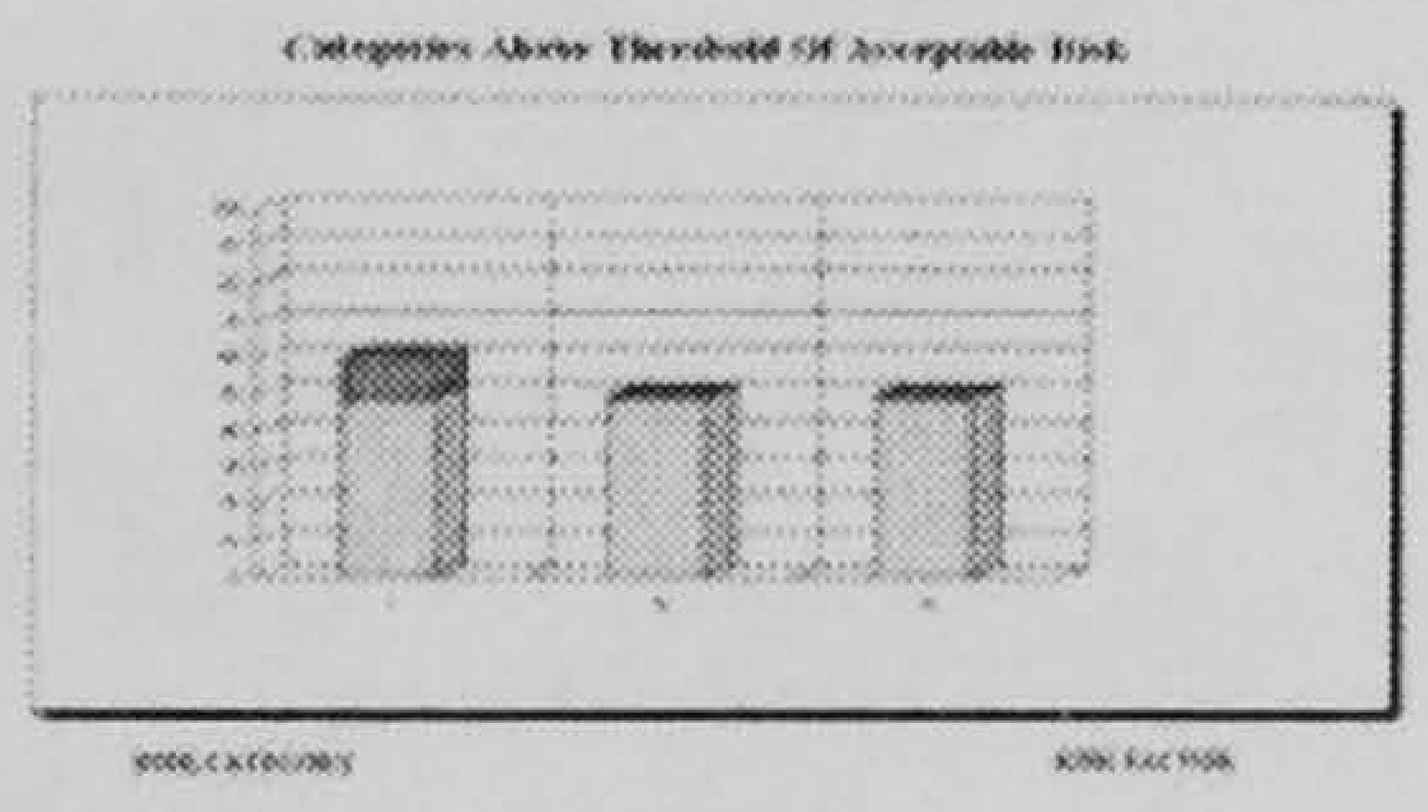
Management Summary (continued):

OVERALL AVERAGE

53.50 %

THE FOLLOWING CATEGORIES REQUIRE PARTICULAR ATTENTION

Categories Above Threshold Of Acceptable Risk



RISK CATEGORY	RISK FACTOR
1 Availability	66.29 %
2 Integrity	58.25 %
3 Confidentiality	58.20 %

Business Impact Assessment (continued)

IMPACT CATEGORY:	*1 Business Impact - Availability*
IMPACT LEVEL:	65.23 %
IMPACT ASSESSMENT:	The impact of even a short period of unavailability would be extremely serious. Within hours, this would have a very significant or even critical effect.
IMPACT CATEGORY:	*2 Business Impact - Confidentiality*
IMPACT LEVEL:	44.74 %
IMPACT ASSESSMENT:	A serious disclosure of confidential or key information/data could have a significant impact upon the business.
IMPACT CATEGORY:	*3 Business Impact - Integrity*
IMPACT LEVEL:	44.74 %
IMPACT ASSESSMENT:	A serious breach of information/data integrity could have a significant impact on the business.
IMPACT CATEGORY:	*4 Business Profile*
IMPACT LEVEL:	37.54 %
IMPACT ASSESSMENT:	The profile of this business from this service is significant.

Detailed Risk Assessment (continued)

RISK CATEGORY:	*1 Availability*
RISK LEVEL:	66.29 %
RISK ASSESSMENT:	The risk of serious unavailability of the business systems is high. Urgent steps should be taken to address this. A specific review or a full risk assessment is recommended to identify the specific measures required.
RISK CATEGORY:	*2 Integrity*
RISK LEVEL:	58.25 %
RISK ASSESSMENT:	The risk of loss of data integrity is considered to be high. Short term action should be taken to address this. A full risk assessment or security review should be urgently undertaken.
RISK CATEGORY:	*3 Confidentiality*
RISK LEVEL:	58.20 %
RISK ASSESSMENT:	The risk of serious unauthorised disclosure of information is considered to be high. Immediate steps should be taken to rectify this. A full risk assessment is recommended in the first instance.

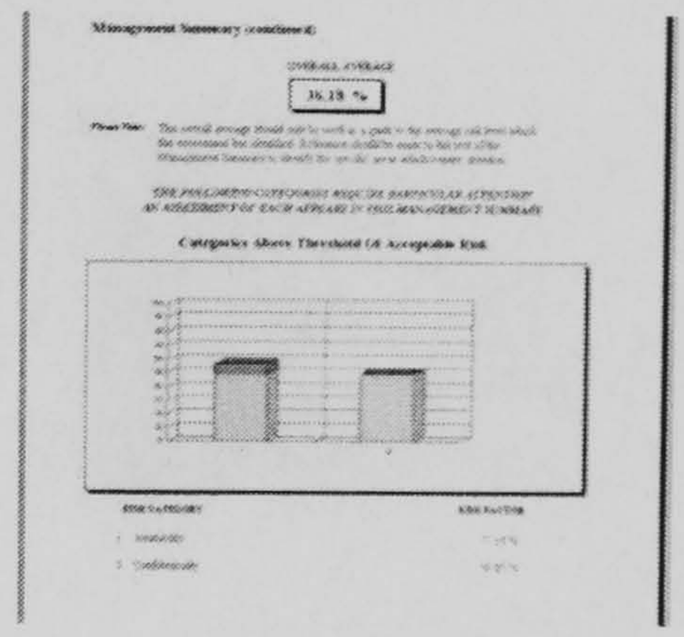
Counter Measures (continued)

Risk Category: ***Availability***

NUMBER	TEXT
6106	Urgent steps should be taken to reduce exposure to fire, flooding and explosion.
6108	Urgent steps should be taken to reduce exposure to hardware, equipment and media unavailability.
6112	Urgent steps should be taken to reduce exposure to Hacking/Electronic Sabotage
6114	Urgent steps should be taken to reduce exposure from the loss of third Party Service

Appendix E: Outputs of the RA Tools

Cobra – medium



Plymouth (EVALUATION COPY)

Business Impact Assessment (continued)

IMPACT CATEGORY: *1 Business Impact - Integrity*
IMPACT LEVEL: 100.00 %
IMPACT ASSESSMENT: A review of critical information/data integrity would have a critical impact to an extreme level that could compromise the existence of the business

IMPACT CATEGORY: *2 Business Impact - Confidentiality*
IMPACT LEVEL: 86.11 %
IMPACT ASSESSMENT: A serious disclosure of confidential or key information/data would have a critical impact to an extreme level that could even threaten the existence of the business

IMPACT CATEGORY: *3 Business Impact - Availability*
IMPACT LEVEL: 78.22 %
IMPACT ASSESSMENT: The impact of even a short period of unavailability would be extremely serious. Within hours, this would have a very significant or even critical effect

IMPACT CATEGORY: *4 Business Profile*
IMPACT LEVEL: 61.56 %
IMPACT ASSESSMENT: The profile of the business functionalities is significant

Plymouth (EVALUATION COPY)

Detailed Risk Assessment (continued)

RISK CATEGORY: *1 Availability*
RISK LEVEL: 57.18 %
RISK ASSESSMENT: The risk of serious vulnerabilities in the business systems is high. Urgent steps should be taken to address this. A specific review or a full risk assessment is recommended to identify the specific treatment required

RISK CATEGORY: *2 Confidentiality*
RISK LEVEL: 50.89 %
RISK ASSESSMENT: The risk of serious unauthorised disclosure of information is considered to be high. Immediate steps should be taken to rectify this. A full risk assessment is recommended as the first measure

RISK CATEGORY: *3 Integrity*
RISK LEVEL: 1.39 %
RISK ASSESSMENT: The risk of loss of data integrity is considered to be low. No major exposures were identified during the high level review.

Plymouth (EVALUATION COPY)

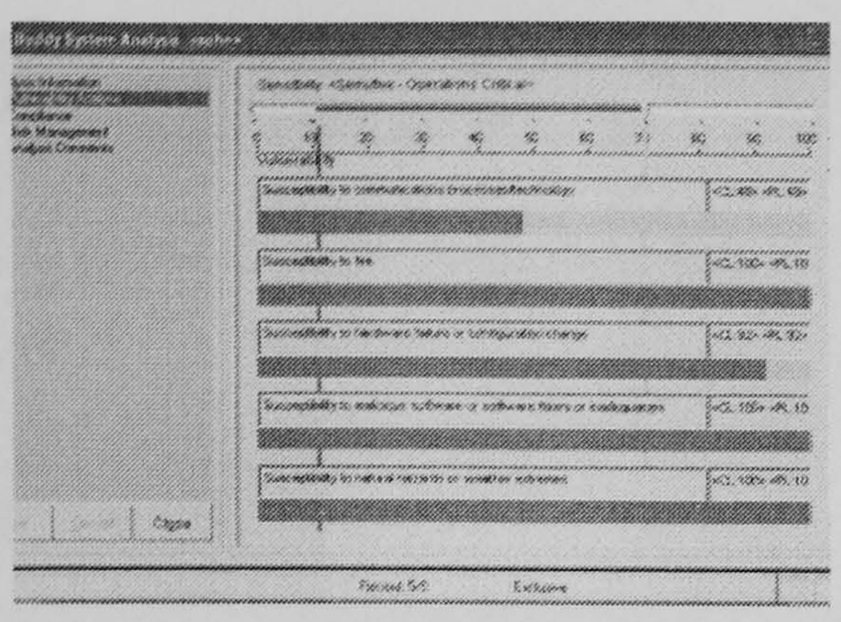
Counter Measures (continued)

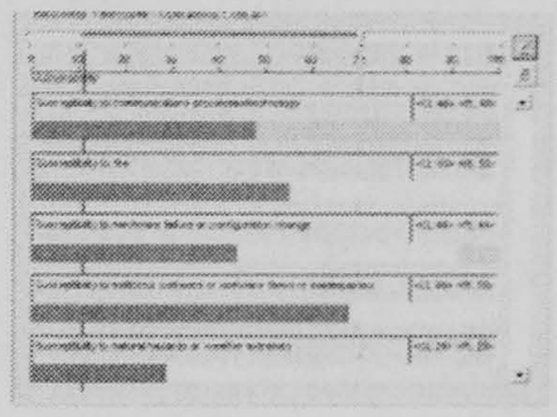
Risk Category: *4 Availability*

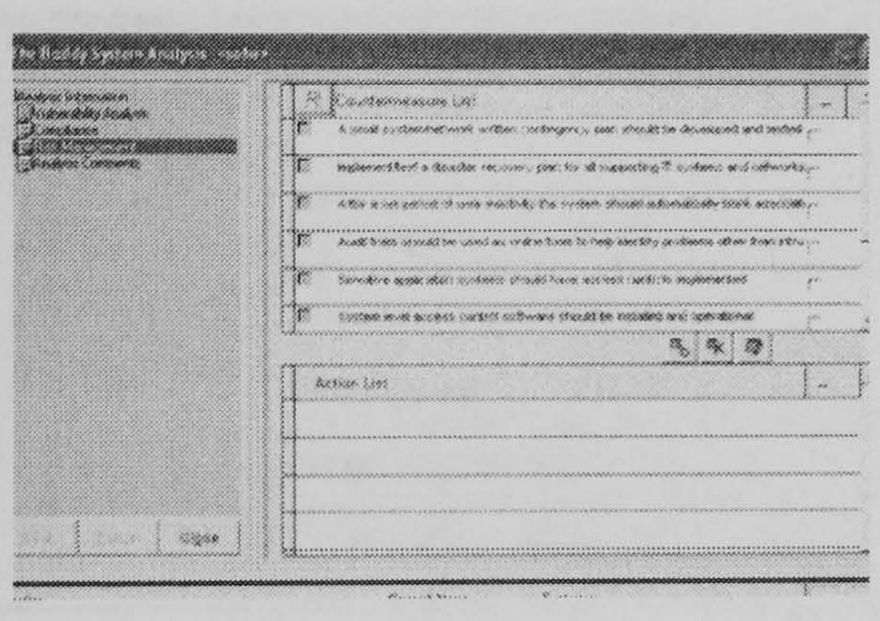
NUMBER	TEXT
6126	Urgent steps should be taken to reduce exposure to fire, flooding and explosion
6108	Urgent steps should be taken to reduce exposure to hardware, equipment and media unavailability
6113	Urgent steps should be taken to reduce exposure to Hacking/Electronic Sabotage
6114	Urgent steps should be taken to reduce exposure from the loss of third party Services
6118	Urgent steps should be taken to reduce exposure from Operator Error/Sabotage
6118	A review should be undertaken to consider any threats not identified above

Buddy - SOHO

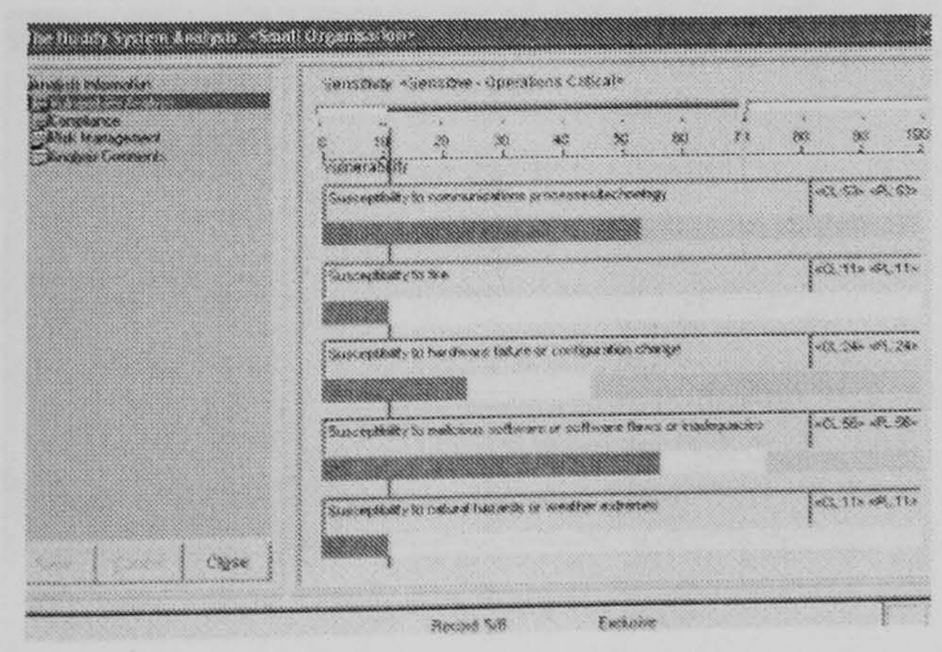
Appendix E: Outputs of the RA Tools

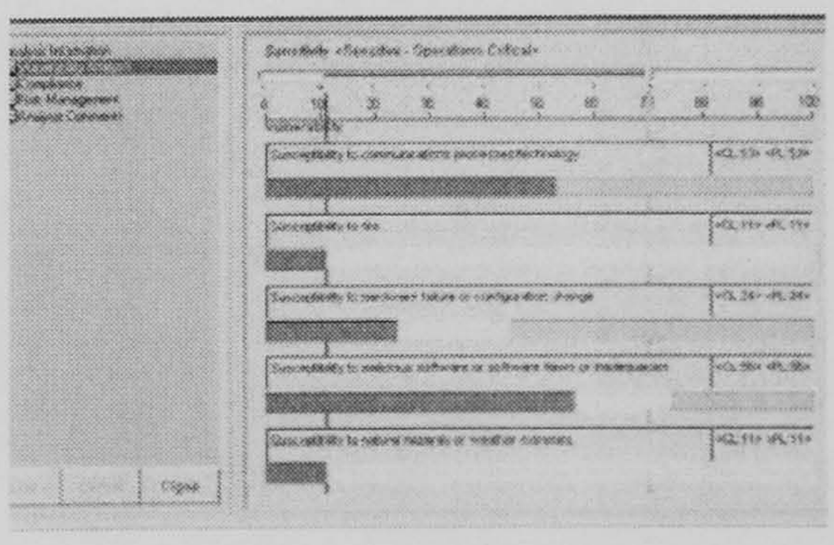




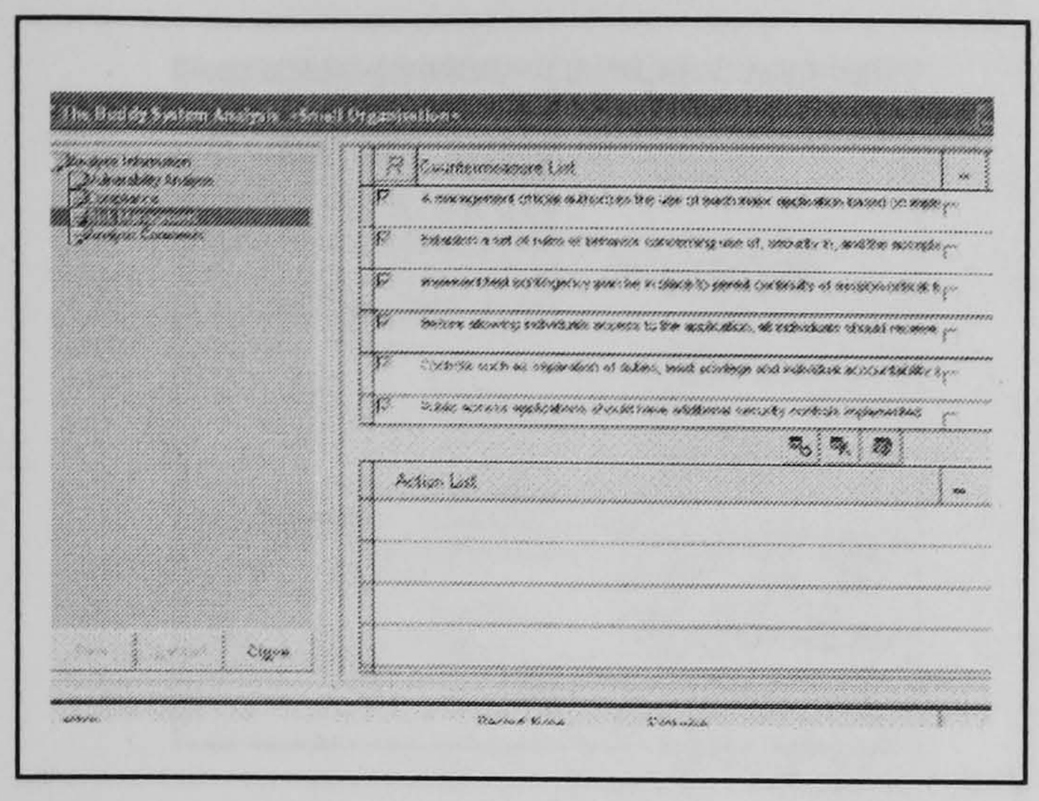


Buddy - Small

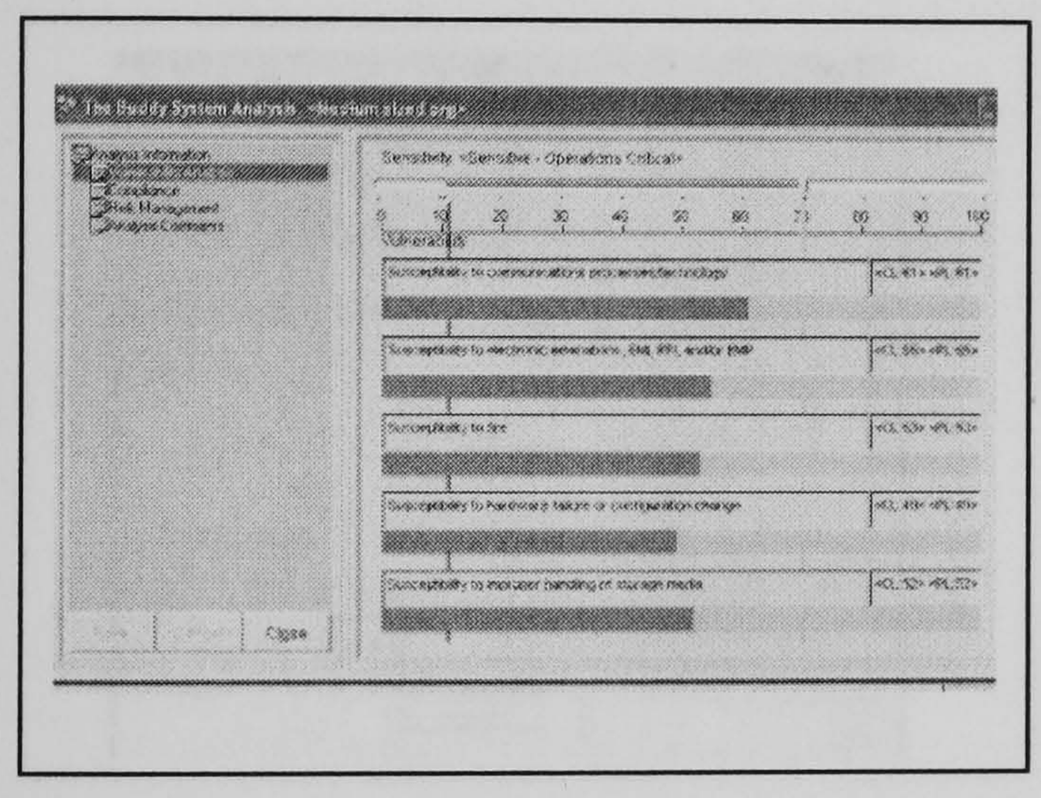


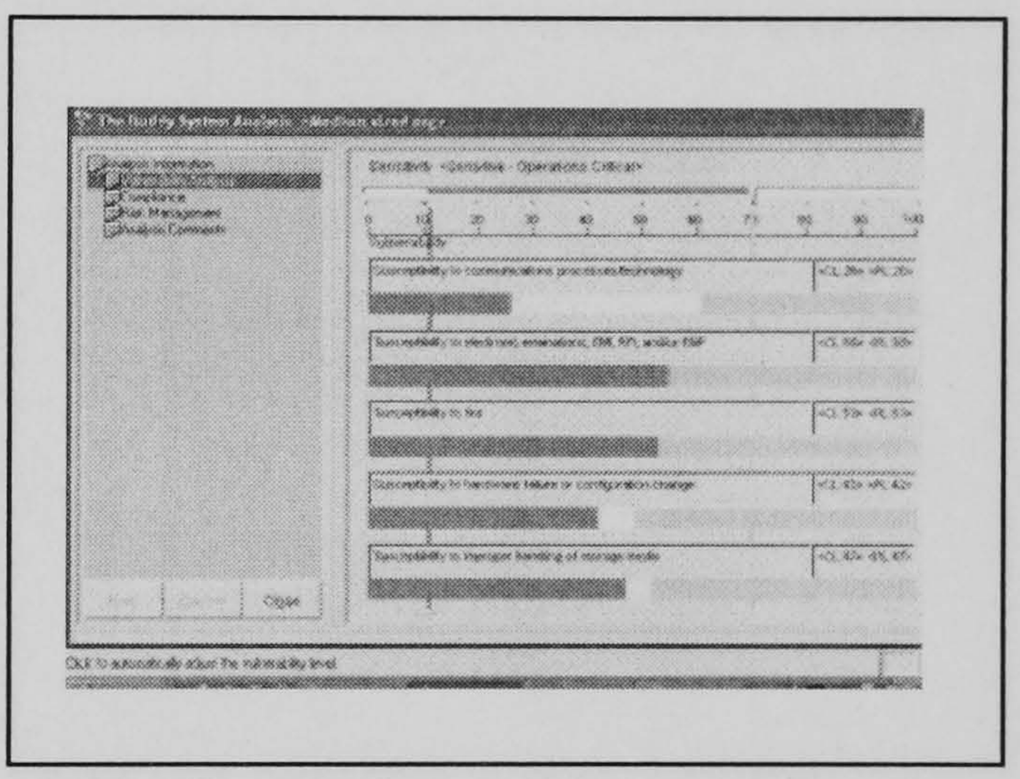


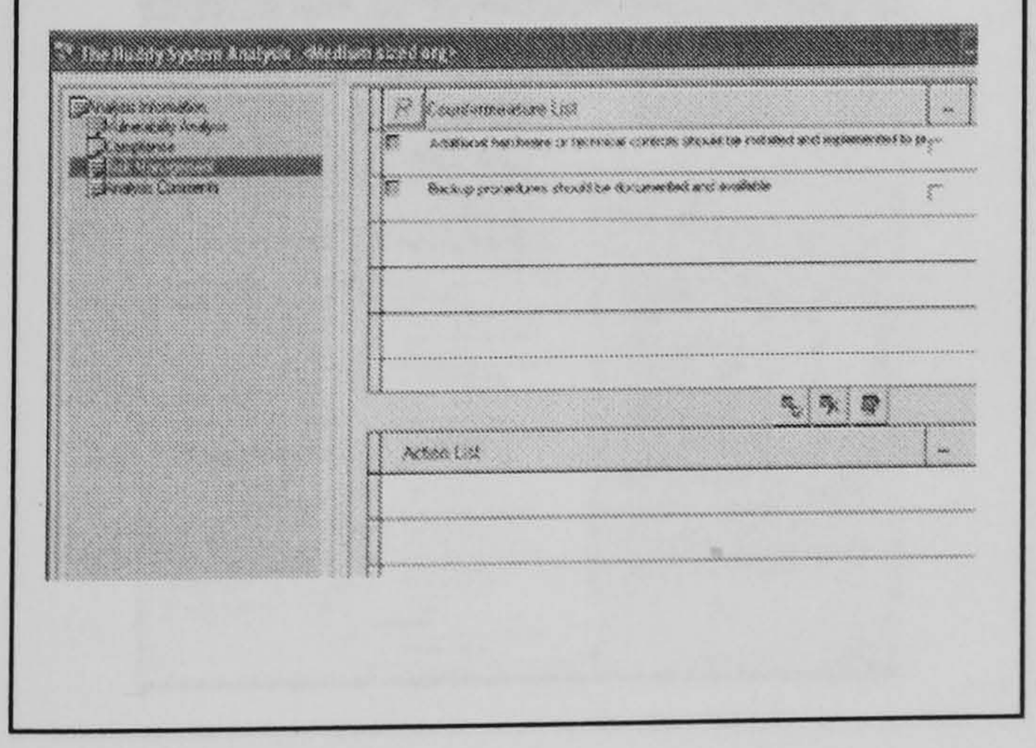
Appendix E: Outputs of the RA Tools



Buddy – Medium

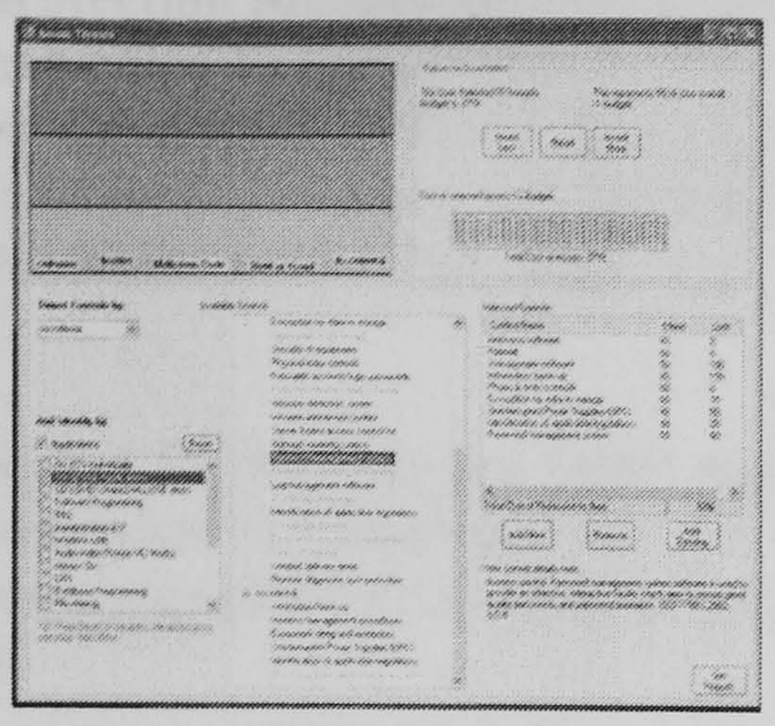




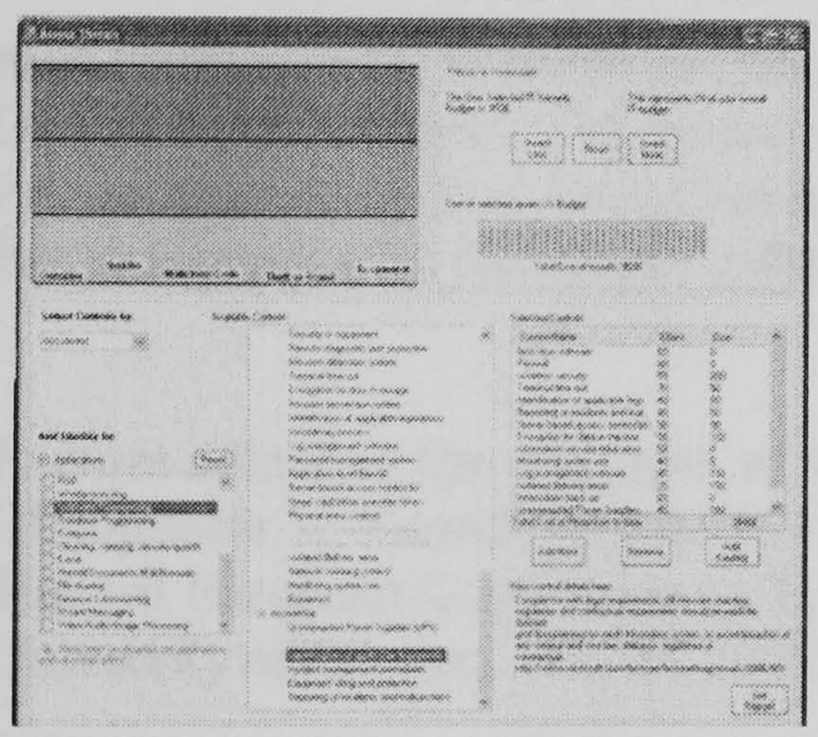


PRAM - SOHO

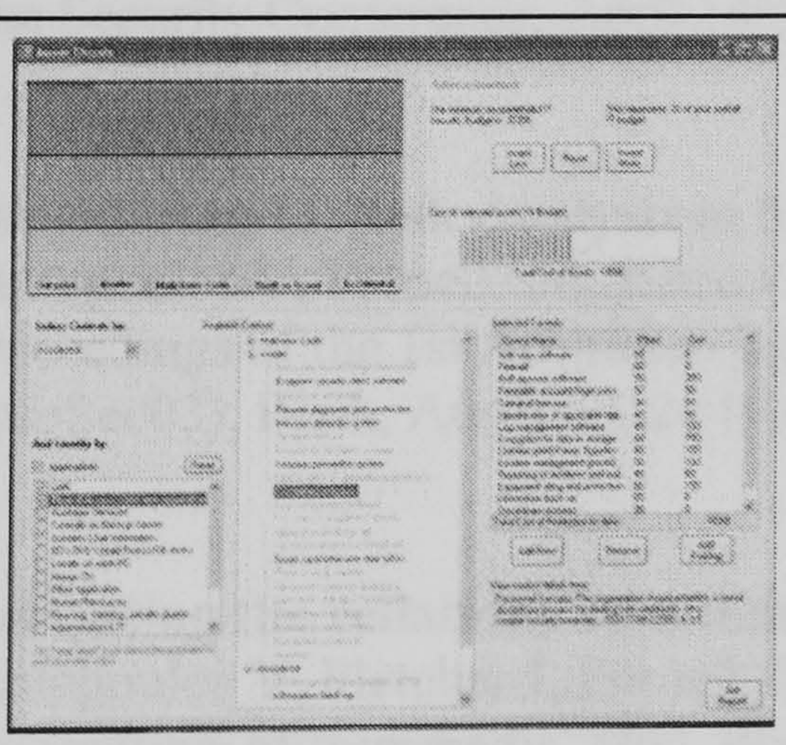
Appendix E: Outputs of the RA Tools



PRAM -Small



PRAM - Medium



Appendix F: Publications

A protection profiles approach to risk analysis for small and medium enterprises
Dimopoulos V, Furnell SM
Proceedings of IFIP TC-11 WG 11.1 & WG 11.5 Joint Working Conference on Security Management, Integrity, and Internal Control in Information Systems, Fairfax, Virginia, 1-2 December, pp267-283, 2005

Effective IT Security for Small and Medium Enterprises
Dimopoulos V, Furnell SM
Proceedings of the Fourth Security Conference 2005, Las Vegas, USA, 30-31 March, 2005

IT Risk Analysis for Small and Medium Enterprises
Kritharas I, Dimopoulos V, Furnell SM
Advances in Network & Communication Engineering 2, pp27-34 2005

Approaches to IT Security in Small and Medium Enterprises
Dimopoulos V, Furnell SM, Jennex M, Kritharas I
Proceedings of the 2nd Australian Information Security Management Conference 2004, Perth, Australia, 26 November 2004, CD-ROM, pp73-82, 2004

Factors affecting the adoption of IT risk analysis
Dimopoulos V, Furnell SM, Barlow I, Lines BL
The 3rd European Conference on Information Warfare and Security Royal Holloway, University of London, UK, 28-29 June, 2004

Using protection profiles to simplify risk management
Dimopoulos V, Furnell SM, Barlow I, Lines BL
The Security Conference, April 14/15, Las Vegas, USA, 2004

Considering IT Risk Analysis in Small and Medium Enterprises
Dimopoulos V, Furnell SM, Barlow I
Proceedings of the 1st Australian Information Security Management Conference 2003 (InfoSec03), Perth, Australia, 24 November, 2003

Evaluating the reliability of commercially available biometric devices
Dimopoulos V, Fletcher J, Furnell SM
Proceedings of Euromedia 2003, Plymouth, England, 14-16 April, pp166-174, 2003