

SJW-02L1-52

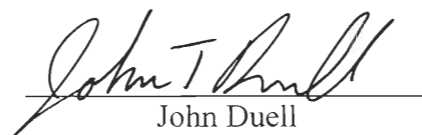
# E-Government Information Security

An Interactive Qualifying Project Report  
submitted to the Faculty of  
Worcester Polytechnic Institute  
in partial fulfilment of the requirements for the

Degree of Bachelor of Science

by

  
Joshua Coakley

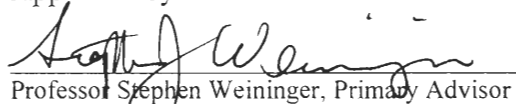
  
John Duell

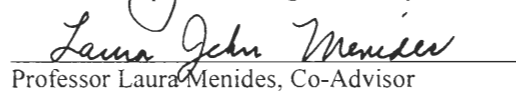
  
Jeffrey Kimball

  
Casey Whicher

Date: 26 April 2002

Approved by:

  
Professor Stephen Weininger, Primary Advisor

  
Professor Laura Menides, Co-Advisor

Sponsor:

Aziza Dar, Liaison  
IT Services Division  
London Borough of Merton, UK

## ***Abstract***

This risk analysis and feasibility study project was sponsored by the Information Technology (IT) Division of Merton. The methodologies used to complete it were interviews and CRAMM software - a risk analysis method. Through the quantitative and qualitative risk assessment of eight systems controlled by the IT Division, it was determined that there are risks, but most have controls in place. It was found that this type of a risk analysis could be expanded to all systems throughout the Council.

## ***Executive Summary***

In the past five years much legislation has been passed in the United Kingdom concerning data protection and information security. This new legislation, combined with the rapid pace of technological growth, is forcing organisations in both the public and the private sector to re-evaluate the procedures and policies on which they rely to safeguard their electronic information. To ensure that the Merton Council complied with these new laws, the IT Division decided to conduct a pilot CRAMM risk analysis. A risk analysis assesses the potential for various threats to harm an organisation. CRAMM stands for Central Government's Risk Analysis and Management Method, and is the most widely accepted method to conduct risk analyses in the public sector in the United Kingdom. It is more detailed and extensive than other risk assessment methodologies, and the IT Services Division did not know if it had the resources for such a demanding analysis on a Council-wide scale. For that reason, we were asked to analyse eight systems using CRAMM, with the twofold purpose of gaining experience with CRAMM and assessing the feasibility of conducting a similar exercise on the rest of the Council.

A software package based on CRAMM greatly aided us in our analyses by providing a quantitative analytical method endorsed by the United Kingdom and 12 other European countries. We would not have been able to initiate such an analysis in the absence of the software. The CRAMM exercise, much like other risk management exercises, requires information on assets and threats. An asset is something of value to an organisation, and can be physical (i.e. workstation,) data (i.e. information stored,) or software (i.e. software packages.) A threat is a problem that could potentially affect an organisation as a whole, or one of its assets in particular.

We used two methods for collecting the threat and asset information necessary for our analyses: one-on-one interviews and group interviews. We conducted 11 one-on-one

interviews with employees who were support staff and senior users of the eight systems with which we were concerned, and two interviews with employees who took care of the hardware on which the systems' data reside. These interviews allowed us to identify the assets of the eight systems, and the controls in place to minimise the impact of threats on the systems. We also gave each interviewee a list of 38 possible threats, provided to us by CRAMM, and asked them to identify the five most dangerous. Each threat has an associated multiple-choice questionnaire generated by CRAMM; we gave each interviewee the five questionnaires corresponding to the threats they identified. This information from the completed questionnaires was entered directly into the CRAMM software, and formed the basis of the quantitative risk analysis.

We also conducted two group interviews with two sections of the IT Division: the Desktop Support Group and Systems and Projects. Through these group interviews, we discussed and explored a few areas thought to be problematic, such as password control, and dial-up connections to the network from employees' homes.

We found that there are some areas in which improvements could be made. Password controls varied across the eight systems, and a standard by which all systems must abide would decrease the risk of unauthorised individuals gaining access to sensitive data. The current Legato tape backup procedure has had problems in the past, mainly due to inadequate support from the outside contractor. A different contractor, or in-house service, could increase the reliability of the backup procedures. Also, the Remote Access Server (RAS) that employees can use to log on to the network does not have a secure connection, and replacing it with a connection based on Virtual Private Networking (VPN) technology could prevent an outside individual from gaining 'backdoor' access to the systems.

The data we entered into CRAMM allowed the software to identify 97 possible controls to help minimise the impact of the threats identified. Of those controls, 47 of them

were already in place in some partial or complete form. Focusing on both the unimplemented and partially implemented, we found that many addressed the areas of concern identified in our group interviews. Specifically, there were six controls relating to password security that we felt were both feasible and useful, five relating to tape backup systems, and one relating to dial-up access, as well as many others.

We believe that a CRAMM analysis of the entire Council is entirely feasible. Employee time was on average one hour per person, including all interviewing. The maximum time we could foresee would be two hours per individual. This is not excessive, and as it could be spread over a period of weeks, is not at all unreasonable. To work most efficiently, we advise that the team conducting the exercise take a training course on CRAMM software, which will hopefully eliminate the time we spent familiarising ourselves with the software and methodology.

Risk and gap analyses are an important step in the growth of any organisation. The Merton Council is currently contemplating a transition to more Internet-oriented services, referred to as E-Government. Internet-based services will create more threats to the information stored by the Council, because there will be a greater reliance on technology. Before this conversion is made, it is important to ensure that current controls do as much as possible to minimise existing risks. Conducting a Council-wide CRAMM analysis will not only help Merton become compliant with laws and standards, but also help ease the transition from its current services to an E-Government. Our project has initiated the risk analysis necessary for the change, and demonstrated that a complete CRAMM analysis of the Council is entirely feasible.

## ***Acknowledgements***

To those without whose help we could not have completed our project:

Gurmel Bansel, Director of IT Services

Paul Biggs, Technical Support Manager

Josh Brandt, WPI Unix System Administrator

Peter Brown, Analyst Programmer

Paul Damaa, Lead Engineer

Aziza Dar, Project Liaison

Geoff Davey, Informations Systems Officer

David Everitt, WPI Associate Director of Human Resources

Tracey Hawkins, Senior User

Jennie Hawks, London Project Site Coordinator

Robert Heap, Analyst Programmer

Steven Key, Payroll Manager

Mark Kitson, Desktop and Server Engineer

Krystyna Kiuber, Analyst Programmer

Steven Lawrenson, Systems and Projects Manager

Colin Lloyd, Systems Control Manager

David Lovatt, Distributed Lead Engineer

Colin Mason, Analyst Programmer

Raymond McInnis, Central Postroom Manager

Professor Laura Menides, Advisor

Chris Nice, Analyst Programmer

Felix Stride-Darnley, ISS Team Leader

John Sykes, ISS HSG Team Leader

Ben Thompson, Director of WPI Computing Systems

Richard Warren, Service Delivery Manager

Graeme Webster, Analyst Programmer

Professor Stephen Weininger, Advisor

# Table of Contents

Abstract.....	ii
Executive Summary.....	iii
Acknowledgements.....	vi
Table of Contents.....	vii
List of Tables.....	x
List of Figures.....	xi
Authorship.....	xii
1. Introduction.....	1
2. Background.....	4
2.1 Merton Local Authority.....	4
2.1.1 IT Services Division.....	4
2.1.2 Systems Studied.....	5
2.2 Information Security.....	8
2.2.1 Data integrity.....	8
2.2.2 Data confidentiality.....	9
2.2.3 Data availability.....	10
2.2.4 Human Factors.....	10
2.3 Legislative Changes.....	13
2.4 Risk Management.....	13
2.4.1 Types of Risks.....	14
2.4.1.1 Legal and Regulatory Risks.....	15
2.4.1.2 Organisational Management/Human Factors.....	15
2.4.1.3 Technical and Operational Risks.....	17
2.4.2 Risk Management Types.....	18
2.4.2.1 Quantitative Risk Analysis.....	18
2.4.2.2 Qualitative Risk Analysis.....	19
2.4.2.3 Gap Analysis.....	19
2.4.3 Risk Levels.....	20
2.4.3.1 Corporate/Strategy.....	20
2.4.3.2 Programme.....	21
2.4.3.3 Project.....	21
2.4.3.4 Operations.....	21
2.4.4 Risk Management Framework.....	21
2.5 Case Study – WPI Banner System.....	23
3. Methodology.....	26
3.1 Scope.....	26
3.2 Interviews.....	27
3.2.1 General Interviewing Information.....	27
3.2.2 Interviews Conducted.....	28
3.3 Group Interviews.....	31
3.4 CRAMM Software.....	32
3.5 Data Collection.....	35
3.5.1 Assets.....	35
3.5.2 Threats.....	35

3.6 Data Analysis .....	36
3.6.1 Risk Analysis .....	36
3.6.2 Gap Analysis .....	36
3.7 Project Management Database .....	37
4. Data.....	38
4.1 Assets Identified.....	38
4.1.1 Physical Assets.....	38
4.1.2 Data Assets.....	40
4.1.3 End User Services .....	42
4.1.4 Asset Reports .....	43
4.2 Threats.....	44
4.2.1 Threats to Specific Systems .....	45
4.2.1.1 Frequently Identified Threats.....	46
4.2.1.2 Dangerous Threats .....	49
4.2.1.3 IT Threats to Entire Council .....	52
4.2.2 Threat Reports.....	54
5. Analysis .....	55
5.1 Risk Analysis .....	55
5.1.1 CRAMM Results .....	55
5.1.2 Greatest Risks .....	58
5.2 Gap Analysis.....	59
5.2.1 Current Controls.....	60
5.2.2 CRAMM Recommendations .....	61
5.2.3 Our Recommendations.....	61
5.2.3.1 Passwords.....	62
5.2.3.2 Remote Access Server (RAS).....	63
5.2.3.3 Backups.....	64
5.2.3.4 Data Protection.....	65
5.2.3.5 Knowledge of Assets .....	65
5.2.3.6 Miscellaneous Recommendations.....	66
6. Conclusions .....	67
6.1 Feasibility Study .....	67
6.1.1 Time Spent on the CRAMM Exercise .....	67
6.1.1.1 Our Work .....	68
6.1.1.2 Council Officer Time.....	70
6.1.2 Recommendations.....	71
6.2 Final Thoughts .....	73
Bibliography .....	75
Glossary .....	78
Appendix A: Merton IT Services Division .....	80
Appendix B: Legislation and Standards Affecting Information Security .....	82
Appendix C: CRAMM Methodology .....	91
Appendix D: The Merton Information Security Policy .....	92
Appendix E: Physical Asset Valuation Report .....	102



Appendix F: Data Asset Valuation Report.....	103
Appendix G: Software Asset Valuation Report .....	105
Appendix H: Definition of Threats .....	107
Appendix I: Sample CRAMM Questionnaire .....	110
Appendix J: Employee Identified Threats.....	113
Appendix K: Threat and Vulnerability Report.....	115
Appendix L: Measure of Risk (MoR) Report .....	117
Appendix M: Controls Suggested by CRAMM.....	125
Appendix N: Meetings and Interviews Report.....	129
Appendix O: Interviews at WPI .....	135
Appendix P: Interviews in Merton .....	143
Appendix Q: Officer Time by System .....	177
Appendix R: Project Timeline.....	178

## **List of Tables**

Table 4-1: End User Services.....	43
Table 4-2: Threats, number of times identified, and systems identifying those threats.....	45
Table 5-1: CRAMM Risk Assessment Matrix.....	56
Table 5-2: Risk Assessment Summary.....	56-57
Table B-1: Reasons for Processing Sensitive Data.....	82
Table B-2: Reasons for Processing Non-Sensitive Data.....	83
Table B-3: Exceptions to Point VIII.....	84

**List of Figures**

Figure 2-1: Iterative Risk Management Cycle.....23

Figure 3-1: Data Gathering Process .....30

Figure 3-2: CRAMM Methodology Flowchart.....34

## Authorship

Joshua Coakley – JC  
Jeff Kimball – JK

John Duell – JD  
Casey Whicher – CW

	Contributors	
	<u>Major</u>	<u>Editor</u>
Abstract	All	All
Executive Summary	All	All
Acknowledgements	---	All
Table of Contents	---	All
List of Tables	---	All
List of Figures	---	All
Authorship Page	---	All
<b>1. Introduction</b>	All	All
<b>2. Background</b>	---	---
2.1 Merton Local Authority	JC,JD	JK
2.1.1 IT Services Division	JC,JD	JK
2.1.2 Systems Studied	JC	CW
2.2 Information Security	JC	CW
2.2.1 Data integrity	JC	CW
2.2.2 Data confidentiality	JC	CW
2.2.3 Data availability	JC	CW
2.2.4 Human Factors	JC	CW
2.3 Legislative Changes	JD	JC
2.4 Risk Management	JK	JC,JD
2.4.1 Types of Risks	JK	JC,JD
2.4.1.1 Legal and Regulatory Risks	JK	JC,JD
2.4.1.2 Organisational Management/Human Factors	JK	JC,JD
2.4.1.3 Technical and Operational Risks	JK	JC,JD
2.4.2 Risk Management Types	JK	JC,JD
2.4.2.1 Quantitative Risk Analysis	JK	JC,JD
2.4.2.2 Qualitative Risk Analysis	JK	JC,JD
2.4.2.3 Gap Analysis	JK,JC	JC,JD
2.4.3 Risk Levels	JK	JC,JD
2.4.3.1 Corporate/Strategy	JK	JC,JD
2.4.3.2 Programme	JK	JC,JD
2.4.3.3 Project	JK	JC,JD
2.4.3.4 Operations	JK	JC,JD
2.4.4 Risk Management Framework	JK	JC,JD
2.5 Case Study – WPI Banner System	JK	CW
<b>3. Methodology</b>	---	---
3.1 Scope	CW	All
3.2 Interviews	---	All
3.2.1 General Interviewing Information	CW	All
3.2.2 Interviews Conducted	CW	All
3.3 Group Interviews	JK	All

3.4 CRAMM Software	JD,JK	All
3.5 Data Collection	JC	All
3.5.1 Assets	JC	All
3.5.2 Threats	JC	All
3.6 Data Analysis	JK	All
3.6.1 Risk Analysis	JK	All
3.6.2 Gap Analysis	JK	All
3.7 Project Management Database	CW	All
<b>4. Data</b>	---	---
4.1 Assets Identified	JK	JC,JD
4.1.1 Physical Assets	JK	JC,JD
4.1.2 Data Assets	JK	JC,JD
4.1.3 End User Services	JK	JC,JD
4.1.4 Asset Reports	JK	JC,JD
4.2 Threats	CW	JC
4.2.1 Threats to Specific Systems	CW	JC
4.2.1.1 Frequently Identified Threats	CW	JC
4.2.1.2 Dangerous Threats	CW	JC
4.2.1.3 IT Threats to Entire Council	JK	JC
4.2.2 Threat Reports	CW	JC,JD
<b>5. Analysis</b>	---	---
5.1 Risk Analysis	JC	JK,JD
5.1.1 CRAMM Results	JC	JK,JD
5.1.2 Important Risks	JC	JK,JD
5.2 Gap Analysis	JC	JK,JD
5.2.1 Current Controls	JC	JK,JD
5.2.2 CRAMM Recommendations	JK	CW,JD
5.2.3 Our Recommendations	JD	CW,JK
5.2.3.1 Passwords	JD	CW,JK
5.2.3.2 Remote Access Server (RAS)	JD	CW,JK
5.2.3.3 Backups	JD	CW,JK
5.2.3.4 Data Protection	JD	CW,JK
5.2.3.5 Knowledge of Assets	JD	CW,JK
5.2.3.6 Miscellaneous Recommendations	JD	CW,JK
<b>6. Conclusions</b>	---	---
6.1 Feasibility Study	CW	JC,JD
6.1.1 Time Spent on the CRAMM Exercise	CW	JC,JD
6.1.1.1 Our Work	CW	JC,JD
6.1.1.2 Council Officer Time	CW	JC,JD
6.1.2 Recommendations	CW	All
6.2 Final Thoughts	JD	All
<b>Bibliography</b>	---	---
<b>Glossary</b>	---	---
<b>Appendices</b>		
Appendix A: Merton IT Services Division	---	---

Appendix B: Legislation and Standards Affecting Information Security	All	All
Appendix C: CRAMM Methodology	All	All
Appendix D: The Merton Information Security Policy	---	---
Appendix E: Physical Asset Valuation Report	---	---
Appendix F: Data Asset Valuation Report	---	---
Appendix G: Software Asset Valuation Report	---	---
Appendix H: Definition of Threats	---	---
Appendix I: Sample CRAMM Questionnaire	---	---
Appendix J: Employee Identified Threats	---	---
Appendix K: Threat and Vulnerability Report	---	---
Appendix L: Measure of Risk (MoR) Report	---	---
Appendix M: Controls Suggested by CRAMM	---	---
Appendix N: Meetings and Interviews Report	All	All
Appendix O: Interviews at WPI	All	All
Appendix P: Interviews in Merton	All	All
Appendix Q: Officer Time by System	JC	JK
Appendix R: Gantt Chart	All	All

# 1. Introduction

Government organisations for developed nations throughout the world store and maintain important personal and financial information for a substantial amount of their citizens. The use of computer database systems to house and regulate this sensitive data has allowed organisations to streamline their information management processes. Along with the benefits these new systems have brought, they have also caused a need for new security measures and procedures to be developed to adequately safeguard important information from theft, destruction, and corruption.

Recent laws have been passed in Britain that were enacted to protect the rights of people whose information is being held by the government and other organisations. The Data Protection Act was passed in 1998 and the Freedom of Information Act was passed in 2000. Around the same time, the British Standards Institute updated British Standard 7799 (BS7799), a document describing proper information security policies, to comply with the new legislation. Although these acts do not take full effect until 2007, they, as well as BS7799, are forcing organisations throughout Britain to reassess their policies towards information security.

The Merton Local Authority, also called the Merton Council (see Appendix A) wrote an Information Security Policy (ISP – see Appendix D) to comply with new laws and with BS7799. The Information Technology (IT) Services Division of the Council wanted to assess the risks that threaten their constituents' data to ensure that their ISP was compliant. This risk assessment, also referred to as a risk analysis, involved valuing their assets, evaluating the risks that threatened those assets, and specifying countermeasures to be taken to minimise the risks. The IT Division also wanted a gap analysis, which describes the path to be taken from their currently implemented countermeasures to those recommended by the risk analysis. Since the IT department is only one division of the Merton Council, our liaison was also

interested in studying the feasibility of conducting a similar risk and gap analysis for other departments of the Council. Our goals, as WPI consultants, were to complete the following three tasks:

1. A risk analysis of the IT Division's assets
2. A gap analysis of the IT Division's countermeasure procedures
3. A feasibility study of conducting the same analyses in other divisions of the Council

This project was important for Merton because they needed to evaluate their current ISP to ensure that it was compliant with these laws and with BS7799. The risk assessment and gap analysis that we performed will be used by the IT Division to implement their ISP throughout the Merton Council. The specific countermeasures that we identified will form the basis of the new policies. Although we did this research for the Merton Council, the knowledge gained can be used as a case study by other organisations conducting risk assessment exercises.

In order to gather information about the security of the IT assets, we conducted interviews. Since there were 55 divisional employees, we were not able to interview them all. First we interviewed the managers, followed by other employees that were recommended to us by the managers. The data collected from the interviews was entered into a software package called CRAMM (Central Government's Risk Analysis & Management Method.) CRAMM helped us create the risk and gap analyses. We kept a log of our actions in order to conduct the feasibility study.

Our project not only helped Merton assess its risks, but also it helped us realise how technology affects and is affected by society. With the introduction of computers, it has become more difficult for organisations to keep information secure. As more laws were passed to keep data and other information secure, organisations began changing their



structures in order to comply with the new laws. The connection between society (e.g. personal information) and technology (e.g. computers and data processing) forms the foundation of our project. Because of these ties, we feel that this project will not only serve the Borough of Merton, but also help prepare us for the tasks that we will undertake after graduation.

## **2. Background**

In order to assess the risks to the data stored by the IT Services Division of the Merton Council, we needed to have an understanding of three subjects: information security; recent legislative changes in Britain (including new standards,) and risk management. To aid us in our assessment, we also researched the WPI Banner system to use as a case study to which we could compare the IT Division.

### ***2.1 Merton Local Authority***

The Merton Council, also known as the Merton Local Authority, administers the Borough of Merton. The council has different responsibilities than the Central Government and the European Union. These include education, sanitation, taxes, street maintenance, open space maintenance, safety of the citizens, and social services of the borough. Because of all their responsibilities, the Council holds vast amounts of personal information about the citizens of Merton. The Council has the responsibility to keep the information secure, and readily available for individuals to obtain information about themselves.

#### **2.1.1 IT Services Division**

The IT Services Division of the Merton Council is primarily focused on supporting all information and communication needs for the Council. There are 55 employees divided into six functional groups within the IT Services Division. In 1998, the IT Division developed an Information Security Policy (ISP) to protect the data held by the Council. IT Services wanted to determine where changes in the policy should be made in order to reduce risks. The ISP that we assessed acts as a pilot for a policy that will be used in the future throughout the entire Merton Council.

The IT Division stores various types of information for Merton. However, there are other data stored by other departments of the authority, such as Social Services, Housing, and

Education. The information stored is personal and potentially sensitive data concerning citizens of Merton. For their benefit, it is imperative that the information remains secure regardless of who is responsible for it, even if the responsibility overlaps departments.

Applying the policy to the entire Merton Council will be worthwhile to the people of Merton because all of their personal information, from tax payments to educational records, will be secure.

## **2.1.2 Systems Studied**

### **Housing Rents and Repairs**

The Housing Rents and Repairs system consists of two databases. One manages rents, repairs, allocations to housing and vacancy in any properties present in the system. The other, smaller database contains lease-hold management data. Details of every property, personal information about each housing tenant, housing waiting lists, and repairs made to the property are recorded in the system. Most of the information stored is not of a sensitive nature. The system also keeps histories of tenants, rent amounts, and repairs. There are interfaces with the Financial Accounting system so that the payments may be recorded, and with the Housing Benefits system so that the correct amount of rent is charged for each property.

### **Housing Benefits**

The Housing Benefits system holds information on every citizen of Merton receiving housing benefits that help them pay their rent or council tax. Every aspect of every claim is included within the system. There is a lot of personal information stored, including insurance numbers, income, capital, date of birth, and other sensitive financial details. The system has interfaces with the Housing Rents and Repairs system and the Council Tax system so that housing benefits can be taken into consideration when rent or council tax bills are calculated.

## **Council Tax**

Council Tax is the local authorities' system for tracking and collecting property tax for the community. Each property designation and the information concerning it are stored as a separate record in the system's database. There are eight tax band levels, and each property is assigned a band level based on its size and cost. The Council Tax system is then able to determine a charge for each account. Additional discounts and benefits are then taken into consideration and figured into the final bill for each household.

## **Exchange Server and Outlook**

The Microsoft Exchange server provides the principal communications method within the Council, and particularly within the IT division. The server runs the program Outlook, which handles the email and personal calendar of each employee. Between 2000 and 2500 employees have accounts on Outlook, although about 150 people are still using MS Mail. This system is vital to the organisation, as the ease of communication it provides would be hard to replace with any other system.

## **Financial Accounting**

The Financial Accounting system keeps track of all fiscal information within the Council, including ledgers, accounts receivable, and accounts payable. The system has interfaces with Council Tax, Housing Benefits, Housing Rents and Repairs, the Cashier's Office, the Payroll system, and any other system that controls money entering or exiting the Council. Financial Accounting processes requests for these systems, but is not involved with their details. For example, when Council Tax needs to refund someone who has overpaid, Financial Accounting processes the refund without any knowledge of the reasons behind the refund.

## **Payroll Services**

The Payroll Services system is responsible for most human resources duties within the Council. The system stores a wide range of data concerning Council employees, including recruitment, job applications, training modules, employee training needs and history, absences, personal details, appraisals, disagreements, disciplinary actions, and a health and safety module. The program that provides this functionality is called PS Enterprise, and is provided by the contract company REBUS HR.

## **Cashier's Office**

The Cashier's Office is responsible for cash receipting, distributing receipts, reporting data and end of day cash and cheque balancing. Each council tax payer has a reference number and each transaction made in the cashier's office is tracked using a coding system. The system also stores which account the payment is going to as well as the type of payment that was received – cash, cheque, credit card or debit card. The cashier's office has interfaces with many of the other systems and many other departments because it is the only office through which money is collected by the Council, and there are many departments that issue bills payable to the Council.

## **SOSCIS (Social Service Client Index System)**

The Social Service Client Index System, or SOSCIS, stores information on the clients of the Merton Social Services department. The responsibilities of the system include maintaining the client index, assessments of the clients and proposals concerning the assessment of clients. The system also records basic information on high sensitivity groups. Under the current system, paper files store the details concerning any information that is sensitive. This system will soon be replaced with a new system called Care First, which will store all information electronically.

## **2.2 Information Security**

Information security (IS) involves protecting computer-related assets such as computers, networks, data, programs, and hardware components. IS has become increasingly important because the Internet allows a large number of unauthorised users around the world to potentially access and alter information (Schultz et al., 620). Information stored on computers can be deleted, changed, or stolen. There are three main security objectives: data integrity, confidentiality, and availability (Schultz et al., 628). Human factors play a large role in all three objectives. Merton is concerned about all three security issues.

### **2.2.1 Data integrity**

Information can be deleted or changed on a computer either by accident or on purpose. Information can also be deleted or changed while it is being sent over a network. Significant effort in information security is put into data integrity (Schultz et al., 629). Integrity also means that any data that is in a computer system or data that is being transmitted between computer systems are free from unauthorised modification (White et al., 2). Important records, such as Merton Council Tax records, can have a drastic impact if the records fall into the wrong hands. For that reason, it is vital that those types of records are only created, modified or deleted by authorised individuals in a carefully prescribed manner (White et al., 2).

One of the greatest problems with the digital world is that it is very easy to produce a forgery and it is difficult to verify the accuracy of anything (Schneier, 76). Fake essays as well as speeches are placed on the Internet at an alarming rate. Throughout human history, context has been used to verify the integrity of information. The electronic world has no context, therefore it is impossible to verify the integrity of information that is available electronically (Schneier, 76).

## 2.2.2 Data confidentiality

Data confidentiality entails making sure that sensitive or proprietary data is protected and not released to unauthorised people (Schultz et al., 630). It is a requirement that in order to ensure confidentiality, data in a computer system and data that are transmitted between computer systems is only revealed to authorised individuals (White et al., 2). Confidentiality does not only pertain to the content of the data. In some cases it may be important that the fact that a file exists is confidential. As an example, imagine a tenant in Merton receiving social service benefits. If his landlord is aware that he is receiving benefits, even if the landlord does not know how much, he may decide to raise the tenant's rent.

Data integrity prevents the unauthorised modification or deletion of data. Data confidentiality expands upon that to prevent the information from being disclosed to unauthorised entities (White et al., 145). There are two basic techniques that provide confidentiality. The first is to trust only entities in a well-defined *security domain*. The second is to hide important information through the use of *encryption* (White et al., 147).

A security domain consists of all hosts and resources, as well as the transmission medium that is used to connect them. These must abide by a formal security policy, which can assure a certain level of security. For a security domain to be effective, hosts in this domain place a level of trust in the other hosts and may thus provide selected services to trusted hosts which are not available to hosts that reside outside of the security domain (White et al., 147). The Merton IT Division is an example of a security domain.

When encryption is used, the information that is to be hidden is transformed from an understandable format to one that is unintelligible to anyone but the intended recipient (White et al., 147). Whenever a transmission has to leave the security domain it is currently in and travel to a different destination, encryption is used. Systems outside a person's security

domain may not always be trusted, so it is important to use encryption any time that information leaves that domain (White et al., 147-148).

### **2.2.3 Data availability**

Data may be deleted, making the data temporarily or permanently unavailable. The methods used to protect data availability are to implement back-up and fault tolerance procedures (Schultz et al., 630). The objective of availability requires that the authorised users of the system not be denied access when access is desired. This objective is also associated with the concept of denial of service. Denial of service is manifested by a reduction in system performance, and does not include normal degradation of the system performance during peak operating periods (White et al., 2). Merton is concerned with data availability, because they are required to be able to produce all information concerning an individual on request.

### **2.2.4 Human Factors**

Many complex security methods have been developed; however, if not installed or used properly, these methods may not accomplish the intended objectives. Most security-related controls rely on people to put them in place and people to follow them. The people following the security-related controls are generally the weak link in information security (Schultz et al., 621).

There are six aspects that are important when considering human factors in information security (Schneier, 256):

1. The perception of risks.
2. The way in which people deal with events that happen very rarely.
3. The problem of users trusting computer, and why that can be so dangerous.
4. The futility of asking people to make intelligent security decisions.



5. The danger of malicious insiders.
6. The danger of “Social engineering” and why it is so easy for an attacker to simply ask for secret information.

Most employees do not know how to accurately analyse risks to information security. They cannot look at vulnerability and make an intelligent decision about the consequences that may follow a poor decision. People overestimate risks that are out of their control or sensationalized in the media, but underestimate risks that are mundane and ordinary. Recognizing and analysing risk is a very important aspect of information security, and when a worker cannot properly do that, the human factor becomes relevant (Schultz et al., 622).

Computerized systems make mistakes so rarely that often people do not know how to deal with the errors that do occur (Schneier, 258). When an alarm condition does not appear frequently, employees do not know how to respond. Many attackers of information security systems target complacent users, so that when there is something strange happening with the computer or system, the user will not know how to respond and the human factor allows the attacker to be successful (Schneier, 259).

Computer users want security, but are often irritated by the inconveniences it may cause. Many times people want to get around security measures, such as passwords, because it makes their life much easier. Security is most effective, and creates fewest complacent users, when users have to interact with the security and make decisions based upon it. However, the users of a system do not want to see the security, and a smart security designer does not want users to see the security that is present on a system (Schneier, 261).

Many times, people do not have any idea of what a computer is doing when it is told to perform a function. There is no assurance that a computer has saved a file, or sent an email, and if it has been done that it was done correctly. Users simply trust computers, which

at times can be harmful. If a person trusts an insecure system with valuable information, it may be very easy for the wrong people to get their hands on that information (Schneier, 265).

There are many different types of malicious insiders. Before the Internet became wide-spread, the term malicious insider usually referred to a person who would steal money from a cash register at which he or she is working, steal blank credit cards, copy military secrets and spread them to enemies, as well as many other types of misdealing (Schneier, 265). Computer systems are particularly susceptible to insiders because there is so much insider knowledge. Auditors of security systems can deliberately overlook things just as a person who installs a firewall can leave a secret opening for themselves. The only way to prevent this human factor from leading to a breakdown in information security is to hire honest people and to have integrity screenings before hiring (Schneier, 266).

“Social engineering” is a hacker term that describes persuading other people to give out sensitive information by pretending to be on the inside (Schneier, 266). A hacker may call up a company pretending to be a network system administrator or security manager and by having some knowledge of the system may procure information such as passwords, or account names of employees so that cryptography, computer security, and network security are all bypassed. Human beings are trustful by nature, so it is very easy for social engineers to retrieve the information that they desire (Schneier, 268).

The human factor is one of the most important aspects of information security. At some point in the transformation of information from the source to the computer, it passes through a person, or people’s hands. The human factor is not only involved in that type of a situation, however; it applies to many other areas in network and information security as security measures are taken or not taken.

## **2.3 Legislative Changes**

Over the last 20 years, the rate of technological change in the field of computers has been rapidly increasing. To keep up with the changing technology, governments have drafted new legislation to ensure that people's rights are not abused by the power now wielded by the organisations that hold vast amounts of information. In particular, the government of Great Britain has drafted three important legal documents: the Data Protection Act (DPA) of 1998, the Human Rights Act (HRA) of 1998, and the Freedom of Information Act (FOI) of 2000. Also, the government has created a new standard for data processing based on these laws: BS7799. All of these had to be understood for us to properly assess the safety, security, and legality of any data processing system. More information on these can be found in Appendix B.

## **2.4 Risk Management**

Risk Management is the process by which an organisation attempts to minimise the cost of taking risks. Risk can be defined as uncertainty of outcome. A risk can have both a positive opportunity and/or a negative threat. Positive opportunity is defined as an expected benefit from taking the risk and negative threat is defined as the expected cost if the risk was realised (Chicken, 2).

Risk taking is inevitable in order to achieve corporate or organisational goals. Goals such as the ability to innovate and to implement electronic service delivery could not be accomplished without the organisation placing itself in some kind of risk (Adams, 4). Eventually, better risk management will allow organisations to perform at a higher level by contributing toward better service delivery, more effective management of change, better project management, supporting innovation, and many other areas of daily business (Draft Guidelines, 7). Because the Merton Council is in a relatively uncompetitive area of

operation, they are in a relatively low risk environment. This means that although there may be many risks the organisation might face, there are few that they will *have* to take in order to perform their functions (Adams, 76).

Implementing an information security policy is one way that an organisation can attempt to minimise the negative threats involved in risks (Eloff et al., 700). The success of the policy is dependent on a few aspects of its implementation. If the information security policy is implemented incorrectly or designed poorly, data thought to be secure may actually be in jeopardy. Another risk is that people might reject the new policies and choose not to follow them.

Our project's technical nature allowed us to focus directly on this area of risk management. In order to see the whole picture we had to be aware of how technical risks might directly affect the people or organisations involved (Neumann, 115). There has already been extensive research on the methods and policies for managing the risks that arise in the area of information security (Pounder et al., 607). Due to the multiple definitions for key terms used in this section we have included a glossary of terms [see Glossary].

### **2.4.1 Types of Risks**

Risk has multiple components. When attempting to identify certain risks they may fall under several key categories (Draft Guidelines, 6):

- strategic / commercial risks
- economic / financial / market risks
- legal and regulatory risks
- organisational management / human factors
- political / societal factors
- environmental factors / acts of god (force majeure)

- technical / operational / infrastructure risks

We focused primarily on the three types of risks that pertain directly to information security. They are legal risks, human factors, and technical or operational risks.

#### **2.4.1.1 Legal and Regulatory Risks**

There are countless regulations and laws faced by organisations. A majority of those regulations can be related to information security within the organisation (Hernon et al., 56). We have already outlined the legal regulations in regards to information security earlier in this chapter through the analysis of BS7799 and the Data Protection Act. The consequences of not following those regulations are severe. They could result in legal action being taken against the Borough of Merton and/or employees of the organisation. As long as the ISP that is developed and implemented minimises the other two types of risks, then legal risks should not be a problem. This is because the Merton government will have to follow the new standards and legislation in order to minimise the risks.

#### **2.4.1.2 Organisational Management/Human Factors**

Organisational management and human factor risks are those that might have a direct adverse effect on either the organisational structure or the individual employees of the organisation (Glendon, 291). These factors are most relevant to our project as we analysed the security and regulations concerning sensitive employee data or any collected private social information for residents of Merton.

Key human risk components can be identified in order to effectively classify a set of personnel factor risks. These components can include motivation, attitudes, perception, and behaviour (Glendon, 262).

Motivational human factor risks are any risks that will have a direct impact on specific personnel's motivational level. For example, the reduction of the annual Christmas

bonus at a local plant in order to cut costs could demonstrate a risk affecting the motivational level of employees (Chicken, 61). In order to maintain financial security the company must cut costs. However, in the process they may affect the motivational level of their employees. A similar potential threat that could arise is if employee raise/bonus information is not kept confidential. Co-workers might then become jealous of each other's salaries and lose motivation.

Attitude risks are those pertaining to the direct change or alteration of an individual's current attitude (Glendon, 70). For example, even if certain employees may have important technical skills, they must be able to effectively work with their fellow co-workers in order to be productive. Because of attitude risks, significant time and resources are spent to combine groups of employees into an effective operating unit. Certain information leaks or security breaks could cause employees to gain information that might bias their view of their fellow co-workers and alter their attitudes.

Perception is the process by which individuals gather information through the use of their senses in an attempt to evaluate their surroundings (Glendon, 102). Risk perception is when humans take this acquired information and apply it to their beliefs concerning certain threats or dangers. An example of this would be scanning the horizon and noticing clouds gathering. An individual would then take this acquired perception to mean that there was a risk of a rainstorm. However, because we are creatures of our environment we are very susceptible to bias that may alter our perception of risk.

In order to allow employees within the organisation to effectively gain appropriate risk perception, a concentrated attempt must be made to eliminate the operational biases to which they might be prone. This directly applies to our project in the sense that we had to assess the day-to-day activities of employees. Certain workers might be operating under the

assumption that the methods they use to process the data they collect are secure and reliable when in fact the exact opposite might be the case.

Personality conflicts are another major aspect of human risk. Many examples exist where major trouble has resulted due to key employee's differences in operational methods or philosophy. Differences might have an impact on the implementation of the information security policy in the sense that some employees might be more willing to adapt to a new process. Others might be far more opposed to change.

The last major area of human risk involves risks that might directly affect an individual's physical safety (Chicken, 73). In terms of information security this would be classified as a secondary risk (Neumann, 7) because no one can physically be harmed from stolen or lost information. That stolen or lost information could, however, be used against an individual. Stolen addresses, phone numbers, or critical medical information can all be used to harm someone physically. These risks are of particular concern to our project.

Even though a faulty or poorly implemented information security policy might not have a primary impact on an individual or employee directly, the risks involved are still substantial and need to be considered. Even though the loss of one telephone number might seem insignificant when looking at the big picture, if we keep in mind the subtle human factor risks behind the scenes we are able to see the importance of keeping that one telephone number safe and secure.

#### **2.4.1.3 Technical and Operational Risks**

Risks can affect all operating areas of the organisation. The types of risks that affect the technical or operational infrastructure of an organisation tend to be similar in nature (Neumann, 5). For example, in our project we face the potential risk of implementing too large a change to an organisational structure too quickly. The daily operations of a company

could be severely hindered by causing confusion among the staff, but could also impact the technical side of the organisation by allowing bad data to enter the system.

A risk would fall under the operational category if the threat it poses will have an adverse effect on the daily operations of an organisation. Through the process of developing and deploying the information security policy, Merton is already making an attempt to eliminate potential operational threats that it might face.

Technical risks are those that pose a threat to the technical components of an organisation. Automatically we think of computers, but in reality affected equipment can be anything from a computer to a copy machine to a complicated automated bottling system. However, we focused on computers and information system related risks for our project.

These risks could impact the following areas:

- Data Integrity
- Data Confidentiality
- Data Availability
- Human Factors

## **2.4.2 Risk Management Types**

There are two primary types of risk management, quantitative and qualitative (Nosworthy, 599). Both focus on the process of identifying risks, and assigning value to specific risks in an attempt to identify and stop potential threats from taking place. In the past organisations had been primarily reactionary, only dealing with threats after they arose, and then taking steps to ensure the problems didn't arise again in the future.

### **2.4.2.1 Quantitative Risk Analysis**

Quantitative risk analysis is a mathematical approach to performing risk analysis (Nosworthy, 599). It consists largely of organisations developing complicated mathematical



models in order to achieve an acceptable level of risk by manually calculating the frequency of a threat occurring. Risk solutions are then calculated using these probabilities. This numerical data can then be applied to such things as corporate insurance to protect high-risk company equipment or personnel. This type of risk management is also rather time consuming and can be costly; however quantitative risk analysis is very effective. CRAMM software allowed us to perform a quantitative risk analysis.

#### **2.4.2.2 Qualitative Risk Analysis**

Qualitative risk analysis is another form of risk analysis, and in general is far simpler than the quantitative process (Nosworthy, 602). It involves a more subjective approach that involves assigning a ranking to specific threats (i.e. high/medium/low or 1-10). This ranking is based on the knowledge, judgement of the people that are doing the judging as well as the severity and point of impact of the risk in question. It then becomes important to document the judgment criteria so that it can be applied fairly to all threats that are analysed.

Since the qualitative risk analysis approach does not involve complex and difficult algorithms it is the most widely used method for analysing risk (Pounder et al., 600). A case can be made that in the quantitative approach the initial algorithm defined is inherently based on subjective interpretations of risk and because of this is no more accurate than a qualitative approach. The only flaw in the qualitative analysis approach is that it lacks the ability to control the criteria upon which judgement is based. With quantitative analysis, judgement is based solely on the algorithm and because of this it is far easier to maintain consistency through the analysis (Trompeter et al., 385).

#### **2.4.2.3 Gap Analysis**

One area that we evaluated in our pilot program was gap analysis. Gap analysis concerns evaluating and improving information security. A gap is an opening – it is the

space between where an organisation is and where the organisation wants to be (Family Business Institute). For our project, a gap was a space in or problem with information security. We needed to figure out what the problem was and to come up with a solution to remedy the problem.

### **2.4.3 Risk Levels**

In our attempt to assign value to certain threats we realised the importance of considering risk in varying levels of importance. Through this assumption we were able to determine that risks must be managed at four primary levels of organisational operation: corporate/strategy, programme, project, and operational risk (Draft Guidelines, 11).

As shown in previous sections, risks can sometimes be hard to classify and might fall under one or several categories. Risks can also sometimes fall between the four primary levels outlined. In certain cases it is important to determine when the specific risks need to be changed from one level to another as the quantitative value assigned to them might shift (Pounder et al., 601). Threats associated with information security can have impacts on all four levels of the organisation.

#### **2.4.3.1 Corporate/Strategy**

Managing risk at the strategic level is concerned with setting a specific strategic direction and balancing potential opportunity against cost and risks (Draft Guidelines, 26). In general, risks at this level occur less frequently than at the other levels. Risks at this level threaten the direction of the company. Some types of risks typically found at this level are commercial, financial, cultural, and political threats. Programme, project, and operations risks may be escalated to this level if and when they exceed certain tolerances (Neumann, 19).

### **2.4.3.2 Programme**

Risks impacting at the programme level of operation will have effects on management's ability to turn high level strategy into new ways of conducting business (Adams, 84). These new methods hopefully will provide benefit to the organisation in some fashion. Threats having to do with acquisition, projects, security, safety, and business continuity will typically affect this level of operation. In terms of information security, risks associated with security of data or data integrity might link to this level of operation (Draft Guidelines, 19). Risks from the project and operation level may escalate to this level when they exceed the specific stipulations set forth.

### **2.4.3.3 Project**

Risks at the project level of operation focus on keeping unwanted outcomes to the smallest magnitude possible. Risks at this level are extremely important to manage for government organizations because these risks usually have to do with threats concerning personal, technical, cost, and scheduling risks (Draft Guidelines, 21).

### **2.4.3.4 Operations**

The operations level of business is primarily concerned with business continuity and the daily practices an organisation might use. Frequently, an organisation might have outside companies that shares risks at this level of operation (Draft Guidelines, 23). Types of threats that usually impact at this level are those that pertain to quality, provider failure, operational support, and environmental issues (Nosworthy, 607).

## **2.4.4 Risk Management Framework**

Now that we have discussed ways to identify and classify risks it is important to develop a method for applying the same criteria to all aspects of the organisation. In order to

do this we must develop a risk management framework that lays out organisational standards for the management of risk (Chicken, 143). In other words, a framework is needed to set the overall context through which risks can be managed and evaluated. The typical elements for a risk management framework are:

- establishing an organisations risk policy
- identifying the main stakeholders
- clarifying all objectives
- defining the main approaches for identifying risks; assessing risks and reporting them; and then taking actions to deal with them
- defining responsibilities for managing risk and reporting to senior management
- establishing quality assurance (QA) arrangements to ensure that risk management reflects current good practice.

It is important to note that risk management is an iterative process, as shown in Figure 2-1 (Draft Guidelines, 8).



**Figure 2-1: Iterative Risk Management Cycle**

## **2.5 Case Study – WPI Banner System**

In order to gain a better understanding of information security policies and how they apply to real world situations, we conducted a case study of Worcester Polytechnic Institute to determine the specific methods used to secure information. This case study included the technical security aspects of WPI’s information storage and management systems. We decided to focus on the Banner enterprise resource and planning system that WPI utilizes because it is the primary system that houses the organisation’s mission critical data.

To learn more about the WPI information security policy, we conducted three interviews with key personnel. Josh Brandt, a UNIX systems administrator at WPI, gave us a working knowledge of the technical aspects of information security and how those aspects

ted in with the information systems that WPI utilizes. We interviewed David Everett, Associate Director of Human Resources, to determine some of the actual information security policies that are used by WPI. By learning some of these policies, we became familiar with what is done to keep employee data confidential and secure. Finally, we interviewed Ben Thompson, Director of Computing Services at WPI and focused specifically on the Banner ERP system. In this interview we also discussed general information security procedures used by WPI as a whole in regards to its electronic data. The summaries for these interviews can be found in Appendix O.

We determined from the interview with Josh Brandt that WPI only uses two primary information systems to store and display organizational data. There is an online White Pages system that displays a person's name and contact information. Also stored within this system are year of graduation and social security number of every WPI student. This system has varying levels of security access. The account on which the user logs in determines how much information the user is able to view. The White Pages system also runs from a lightweight database application or LDAP for short, which is able to encrypt data using a complex encryption scheme known as KERBEROS. This encryption method was developed at MIT and basically allows for the transfer of sensitive data online.

The other major system used by WPI to store and manage information is the Banner Enterprise Resource and Planning (ERP) system. This is a full ERP system developed for educational organizations. It stores everything from student grades to employee salary information. Because of this sensitive data, there are a vast number of technical security aspects utilized in an attempt to secure the data. Some of the methods used are multi-layer encryption, specific security level definitions, and explicit roles within the security levels. Even the physical layout of the network is set up in a manner such that sensitive administration computers are located on different network segments. This measure

guarantees that people cannot easily monitor the transfer of data to and from these sensitive computers.

Through our discussions we were able to determine that WPI does not have an explicitly written ISP. However, WPI does follow the Family Educational Rights and Privacy Act (FERPA) very closely. It uses this document to define who can have access to specific information, and to determine how sensitive data must be kept confidential. Some specific examples of this would be if a potential employer called looking for a student's ID number or mail address, WPI would not give out that information. Despite the fact that they cannot directly give the information to the potential employer, WPI might refer the caller directly to the student. The institute also extends FERPA to protect employee and alumni data although the act only specifically relates to student information.

Because WPI is a private institution, it is subject to relatively fewer governmental regulations on how it must store and maintain the data that it collects. For this reason WPI is self regulating in terms of securing its information. In terms of legal issues, WPI requires a warrant from all police organisations in order to release personal information. All of the policies and security measures which we encountered were helpful to us although they were not specifically tailored to government organisations.

Through our case study at WPI, we were able to determine how information security impacts real world organisations. We were able to draw upon this data to apply the policies we learned about to the IT Services Division of the Merton Council.

### **3. Methodology**

Our project team used three methods to create our risk assessment and gap analysis for the IT Services Division of the Chief Executive's Department of the Merton Local Authority. Two of our methods, interviews and group interviews, were used to collect information from some of the 55 employees of the IT Division. We were most interested in gathering information on the assets of the division and the risks that threaten those assets. The third method was to use CRAMM software to create a risk analysis and a gap analysis. The data that we collected from the interviews and group interviews provided the basis for these analyses. Our schedule for completing these tasks is included in Appendix R.

#### **3.1 Scope**

It is vital to define the scope of any project that one is undertaking. Scope refers to the area that is covered in a project, and the boundaries in which it must remain. If the scope of a project becomes too large and the boundaries are too wide, the project has a greater chance of failing. We scheduled weekly meetings with our liaison to review the scope.

We initially defined our project to include the entire IT Division of the Merton Council. Upon beginning the project, we realised that we would not be able to accomplish our goals unless the scope was changed. We were given a list of about fifty systems, all of which are used in the Council. Since it was not feasible for us to conduct a risk assessment of every system, we narrowed our scope to seven systems. Systems and Projects Manager Steve Lawrenson helped us with this process by telling us which systems are most valuable to the Council. We changed the scope to include risks to the entire division, not simply the seven systems. Those risks had already been determined by the division and included: network logon / loss, password control, server backups and adding an alternate machine room. Since



we initially defined the scope of our project and maintained it throughout our time in Merton, we were able to follow correct project methodologies.

## **3.2 Interviews**

Our main method of collecting information for our risk and gap analyses was through interviews with senior users of the eight systems we considered as well as employees within the IT Division.

### **3.2.1 General Interviewing Information**

When we interviewed the employees, we worked in teams of two. One person asked the questions and interacted with the interviewee. The second person took notes on a laptop, and later edited them to create the summary of the interview. This was the system used throughout the interview process. In some cases, it was useful for two people to take notes so that they could be compared for accuracy. Every interviewee was documented in the bibliography. The summaries of the interviews can be found in Appendix P.

While conducting the interviews, it was important to remain professional and confident, since we needed the trust of the employees with whom we were working and interviewing. Many of the employees have been working for Merton's IT Services for over 10 years, so they may have been reluctant to trust students with far less experience. We tried to make discussions seem natural so that the interviewee felt comfortable and would be willing to share information necessary for our analysis. It was not difficult to become comfortable with the interviewees because we worked with them every day.

At the completion of each interview, we asked interviewees if we could include a summary in an appendix of our report. We also asked if we could reference their name throughout the report. We did that to ensure that the employee was aware of our intentions

and approved of them. In all cases, the interviewee was very willing to help us in any manner possible.

### **3.2.2 Interviews Conducted**

We first identified the employees that should be interviewed; we were most interested in interviewing the managers of each system and a senior user from the client department for applicable systems. We used the list of employees, job titles, and functional groups along with the organisational chart of the IT Services Division to determine which employees were managers, administrators, programmers, or engineers. Our first interview was with Steve Lawrenson, Systems and Projects Manager. He told us which systems we should focus on. Four weeks into the project another system was added because the managers of the system heard of what we were doing and were curious about what risks were present within their system. There were seven systems that Steve Lawrenson suggested we concentrate our assessment on, so by adding one more we had a total of eight systems on which to concentrate:

1. Council Tax
2. Housing Benefits
3. Payroll (PS Enterprise)
4. Cashier's Office
5. Financial Accounting
6. Housing Rents and Repairs
7. Outlook / Exchange
8. Social Services Client Index System (SOSCIS)

He also provided us with a list of employees that we should interview, including people in the IT Division and in the client department. Based upon that information, we set up interviews with the manager of each system and a senior user of each system.

The semi-standard interviews contained questions pertaining to the assets and threats of each system we were investigating. Some of the questions that we asked each employee interviewed were:

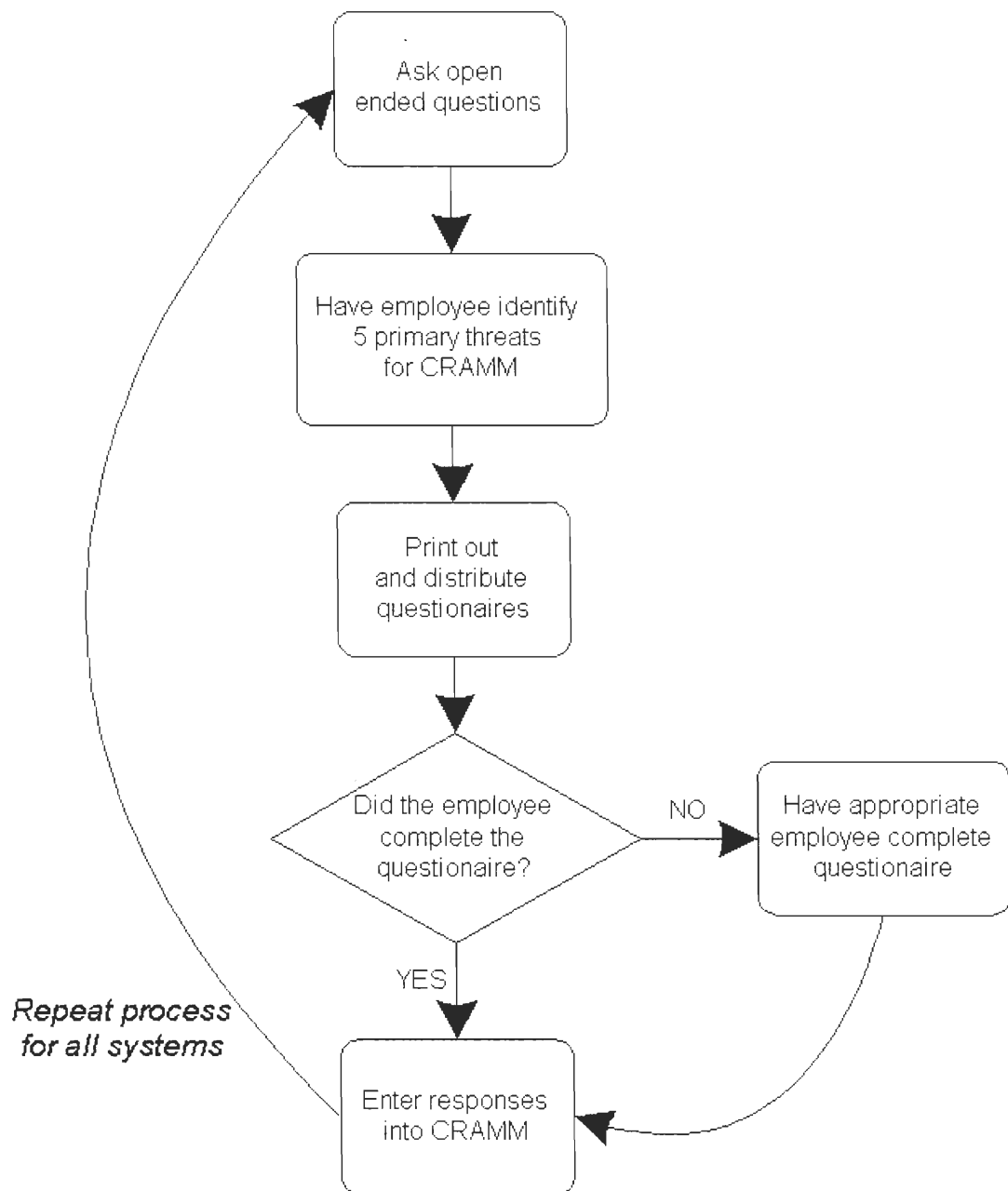
1. What responsibilities does the system in question have?
2. What types of data does the system need?
3. Is that data shared with any other systems?
4. What control mechanisms are in place for information security?
5. Who are the main users of the system?
6. What types of access do they have?

After asking those questions, we gave each employee that we interviewed a list of 38 threats (Appendix H) that came from the CRAMM software. We asked that employee to identify the five or six most prevalent threats to their specific system. Once identified, we printed questionnaires for each threat from CRAMM. A sample CRAMM questionnaire can be found in Appendix I. They were designed to quantify the threats and vulnerabilities to the system in question. Each questionnaire consisted of two parts. The first part asked the employee about the danger of the threat that was identified. The second part asked how vulnerable the system was to the threat in question.

Once the questionnaire was completed, the employee returned it, and we entered the answers into the CRAMM software. CRAMM analysed each questionnaire based upon how dangerous the employee felt the threat was to the system and how vulnerable the system was to that threat. Through that analysis, CRAMM assigned a risk level and impact level to the system based on what would happen if the threat occurred.

Some of the employees could not accurately answer some of the questions, so if that was the case an expert was referred to us by the employee completing the questionnaires. Also, if two interviewees for the same system identified the same threat, we used the answers

from the employee whose job gave them more experience with that particular threat. Figure 3-1 summarizes the data gathering process that we used.



**Figure 3-1: Data Gathering Process**

Around the same time we were interviewing Steve Lawrenson, we were collecting information on the assets of the IT Division. Those assets include physical, data and system assets and are described in more detail in Chapter 4, *Data*. We set up an interview with Paul Biggs, Infrastructure Manager, who was able to provide us with all of the information we

needed about servers and other physical assets. The servers are the majority of the physical assets, and we needed to know which servers were used for the various systems in which we were interested. After we interviewed Paul Biggs, we began interviewing the manager and senior user of each system.

### ***3.3 Group Interviews***

Group interviews were our secondary method for gathering information. We conducted two group interviews to gather information from the people who use the network. We needed information concerning network access and security from people who used it on a daily basis. Although we collected information from previous interviews that described how network access is supposed to be restricted, it was important to ensure that the policies were working. We had two sessions with different sections of the IT Division. One was with the Systems and Projects section and the other was with the Desktop Support Group. Through those two sessions, we were able to identify some of the problems that the employees of the IT Division face daily.

The process of identifying which employees to invite each group interview was quite simple. We contacted Steve Lawrenson, Systems and Projects Manager and Richard Warren, Service Delivery Manager. We asked them each to identify approximately five employees who they would allow us to meet with and a good time for us to meet. They were able to easily work that into their schedules, so the process was completed quite readily.

We utilized several key strategies in the process of setting up our group interviews. We focused on detailed in-depth information from the participants. Since we had interviewed many of the employees in the IT Division, we made an attempt to elicit a creative and open-ended discussion at the group interview session. We also made sure that all of the participants were aware ahead of time of the group interview process.

We laid out a guide for conducting the session specifically tailored to the personnel that participated in the group interview and the information we wished to acquire. We did this by setting up a series of short answer questions that could be addressed by the members individually or together.

We specified a group moderator whose primary functions were to keep control and keep discussion flowing. This person was responsible for the introductions and introductory activities. He was also responsible for dealing with any sensitive issues that arose. We restated the rules and guidelines for the session. The moderator stepped through the short question and answer section of the process. The entire team was aware of the procedure so that if the moderator began to falter one of the note takers or the pure observers would be able to interject and help to continue the flow of discussion.

There were two note takers present at the session in order to fully capture all information. Also, we were able to utilize a fourth group member as an outside observer and partial moderator in order to help maintain control.

Our findings were then sent to the participants so that they had a chance to review the information and verify that all acquired data were accurate. The participants in each group interview are listed in the Bibliography and the minutes from each session can be found in Appendix P.

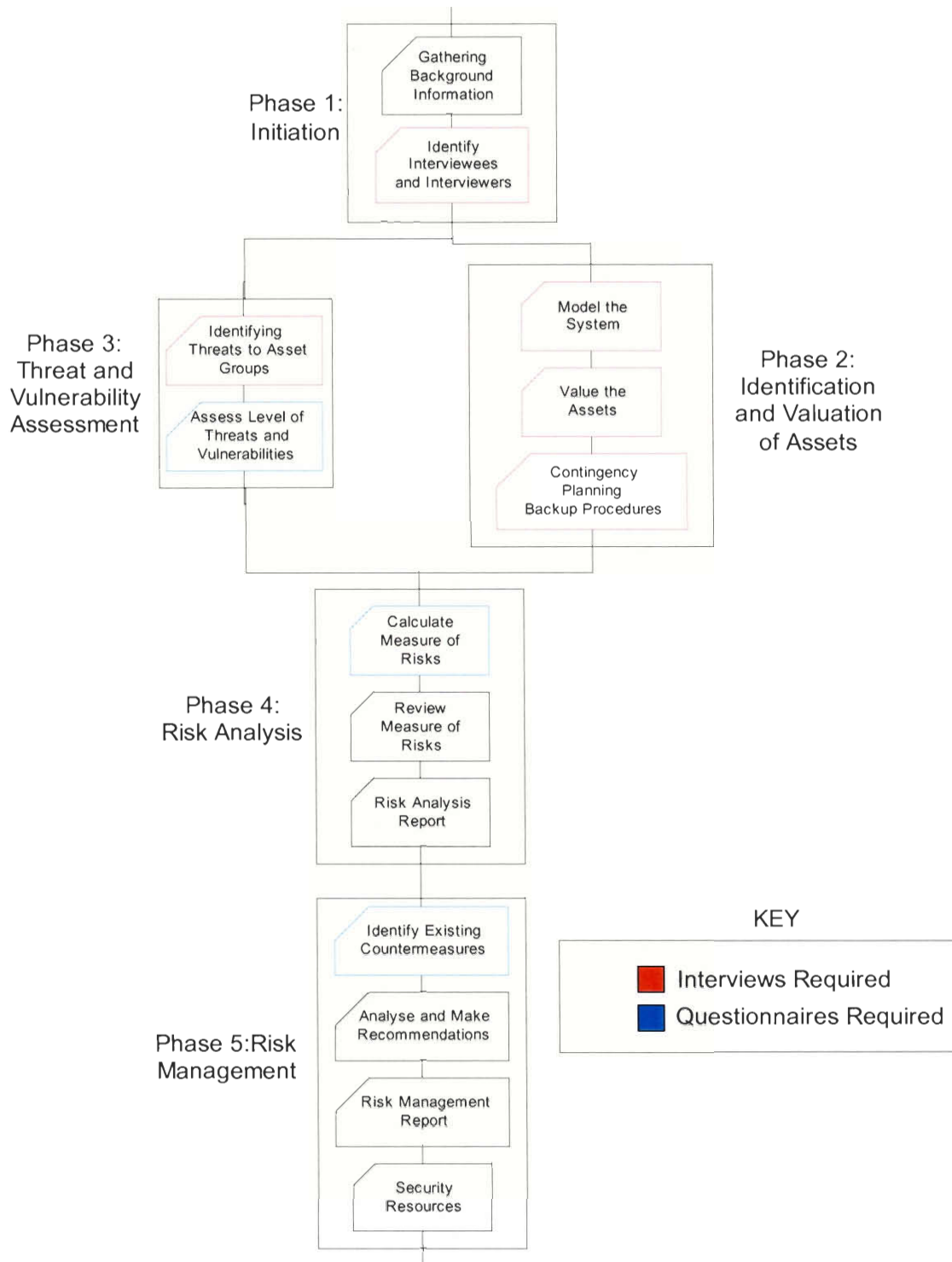
### **3.4 CRAMM Software**

CRAMM is the Central Government's preferred Risk Analysis and Management Method and is used throughout Britain and in many other countries. The CRAMM method of conducting risk analyses is divided into three stages. The first stage involves assigning values to all assets of an organisation. The second stage involves collecting information concerning the threats to the assets from the first stage. The third stage is concerned with

selecting the proper countermeasures and controls to be implemented in order to minimise the risks.

To facilitate risk management exercises, Central Government created a software package based on the CRAMM standard of risk analysis. We used the software for two reasons: it is a thorough and quantitative risk analysis method whose wide acceptance throughout Europe demonstrates its quality, and its use complies with British standards for risk management exercises.

When the software was written it was divided into five phases, rather than three stages, and the phases were further split into a series of data collection and analysis operations. A flow chart depicting these phases and operations can be found in Figure 3-2. The outer boxes represent phases, while the inner boxes represent operations. For a more detailed explanation of these processes, see Appendix C.



**Figure 3-2: CRAMM Methodology Flowchart**



## **3.5 Data Collection**

We needed to collect data on three topics: the assets of the IT Division, the threats to those assets, and the countermeasures currently implemented. This information is required for the risk and gap analyses.

### **3.5.1 Assets**

There were two key methods that we used to enumerate and value the assets; analysing the lists of assets that had been previously compiled within the IT Division, and interviewing managers who had knowledge of the assets of the IT Division. Physical and system assets were given to us on several asset registers; we conducted interviews to obtain information concerning the data assets.

The values of the assets were determined by examining the impact on the IT Division if that particular asset were lost. The relationship between two assets describes the dependence of one asset on the other. An example of a relationship would be the dependence of the data in a personal computer (PC) on the proper working of the PC. If the PC, a physical asset, fails and there is no backup system, the organisation would also lose the data stored on the PC, a data asset.

### **3.5.2 Threats**

Once the assets, their values, and the relationships among them were entered into the CRAMM software the next step involved investigating the threats to and vulnerabilities of the system. The software had a list of the various threats that could potentially affect the organisation. Each threat was associated with a list of questions within the software. We asked each employee to identify which threats would be most harmful to their system. From those threats we printed a questionnaire from CRAMM for them to complete. The answers to

these questions were entered directly into the software, which then compared the threats to the assets in order to calculate the risks to the system.

### **3.6 Data Analysis**

After the information concerning threats and assets was collected, it was entered into the CRAMM software and analysed. The first step was to run a risk analysis, in which CRAMM assigned risk levels to the threats, and looked at the controls that could be implemented to minimise those risks. The second step was to perform a gap analysis, in which we compared those controls to the countermeasures that were currently being implemented throughout the division.

#### **3.6.1 Risk Analysis**

After we completed our data collection, the CRAMM software evaluated the risk levels and identified the countermeasures that could be used. We then compared the controls supplied to us by the software with the controls currently being used in order to determine areas of weakness and areas of overlapping controls.

With the list of countermeasures or controls, we used the software to determine which controls would be most useful. We prioritised the countermeasures and described the best ways to implement those countermeasures to the IT Division.

#### **3.6.2 Gap Analysis**

A gap analysis document discusses three key topics. The first is a description of where the organisation currently stands. For the Merton IT Services, we stated the countermeasures that were currently in use. The second part of the gap analysis is a description of where an organisation would ideally like to be, with all its current problems solved. In this section, we described the countermeasures that were suggested by the

CRAMM software. These countermeasures would manage the identified risks most effectively. The final section of the analysis describes a path by which an organisation can bridge the gap between their current status and the status that they wish to achieve. We have described the countermeasures offered by the software and not currently implemented, and how they can be used effectively within the division. To see the results of the gap analysis, see section 5.2.

### ***3.7 Project Management Database***

We used an Access database as a log to record any problems we encountered as well as details of all meetings and interviews held. This log allowed us to identify the problems, classify them at a certain level, recognise methods to reduce or remove them, and set a date for them to be resolved by. Through the use of the log, we were able to stay on task and complete our project on time. The meeting and interview recordings section of the database was necessary to complete our goal of doing a feasibility study for a risk assessment exercise for the entire Merton Local Authority. By recording how much time each meeting and interview lasted, as well as the substance of the contact, we were able to determine whether or not a risk assessment of the Council would be feasible.

## **4. Data**

There were two types of data collected while we were studying the systems: assets of the IT Division and threats to those assets. Assets of the IT Division included the Physical Assets, Data Assets, and End User Services. Information on the assets was important in assigning values to each system. Data collected on the threats to the assets of the IT Division and the vulnerabilities of the Division to those threats were important in determining the level of risk to each system. [See the Glossary for a definition of assets and threats.]

### ***4.1 Assets Identified***

One objective of our interviews was to learn about the assets of each system. Every system has server(s), workstations, miscellaneous equipment, stored information, software applications, and end user services provided to the public or other systems. Each is valuable and must be identified to accurately assess the risks to the system. Assets are divided up into different categories; the assets we explored were physical, data, and end user services.

#### **4.1.1 Physical Assets**

A physical asset is a piece of property important to a system. We identified three primary types of equipment throughout our assessment: servers and host PCs, workstations, and miscellaneous equipment. Each server is either a Mainframe system, a UNIX system, or a Windows NT system. These servers range in cost from a flat fee of £30,000 for one of the NT servers to a yearly cost of £800,000 for the ICL VME mainframe server. The VME mainframe hosts Council Tax, Housing Benefits, and SOSCIS; it is the oldest server still in use by the Council.

There are two servers that use a UNIX operating system. One of these, called ThreshLive hosts the Housing Rents and Repairs system. This server uses a version of UNIX known as ICLUNS, which is an older UNIX operating system. The approximate cost of this

server is £100,000. The other UNIX server is the Sequent IBM UNIX server running the Financial Accounting system; it costs £100,000 to install and was upgraded six months ago.

There are five NT servers: one PS Enterprise (Payroll) server, one Cashiers Office server, and three Exchange/Outlook servers. The approximate replacement cost for each of these is £30,000.

Another type of physical asset is the personal workstation. The departments using the systems operate on a variety of workstations of different ages and costs. When assessing workstations, we assumed a one-to-one ratio between workstations and employees. There might be some overlap because some users have access to multiple systems, hence reducing the total number of workstations. However, overlap should be minimal, and because the cost of the servers is far greater than that of a few workstations, this approximation did not affect our analysis.

The workstations were primarily Dell computers configured with Microsoft Windows NT. We estimated an individual workstation replacement cost of £800, including a monitor and peripherals. The number, type, and cost for the IT division's workstations that we considered were significantly more accurate than those of other departments because we had direct access to that information. This workstation information was primarily used in our evaluation of the Microsoft Exchange email system.

There are two pieces of miscellaneous equipment that affect all of the systems: the air conditioning unit and the central UPS unit. The air conditioning unit is responsible for maintaining a constant temperature throughout the computer room. The UPS is responsible for maintaining a constant power source to all of the servers, as well as handling the safe shutdown of all servers in the event of a power loss. The replacement cost of the UPS is £45,000. The only other systems with additional miscellaneous equipment besides standard printers are the Council Tax and Housing Benefits systems.

Council Tax utilizes two additional servers to handle form generation and printing called REDTITAN and FUNASSETT, which queue necessary files before sending them off to the two Xerox Laser Printers. The two servers have a replacement cost of around £1,500 each, and the two printers cost around £40,000 each.

Finally there is a document imaging system for both the Housing Benefits and Council Tax systems. This system is responsible for scanning in and then storing important financial documents for the two systems as a means of backup. A scanner and NT Server with two 8-gigabyte optical disk drives make up the system. The entire system resides on the second floor, and has an estimated value of £100,000.

### **4.1.2 Data Assets**

A data asset is defined as a collection of information significant to the system. We identified the specific data assets for each system, and the types of data that they hold. For some systems we also looked at specific data fields that are stored.

The Council Tax system utilizes an IDMS database to store all of its crucial records. Much like a majority of other systems the Authority has, Council Tax makes use of a development and production database scheme. The system has two databases configured in exactly the same way. The production database is the normal operational database where day-to-day updates are made. This in turn updates the development database that exists for IT to make changes to and test the system without bringing it down. The development region also serves as a backup for the production and can be brought online if problems arise.

Council Tax stores records by property and attaches people to those records. It can then generate bills by property for the owners of each property. The system stores very little personal financial data. It stores name, address, phone number, what each individual owes, and account balance.

The Housing Benefits system also utilizes the development/production database scheme. Unlike Council Tax, which distributes tax bills uniformly according to banding levels, Housing Benefits assess benefit distribution on a case by case basis. In order to do this, the system must store sensitive personal and financial data. Data fields such as name, address, date of birth, insurance numbers, income, capital, and other personal information are all included. Details of how much rent tenants actually pay and aspects of the individual claims are also stored.

Housing Rents and Repairs (HRR) uses two mirror-image 8 gigabyte INGRIS databases to store its information. HRR stores a large variety of data because it has a many different functions, including information concerning properties, tenancy history, current rents, rent history, and repair history. The information is so detailed that it even stores the location of toilets within the properties for repair purposes.

The Cashier's Office system utilizes a SQL server database to store its primary data. Each transaction that occurs is referenced against a specific code in the database which relates to a person's specific reference or account number. The Cashier's Office tracks daily transactions and stores all information vital to those transactions, including amount, method of payment, and account balance.

The Payroll System (PS Enterprise), like the Cashier's Office system, uses a SQL Server database to store its data. PS Enterprise is a full human resources tool and has modules for recruitment, job applications, training, employee history, payroll, and attendance. It will track and store all the data necessary for these modules, and much of that is sensitive employee data.

Financial Accounting (FMIS) tracks fiscal information within the Authority. It keeps a ledger of accounts receivable and accounts payable. In this system, personal information for employees is not tracked; however, there are some personal data stored for residents if

they collect either housing or social benefits. The system holds names and addresses of businesses inside and outside of the Borough. FMIS uses an INGRIS database much like the Housing Rents and Repairs; however, it has three database regions for additional security. It maintains live, test, and development regions.

The Social Service Client Index (SOSCIS) holds detailed personal information on people to whom social services are targeted. It is on a mainframe and therefore utilizes a proprietary IDMS database very similar to Council Tax and Housing Benefits. However, there is significantly more sensitive and personal data stored within this system. It tracks name, address, client grouping, ethnicity, date of birth, date of referral, problems that arose, assessments, who did the assessments, and basic notes.

The Microsoft Exchange system is distinct from the other systems that we examined with regard to data assets. It stores very little information in its database. The Council only requires it to hold the users' names, emails, and phone numbers. Whatever additional information that might be stored would have to be specified directly by the user. This includes job title, fax number, or home phone number. There are three concurrent versions of this data stored across three servers to maintain system reliability.

### ***4.1.3 End User Services***

The services that a system of the Council provides to the public, other parts of the Council, or outside organisations, are called end user services. All other assets, including data and physical assets, are required by a system so that it can provide these services. Table 4-1, a report from the CRAMM software, lists and describes the end user resources of each system. Financial Accounting has two end user services, while every other system only has one.



**Table 4-1: End User Services**

<i>End User Service</i>	<i>System</i>	<i>Description</i>
Benefit Distribution	Housing Benefits	Prints checks for benefit recipients three times a week
Financial Tracking	Financial Accounting	Tracks fiscal information within the Council, ledgers, accounts receivable, and accounts payable, for inquiry purposes
Human Resources	Payroll	Keeps track of all information concerning Council employees pertinent to Merton
Microsoft Outlook	Outlook/Exchange	Inter-office email, personal schedules, room and meeting booking
Money Collection	Cashier's Office	Collects and keeps track of all money entering the Council
Property Tracking	Housing Rents and Repairs	Keeps track of rents paid and repairs needed to Council house properties
Refunds	Financial Accounting	Processes refunds for Council Tax and other systems
Social Services Client Tracking	SOSCIS	Keeps track of the index of social service clients
Tax Collection	Council Tax	Collects Council Tax, or property tax, from the constituents of Merton

#### **4.1.4 Asset Reports**

Once all of the information concerning the assets was entered into CRAMM, we generated reports for each of the different types of assets, including physical, data, and software valuation reports. Appendix E, the Physical Asset Valuation Report, lists all of the physical assets that we studied and a brief description of each. It then gives a scalar value of the asset from one to ten. The highest value asset in our review was the ICL VME mainframe which, came in at a five. The last column of this report states the approximate replacement cost for each asset. The assets are the subtalled by category and a total physical asset replacement cost is listed at the bottom.

Appendix F, the Data Asset Valuation Report, details the importance of the data for each system. The first column of the report is an impact statement that describes the potential problem (i.e. Unavailable for 15 minutes.) The next statement is a guideline for how the business could be affected (i.e. Disruption to activities.) The last field is a scale measure of the potential impact on the business, which ranges from one to seven.

The final asset report is the Software Asset Valuation Report (Appendix G), and this uses a somewhat similar approach to valuation as the data asset report. The report also details the type of each software package and gives a rough annual fee for the package. This combined with the impact, guideline, and scale value would then give us the overall valuation for each of the software assets.

## **4.2 Threats**

The second objective of our interviews was to identify the threats that were present to each system. CRAMM software provided us with a list of 38 threats that ranged from technical failure of host or network service to fire. The full list can be found in Appendix H. Once the interviewees identified the threats, we printed a CRAMM questionnaire concerning those threats, and the vulnerabilities to the organisation based upon those threats.

Out of all the potential threats identified by CRAMM, there were 10 threats that were not identified by any interviewees. There were many identified by one or two of the interviewees and only seven identified by more than two employees. Those identified by only one or two employees were still considered, and some pose more of a danger than those identified more often. If a threat was identified multiple times, it is regarded as a common threat, although not necessarily a dangerous threat. The threats identified by each interviewee can be found in Appendix J. Based on analysis by the CRAMM software, it was found that some of the recurring threats were less dangerous than ones that were identified fewer times. However, the number of occurrences of the commonly identified threats in the

Council was more frequent than some of the more dangerous ones; hence making them of greater concern to the employees.

#### 4.2.1 Threats to Specific Systems

In this section, the threats that were most frequently identified by interviewees as well as the threats that were determined to be the most dangerous by CRAMM are described.

Through the use of an Excel worksheet we were able to track each threat that was identified, how many times that threat was identified, and by which systems it was identified. Based upon the threats that appeared most frequently, we were able to determine which threats intimidated the employees the most, and which systems were at risk to certain types of threats. The worksheet used to keep track of that information is shown in Table 4-2.

**Table 4-2: Threats, number of times identified, and systems identifying those threats**

Threat	#	Systems
Technical Failure of Host	5	Council Tax, Financial Accounting, Housing Rents and Repairs (2), Payroll
Application Software Failure	5	Financial Accounting, SOSCIS, Payroll, Housing Rents and Repairs, Housing Benefits
System and Network Software Failure	5	Cashier's Office, Housing Rents and Repairs, SOSCIS, Housing Benefits (2)
User Error	3	Council Tax, Financial Accounting, Payroll
Staff Shortage	3	Council Tax (2), Payroll
Hardware Maintenance Error	3	Council Tax (2), Housing Benefits
Technical Failure of Network Service	3	Housing Rents and Repairs (2), Housing Benefits
Introduction of Damaging or Disruptive Software	2	Cashier's Office, Housing Rents and Repairs
Air Conditioning Failure	2	Council Tax (2)
Software Maintenance Error	2	Council Tax, Payroll
Communications Failure	2	Council Tax, Housing Rents and Repairs
Power Failure	2	Financial Accounting, Housing Rents and Repairs
Misuse of System Resources	2	Exchange, Housing Rents and Repairs
Theft by Outsiders	2	Cashier's Office, Exchange
Fire	2	Cashier's Office, SOSCIS
Technical Failure of Storage Facility	2	SOSCIS, Housing Benefits
Operations Error	2	Council Tax, Housing Benefits
Unauthorised Use of an Application	2	Financial Accounting, Housing Benefits
Masquerading of User ID by Outsiders	2	Exchange, Housing Benefits
Masquerading of User ID by Insiders	1	Financial Accounting
Technical Failure of Print Facility	1	Cashier's Office
Communications Manipulation	1	Exchange
Communications Infiltration	1	Exchange
Masquerading of User ID by Contractors	1	Exchange
Natural Disaster	1	Housing Benefits
Terrorism	1	SOSCIS

CRAMM software was used to quantify which threats were the most dangerous to the IT Division. It may have been possible to determine qualitatively which threats were most dangerous without the software; however, CRAMM scaled the threats as very low, low, medium, high, or very high. The vulnerability associated with that threat was categorised as low, medium, or high. Those categorisations were done by CRAMM once the answers to the threat and vulnerability questionnaires were entered into the software. Sometimes the threat level may be high, yet the vulnerability may be medium or low. Both the threat and the vulnerability categories were taken into consideration when a risk level was assigned.

#### **4.2.1.1 Frequently Identified Threats**

Since it would not be feasible to describe in detail each threat that was recognized by any of the interviewees, only the most frequently identified threats and most dangerous threats are described in depth. Frequently identified threats included any threat that was acknowledged by three or more different interviewees. Using Table 4-2, those threats can be easily identified.

The most frequently identified threat was technical failure of host, which was identified by representatives of the Council Tax, Financial Accounting, Housing Rents and Repairs (2) and Payroll systems. The questionnaire that was associated with this threat asked about the age of the host, its design, and whether it is being extended beyond normal capabilities. The questionnaire was also tailored to the vulnerabilities, such as replacing the host and how long it would take to repair a problem to the host. The questionnaire was intended to identify the factors that increase the likelihood of a failure of the host and the ease of resuming service following such a failure.

Application software failure was also a commonly suggested threat. The systems that identified that threat were Financial Accounting, SOSCIS, Payroll, and Housing Rents and Repairs. The threat and vulnerability questionnaire asked about the frequency of occurrences

of an application software error for different amount of times and how often information had been disclosed or modified because of an application software error. In general, the threat questionnaire pertaining to application software failure covered the possibility of errors in application programs.

The threat of system and network software failure was also identified by employees of the Cashier's Office, Housing Rents and Repairs, SOSICIS, and Housing Benefits. The questionnaire associated with this threat asked about the amount of times that a system or network software failure had caused certain amounts of service loss as well as how many times such a failure has caused data to be modified, disclosed, or destroyed. The vulnerability section of the questionnaire concerned the amount of time it would take to restore the services if there was a system or network software failure. In general, the threat of system and network software failure covers the possibility that the system or network software might fail, causing not just a loss of service, but also potentially weakening other security mechanisms.

The threat of user error was primarily identified among the IT Services employees rather than the expert user employees. People who work in Social Services or other departments within the Council are often not very familiar with computers. More errors are made when a user is not comfortable with the software that is being utilised or computers in general. The systems that identified user error as a threat were Council Tax, Financial Accounting, and Payroll. The questionnaire was concerned with how often in the last three years a user error has led to problems with service and disclosure of data, as well as how many users there are for the system in question, and how much pressure they are under. The questions also concerned the experience of the user as well as the complexity of the programs that were being used. Generally, the threat of user error covers the possibility that the users might make mistakes when using an application.

The threat of staff shortage is a common fear in any organisation. In many workplaces, employees feel as though the department that they work in is understaffed. Therefore the workers that are employed are overworked, unhappy, and less productive. In two interviews, the Council Tax system identified staff shortage as a threat, and it was also identified by the Payroll system. The fact that the threat was identified by both interviewees of the Council Tax system is understandable, because this was the end of the financial year and all of the bills were being sent out. This is always the busiest time of the year, so they felt many pressures and felt that additional staff members would be helpful. The questionnaire was concerned with the disruptions to the IT service, staff morale, and the number of staff that could be absent without causing a problem within the organisation. In general, the threat of staff shortage covers the possibility of the absence of key personnel for whatever reason and the ease with which they could be replaced. The vulnerability to staff shortage depends on the extent to which shortage of staff would affect the business processes.

Hardware maintenance error was identified as a threat by both Council Tax interviewees and the Housing Benefits interviewee. The questionnaire asked how many times hardware maintenance errors had led to the loss of service, the number of people that repair errors to hardware, and the length of time that a repair required under normal circumstances. In general, the threat of hardware maintenance error covers the possibility that those people responsible for maintaining the hardware might make mistakes when carrying out their work.

The threat of technical failure of network service is a common fear of many employees within any organisation. Employees are reliant on the network because many items, including calendars and important emails, are only accessible through the network. This threat was identified through both interviews with the Housing Rents and Repairs system and one of the interviews with the Housing Benefits system. The questionnaire was

concerned with trends of network failure and the effect that network failure would have upon the users of the system. In general, the threat of failure of a network service identifies the factors that increase the likelihood of a failure of network service. The vulnerability to network failure depends on the ease of resuming service following a failure.

#### **4.2.1.2 Dangerous Threats**

Based upon the Threat and Vulnerability Summary that was developed by CRAMM, a dangerous threat was one labelled either high or very high and a dangerous vulnerability was one labelled high. Since some threats were identified by more than one system, we decided that if any of the systems were labelled high or very high, then that threat was dangerous. Sometimes the Council was vulnerable to dangerous threats, while other times it was not. In the same sense, sometimes a threat was not dangerous at all, but the Council was more vulnerable to that threat than it might have been to a dangerous one. The Threat and Vulnerability Summary that was generated using the CRAMM software can be found in Appendix K.

Masquerading of user identity by insiders is a threat that was labelled very high, with a high vulnerability. This threat covers attempts by authorised users to gain access to information to which they have not been granted access, for example, by posing as another user. This threat was identified through an interview with an IT representative of the Financial Accounting system and may be specific to that system, although it also may be applicable to other systems. Masquerading of user identity by outsiders was identified as a threat through an interview concerning the Exchange/Outlook system. This threat is similar to that of insiders attempting to view files they do not have access to. The threat level is also high, but the vulnerability is only seen as medium since insiders have easier access to the network and all of the systems than outsiders do. Anytime an employee or outside party

attempts to access an area which they are unauthorised to enter, it is dangerous to the organisation.

Communications failure was a threat that was identified by the Council Tax system and the Housing Rents and Repairs system. The threat for Council Tax was labelled as very high, with a high vulnerability. For Housing Rents and Repairs, the threat level was identified as high, and the vulnerability level was also identified as high. Communications failure refers to the disability to communicate through the use of electronic means. It may also be considered as physical communications failure between the client department and the programmer of the system since they are in different departments and on different floors. Communications failure can have a huge effect on an organisation if there is a breakdown between one end of the system (IT) and the other end of the system (Client Department.)

Technical failure of network service was identified through two of the interviews with representatives of the Housing Rents and Repairs system and one interview with the Housing Benefits system. The Housing Benefits system was labelled with a threat level of low, but a high level of vulnerability. The Housing Rents and Repairs system identified the threat level as high, but the vulnerability level as medium. The fact that two different systems identified that threat and that there are different threat and vulnerability levels shows the differences that there are from one system to another. Although the two systems may have been similar in some ways, they are not exactly the same in every way. The subtle differences between the systems, the employees of the systems, and the opinions of the people that completed the questionnaire explains the differences in the quantification of the threats and vulnerabilities.

Based upon the threat and vulnerability summary, air conditioning failure has a very high threat level. The threat of air conditioning failure covers the possibility that work may have to be suspended because temperatures in the location fall outside of acceptable



parameters. However, since the Council is not located in an area that deviates from the appropriate temperature range without air conditioning, it is not vulnerable to such a threat.

Application software failure was identified frequently and is also considered a dangerous threat to which the Council is vulnerable. With a very high threat level and a high vulnerability level for the Financial Accounting, Payroll, and Housing Rents and Repairs systems, application software failure is a very dangerous threat that the Council is very vulnerable to. One other system, SOSCIS, identified the threat, but the threat level was low, while the vulnerability level was still high. With the failure of application software, no business may be conducted by the system that has the failure, so a large impact will be felt. Computers and the software that go along with them are at times temperamental and can fail at any time. Since such an error is at times difficult to predict, it is difficult to prevent its occurrence.

Hardware maintenance error was identified by both interviewees responsible for the Council Tax system as well as the interviewee that was responsible for Housing Benefits. The threat level for both of those systems was very high, and the vulnerability level was also high. This means that there are problems that should be taken care of within the section of the IT Division that is concerned with the upkeep of all hardware. It is understandable that the threat is very high if there is a hardware error because all information that is stored by the hardware may be lost. The fact that there is a high vulnerability for both systems means that there may need to be changes made in the way that errors in the hardware are handled.

Computers are very complex. Many times, the user of a computer is not familiar with all of its operations, or how many tasks are done by a computer. Employees of the Social Services or Human Resources Department may not have had very extensive training on a computer; therefore they are prone to making mistakes. User error had a very high threat level and a high vulnerability level for all three systems that identified it as a threat: Council

Tax, Financial Accounting, and Payroll. As technology advances and more people become comfortable using computers, this threat will slowly fade away. However, there are vulnerabilities that are created when users make unnecessary errors.

#### **4.2.1.3 IT Threats to Entire Council**

Along with all of the threats that were identified for the eight systems, we also identified potential risks to IT Services and the Council as a whole. We conducted two group interview sessions, one with the Systems and Projects group and the other with Desktop Support Group. Summaries of both the group interview sessions can be found in Appendix P.

The first area of concern that we identified were network logon issues. These not only pertained directly to logging on the Council's network, but also to network access to the various systems. From the information we gathered we were able to determine that network logon issues are a rather rare occurrence for most of the IT staff. The problem occurs more frequently among system users due to error on the part of the user rather than the network. The problems tend to be minor and easily solvable.

The second area of concern related to password maintenance and control procedures. There is a substantial difference in password control procedures between the two groups. The Systems and Projects group had at most 12 passwords to remember, and those were usually passwords related to specific systems they worked on.

In most cases, we found that the systems required for passwords to be changed on a monthly basis. The mainframe systems passwords are all generated randomly by the mainframe and then printed and sealed in envelopes, all without human intervention to prevent them from being compromised. They are then distributed to the appropriate individuals. In all cases the Systems and Projects group does not have the passwords to access live data. They only have access to the development and test systems.

The issues relating to password control for the desktop support group (DSG) team were significantly greater. We found that these employees had approximately 50 administration passwords they had to use for a variety of systems and computers. There was also no requirement for regular password change in the department. As a result, a master password list for all the systems is printed and stored in a sealed envelope in a secure location. However, most employees can obtain access to the list in the event that they might need to fix a computer after hours.

The third major area of concern was any threat concerning remote access to Merton's systems. The Council utilizes a Remote Access Server (RAS) that employees can use via modem to check system availability, access files, or to perform other functions for which they might need network access. There is also web access for the Microsoft Exchange email system to allow for employees to check their work email from outside the building. The main concern that was identified was the possibility that a user from home might be connected to both the external Internet and the remote access server at the same time. This would have then created the possibility for an unauthorized person to gain access to the Council's network via the Internet. Currently, it is not a primary concern because few employees can be connected to the internet and RAS at the same time, and those that do have protected their home systems with firewall utilities.

The last major topic was the potential risk of using portable workstations. The groups only used a limited number of portable workstation, about five laptops per team. There was no central point from which an individual could borrow a laptop; however, someone at home who is on call could receive one. People who used the laptops didn't have access to confidential data, and at no time were their passwords or sensitive information stored on paper. If a portable workstation was stolen or lost it would be reported to the service desk. They in turn would fill out an insurance report, and report the loss to the police. If stolen, the

administrative passwords on the laptops could be cracked, and the perpetrator would be able to gain access to a limited number of network user passwords as well. This topic is of less concern to the Authority than the other areas of security.

#### **4.2.2 Threat Reports**

Once all of the information from the questionnaires was entered into CRAMM, we generated reports for each threat and the systems identifying it. The reports straightforwardly describe the danger level associated with each threat. These reports were not used in the analysis of the data, but they were helpful in seeing which threats were commonly identified and which threats were thought of as insignificant by most employees. The threat reports can be found in Appendix K.

## **5. Analysis**

Using our data, we conducted both a risk analysis and a gap analysis. The risk analysis consisted of identifying the greatest risks to the IT Services division, and when applicable, to the entire Council. The gap analysis process involved describing IT's current information security position, their ideal security position, and a means with which to reach their ideal situation.

### **5.1 Risk Analysis**

The following analysis consists of two parts: the quantitative analysis provided by CRAMM, and our qualitative assessment of those results.

#### **5.1.1 CRAMM Results**

After we calculated the value of the assets and used CRAMM to measure the threats and vulnerabilities, we constructed a risk analysis summary from CRAMM that specified the risk level for each threat. CRAMM uses a pre-determined risk analysis matrix to assess the maximum risk value. The matrix, shown in Table 5-1, correlates the asset value, threat level, and vulnerability level to determine the risk level for that threat. For example, the threat 'communications failure' for the Council Tax system was assessed to have a very high threat level and a high vulnerability level. From the data we gathered on assets we were able to determine that Council Tax assets were valued at three on a scale of one to ten. This correlated to a maximum risk level of four in Table 5-1.

**Table 5-1: CRAMM Risk Assessment Matrix**

	Threat	VL	VL	VL	L	L	L	M	M	M	H	H	H	VH	VH	VH
	Vulnerability	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H
<b>Asset Value</b>	1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
	2	1	1	2	1	2	2	2	2	3	2	3	3	3	3	4
	3	1	2	2	2	2	3	2	3	3	3	3	4	3	4	4
	4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
	5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
	6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
	7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
	8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
	9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
	10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

Using CRAMM reports, we grouped the data together by system to show the maximum risk levels in Table 5-2. From this information we were able to determine what the most dangerous risks were, and where the Council should focus its efforts at improvement.

**Table 5-2: Risk Assessment Summary**

<b>Council Tax</b>			
Description of Threat	Max. Threat	Max. Vuln.	Measure of Risk
Communications Failure	Very High	High	4
Air Conditioning Failure	Very High	Medium	3
Hardware Maintenance Error	Very High	High	3
User Error	Very High	High	3
Technical Failure of Host	Medium	Low	2
Operations Error	Medium	High	2
Software Maintenance Error	Very Low	Medium	2
Staff Shortage	Low	Low	1
<b>Housing Benefits</b>			
Description of Threat	Max. Threat	Max. Vuln.	Measure of Risk
Hardware Maintenance Error	Very High	High	4
Operations Error	Very High	High	4
Masquerading of User Identity by Outsiders	Very High	Medium	3
Application Software Failure	Very High	High	3
Unauthorized Use of Application	Medium	High	3
Natural Disaster	Very Low	High	3
Technical Failure of Network Service	Low	High	2
System and Network Software Failure	Medium	High	2

**Table 5-2: Risk Assessment Summary (cont.)**

<b><i>Housing Rents and Repairs</i></b>			
<b>Description of Threat</b>	<b>Max. Threat</b>	<b>Max. Vuln.</b>	<b>Measure of Risk</b>
Communications Failure	High	High	4
Introduction of Damaging or Disruptive Software	Low	High	3
Technical Failure of Host	Medium	High	3
Technical Failure of Network Service	High	Medium	3
Application Software Failure	Very High	High	3
System and Network Software Failure	Very High	High	3
Power Failure	High	Medium	2
Misuse of System Resources	Medium	Medium	1
<b><i>Exchange and Outlook</i></b>			
<b>Description of Threat</b>	<b>Max. Threat</b>	<b>Max. Vuln.</b>	<b>Measure of Risk</b>
Masquerading of User Identity by Outsiders	Very High	Medium	3
Masquerading of User Identity by Contractors	Very High	High	2
Communications Infiltration	Very Low	Medium	2
Misuse of System Resources	Low	Medium	1
<b><i>Financial Accounting</i></b>			
<b>Description of Threat</b>	<b>Max. Threat</b>	<b>Max. Vuln.</b>	<b>Measure of Risk</b>
Masquerading of User Identity by Insiders	Very High	High	5
Unauthorised Use of an Application	Medium	Medium	4
User Error	Very High	High	4
Technical Failure of Host	Low	Low	3
Application Software Failure	Very High	High	3
Power Failure	Low	Low	1
<b><i>SOSCIS</i></b>			
<b>Description of Threat</b>	<b>Max. Threat</b>	<b>Max. Vuln.</b>	<b>Measure of Risk</b>
Fire	Medium	High	4
Terrorism	Very Low	High	3
System and Network Software Failure	Medium	High	2
Application Software Failure	Low	High	2
<b><i>Payroll System</i></b>			
<b>Description of Threat</b>	<b>Max. Threat</b>	<b>Max. Vuln.</b>	<b>Measure of Risk</b>
User Error	Very High	High	4
Technical Failure of Host	Medium	High	4
Software Maintenance Error	Medium	Medium	3
Staff Shortage	Very Low	High	2
Application Software Failure	Very High	High	2
<b><i>Cashiers Office</i></b>			
<b>Description of Threat</b>	<b>Max. Threat</b>	<b>Max. Vuln.</b>	<b>Measure of Risk</b>
Introduction of Damaging or Disruptive Software	Low	High	3
Technical Failure of Print Facility	Medium	Low	3
Fire	Low	High	3
Theft by Outsiders	Very Low	Low	2

## 5.1.2 Greatest Risks

Many risks to particular systems were identified through interviews and through use of CRAMM. In order to narrow our assessment we focused on the greatest risks to each system and the potential effects they might have on the Council.

CRAMM generated reports measuring risks to all the systems we identified. The risks were measured on a one-to-seven scale, with one being the lowest and seven being the highest. Table 5-2, found in the Section 5.1.1, depicts a summary of the risk analysis report organised by system from the CRAMM - generated report. The CRAMM Measure of Risk Report can be found in Appendix L. The highest risk level we found in conducting our review was five, so we decided to only consider risks with a level of four or higher as being of the utmost importance to the council.

The Financial Accounting system had three risks with a measure of four or higher. We found this system had more dangerous risks than others because it contains more valuable data than any other system. As you can see from Table 5-1, even if the threat and vulnerability levels are very low, when the asset is valued highly the risk is considered to be great. The threat of 'masquerading of user identity by outsiders' had a risk measure of five; the threats of 'unauthorised use of an application' and 'user error' had a measure of four. With approximately 700 system users, the likelihood of the misuse of a user identity or application is increased and it also becomes more likely that a user will make an error.

Council Tax, Housing Rents and Repairs, and SOCSIS each had just one threat associated with a risk measure of four. Council Tax and HRR had a high risk associated with the communications failure threat because if employees are unable to communicate electronically, their work comes to a halt; their work is centred on accessing the system electronically. Also, since Housing Rents and Repairs has users outside the Civic Centre it is much more susceptible to communications problems. For SOCSIS, fire was considered a



high risk because the majority of information is stored on paper files, and there is no electronic backup for this information.

Housing Benefits had two risks with a measure of four. One of Housing Benefits' greatest risks was the threat of a hardware maintenance error. This was most likely due to the fact that the system is housed on an older mainframe system. However, we found that hardware maintenance is managed particularly well. The authority also has a very good service contract with the mainframe provider; because of this, we felt that although CRAMM rated this as a high risk, it is more likely a lesser problem. The other major risk to the system was the threat of 'operations error;' an employee operating the host system may make mistakes. The identification of 'operations error' was most likely was a result of the cost of the asset. The VME mainframe is a very expensive asset costing more than all of the other physical assets combined, which caused the risk level to be rated higher.

Outlook/Exchange did not have any major areas of concern associated with its threats. The risk level of the threat 'masquerading of user identity by outsiders' was three, so we did not consider it because of its lower ranking.

The Payroll System had two perceived risks with a value of four. The first was user error. Analysis suggested that users who were operating in error could have been a risk to the system. Hypothetically, a user entering incorrect data, or configuring the system improperly could have caused the system to become unstable. 'Technical failure of host' also received a risk ranking of four because the NT host is less stable than the UNIX or Mainframe hosts.

## **5.2 Gap Analysis**

Our gap analysis studied the IT division's current position, and where they would like to be with regard to security standards in the future. Through this analysis we were able to identify and assess measures to move the organisation across the gap.

## 5.2.1 Current Controls

We discovered there are varying levels of security controls within the eight systems. There are some controls, such as passwords and tape backups that are universal. However, there are other controls that vary from system to system.

Passwords are used by all eight systems to restrict access. Only authorised users of each system are allowed to log in with a username and password. Users' passwords must be changed regularly, and for most systems it is changed every 28 days. Each user also has a security profile, which defines his access levels and functions within the system. The users' passwords only give them access to the parts of the systems that are necessary for their jobs.

A tape backup for every system is performed at the end of each day. The backup system is referred to as Legato, the name of the French supplier of the system. A full backup of every system is done on each weekend, and on Monday morning these tapes are taken off site. Every weekday evening a differential backup is performed by Legato. This entails only backing up the files that have been changed thus far that week.

The Financial Accounting system has two additional controls. First, the connection to the system times out if a user is idle for 20 minutes. The second control is that fewer than 10 people have full access to all data stored by the system.

Council Tax, SOSCIS, and Housing Benefits are all on the VME mainframe, which provides substantial protection. Due to the age of the VME database, it is difficult to improperly change data on the system. If someone is able to get into the system, the only data that can be changed is in the development database; it would be impossible to affect the live database. There is a weekly integrity check on the server, in which all of the pointers between data are checked. The pointers are reference points between different data objects that tell the database where to look for specific information.

The Housing Rents and Repairs system restricts complete access to three people, while all other users of the system have limited access. The Database is check-pointed to a disk with Journal running on it, so if the system crashes during the day, it will automatically go through Journal and redo everything from the previous day's backup. In the Cashier's Office certain users have more access than others; for example a manager's access level is fifteen, a supervisor's level is ten, and a cashier's level is five.

### **5.2.2 CRAMM Recommendations**

After completing the analysis portion of our CRAMM review, the software provided us with a detailed list of proposed countermeasures and the systems to which they pertained. Generally we found that although CRAMM linked the controls to specific systems, most applied to all systems. Due to time constraints on our project we were not able to identify all of the controls that the Council already had in place; however, we were able to determine some. Appendix M lists the 97 controls provided to us by the software. We identified the controls that were currently implemented in full or in a limited form throughout the Council. Finally we marked the controls that we felt were of importance to the Council and that we would recommend as areas to be looked into.

### **5.2.3 Our Recommendations**

Some of the controls recommended by CRAMM are already implemented, some are not feasible, and some are too vague to be useful. We examined the controls and have taken into consideration information that the CRAMM software could not, such as our group interviews, other interviews, and our daily experience in the Merton workplace.

### 5.2.3.1 Passwords

One area in which we have some recommendations is passwords. Ten CRAMM-recommended controls dealt with passwords, while passwords were also identified in our group interviews as a risk. Below is a list of the most important CRAMM controls not currently implemented:

- The password should be of sufficient length to ensure that they are difficult to decrypt
- Passwords should be changed regularly
- Passwords should be stored in a one-way encrypted form
- Passwords should be changed whenever they have been compromised
- User access rights should be reviewed at regular intervals
- Access to System Administration accounts should be strictly controlled

Password length, form, and turnover rate vary from system to system. Although all systems are not required to manage passwords in exactly the same manner, they should use the same standards for controlling passwords. When users change passwords, they can often change it to whatever they want. Requiring passwords to be of a certain length would be a useful control. Also, not all passwords are regularly changed, which is a potential problem.

During our group interviews, we examined two password problems: lost laptops, and the list of administrator passwords. Although the employees speculated that the passwords used to log on to a lost laptop would be changed, there was no policy of which they were aware. A policy stating such would ensure that compromised passwords are changed.

The 100 administrator passwords are stored in a sealed envelope so that it is available in case a system goes down and the person who knows the password is not available. However, there is not a list of people certified to access the passwords, so it is the judgement of the service desk personnel working at the time to decide if an employee can obtain the needed password. Also, regardless of whether the employee needs one password or ten, he

gains access to all of the passwords. Once the employee leaves the room, he can do anything he likes with the list, such as photocopy it. We recommend that the list be stored in approximately five groups of twenty passwords each, to restrict the number of passwords an employee can have access to at any given time. Also, there should be a list of authorised employees who are allowed to access the passwords. Since it is necessary to keep a hard copy of the passwords, little can be done to avoid the risk of photocopying. Currently, these administrator passwords are not changed on a regular basis. If they were changed regularly, photocopies would only be a risk for a small period of time. This measure would lessen the risk from photocopying.

User access rights should be reviewed at regular intervals so that as job requirements for an employee change, the data available to him changes accordingly. If an employee's needs are broadened, but his access does not increase accordingly, he will not be able to perform his job as required. Conversely, if the user needs less access, it would be imprudent for the organisation to continue to give him the greater access that he previously required.

#### **5.2.3.2 Remote Access Server (RAS)**

There was one CRAMM recommendation pertaining to the Remote Access Server (RAS) that we also endorse: teleworking should only be authorised if the appropriate security arrangements are in place. As identified in our group interviews, there are some concerns with the RAS. If a person is connected to the Internet via a broadband connection and at the same time is connected to the RAS, it is possible that an outsider could record the keystrokes used to log onto the RAS, and in the future be able to log on. Broadband connections are not yet popular in the UK, but in the future they will become more widespread in the homes of employees. The RAS system should not be used by anyone with a broadband connection without the necessary firewall software. We recommend that the organisation make that software available to anyone requiring it, for the duration of the RAS system use.

Another system is being created within the IT Division using Virtual Private Networking, or VPN, technology. VPN is a secure, encrypted connection that will allow users to log on the network and be connected to the Internet without the risks involved in using the RAS. The VPN connection is currently being tested, and has approximately five users. As soon as it is ready, it should be implemented to reduce the risks inherent in the RAS connection.

### **5.2.3.3 Backups**

Backing up systems and their data is essential in order to ensure continued service in case a server or a hard drive is temporarily or permanently lost. This is currently done through the Legato system. Of the CRAMM recommendations, we advise exploring the following five:

- Back-ups should be taken of all essential business data
- Back-ups should be taken of all software applications
- It should be possible to re-create data lost since the most recent back-up
- Security tests should be conducted against the security requirements, using agreed acceptance criteria
- A stand-by host should be available to take over processing in the event of a disaster or other incident

The first three points address the function of the Legato system. Currently, Legato is working properly; two or three restores are done correctly each day. In the past, problems have arisen mainly due to the ICL support team. This problem, combined with the high cost, lead us to recommend exploration of a different method of tape backups after the contract with ICL expires.

The fourth control, which recommends testing security measures to ensure they are working correctly, should be applied to all security measures. However, we feel it should be

applied to the Legato system in particular, since Legato has had problems in the past and so much reliance is placed on it. Regular checks to ensure that the tapes are properly storing the information for both differential and complete backups should be performed.

The last control is in the process of being implemented by the Exchange/Outlook system. Currently there are three servers, named Exchange 1-3. There is a plan to reduce the number of servers to two, and have these two be duplicates so that if one fails, the other one will still be able to perform effectively. This is very important for the Exchange/Outlook system, because if the email fails to work, it affects the entire Council immediately. It is unfortunately not fiscally reasonable to have similar server duplicates for the other systems because of the cost of servers. If it is ever financially possible, however, duplicate servers and hard drives should be considered.

#### **5.2.3.4 Data Protection**

There were two CRAMM recommendations concerning data protection that we also support:

- Information systems handling personal data should comply with the principles of the data protection legislation
- The data subjects' rights should be enforced

Information concerning data protection legislation can be found in Appendix B, and it would be unnecessary to list here the various laws with which an organisation should comply.

#### **5.2.3.5 Knowledge of Assets**

Another area in which CRAMM identified some controls to be implemented is that of asset knowledge; two are given below.

- All workstations attached to the hosts should be identified
- All major information assets should be accounted for

It is important to keep track of every workstation within the systems. Currently they all have an ID tag with a number, which allows them to be tracked. However, this tracking does not extend to their actual or intended use. Knowing which workstations are being used for which systems would allow for more control over access to the systems, and easier identification of unauthorised access.

Similarly, it is important to keep track of the data stored by each of the systems, so that they can be properly monitored. Each system has its own data asset. The type and quantity of information stored in each should be known and recorded; this will help in future assessments.

#### **5.2.3.6 Miscellaneous Recommendations**

There are a few more recommendations that do not fall into a single category, but are all self-explanatory:

- All suspected or detected attempts to breach security should be investigated
- Regardless of ownership, any equipment used for information processing should be authorised by management
- The potential for the introduction of malicious software into the IT system should be minimised



## **6. Conclusions**

Our main conclusions involve evaluating the feasibility of completing a risk assessment of the entire Council, and our final thoughts on the project as a whole. The feasibility study included the Council Officers' time, and our time spent on the risk assessment from interviews, questionnaires and CRAMM usage, which were recorded and tracked by use of a database. Through our recommendations, we intend for Merton to be able to effectively manage future problems regarding information security.

### ***6.1 Feasibility Study***

The goal of conducting a feasibility study was one that was added to our project after we arrived in London. While in Worcester, we knew that our IQP was a pilot for a larger project, but we were not sure what the larger project was, or how we would affect it. We now know that the larger project was to conduct a risk assessment of the entire Council using CRAMM software. Through the use of an Access database we were able to track the time that we spent working on the pilot and the amount of time that the Council Officers spent on it. The list of all meetings and interviews can be found in Appendix N. We were then able to determine whether or not the full risk assessment would be feasible and the amount of time and effort such an undertaking would require.

#### **6.1.1 Time Spent on the CRAMM Exercise**

For our liaison, the most important part of our feasibility study was to determine how much time was required to conduct a CRAMM study. The Council had never used CRAMM and very few of the employees that we interviewed were familiar with that type of risk assessment. Since few of the employees of the Council had even seen CRAMM, and none had ever conducted a risk assessment using the software, the amount of time that we took to familiarise ourselves with the software package was also of importance. The CRAMM user's

guide is a 375-page document that describes the concepts of a CRAMM assessment and how to use the software. One of the recommendations for completing a CRAMM assessment is that all of the reviewers are experts with the software and at least one of them should have previously completed a CRAMM risk assessment. Such CRAMM expertise is very expensive, costing upwards of £1,000 per day. It is not feasible for an organisation in the public sector to hire consultants to conduct a risk assessment because Merton simply does not have the financial resources.

#### **6.1.1.1 Our Work**

Much of the time that we spent on the project was going through the CRAMM manual and the software itself to determine which questions needed to be asked and what types of additional information were necessary in order to create a successful review. Since none of us were familiar with the method or the software before we arrived at the Merton Civic Centre, there was a long initiation process for us to become fully comfortable using it. We began the review and became moderately comfortable with the software before the interviewing process began. As we progressed through the software operations, we became more comfortable with the process and knew which questions to ask at each interview. We had difficulties in the beginning, not knowing which questions were completely necessary at all times, but by the end we knew what to ask each interviewee. Since we were learning as we worked we had to go back to many of our first interviewees and ask them questions we did not realise would be pertinent at the time of the original interview.

Another aspect of working on a project that was new to us was the concept of project management, and the methodologies that are concerned with it. The first meeting that we had concerned PRINCE2, a project management methodology that is used in the UK. Since the concept was new to us, we had an adjustment period until we became at ease with the method. If this project were to be completed by Merton IT or other departmental staff, they

most likely would be familiar with this process, and hence would not have to spend as much time as we did learning about these concepts.

Similarly, we were unfamiliar with the responsibilities of the Council and their various systems. Much of our time was spent in gathering information about them. Employees of the Local Authority would not have to spend this time familiarizing themselves with the systems since they work with them daily.

Throughout the IQP, we spent time communicating our project to other people; the amount of time required would be similar to that which a non-IQP group of employees would need. We had weekly progress meetings with the advisors and our liaison, which is necessary in any project to ensure that the scope is reasonable and the project will reach the desired completion within the available time. Any project will also require a final report and presentation. In this sense, all of the work that was necessary to complete our project for WPI and for our sponsor required the same amount of work as it would for any organisation conducting a risk assessment using CRAMM.

In the beginning of our interview process, we did not know all the information that CRAMM required. We conducted 11 interviews concerning the systems that we were studying. For two of those interviews, we were later required to ask additional questions that we did not know were necessary until we moved further on in CRAMM. Each system interview lasted approximately 30 minutes, and each additional information interview lasted approximately 15 minutes, so the total interview time was about six hours. Each interview also required a one half hour of preparation time and at least 30 minutes to format the interview summary. The total interview time for all of the systems that were studied was approximately 18-20 hours. Some of the systems required more time than others because of the number of interviews that were necessary, but in general each system required about two hours and 30 minutes of interview time.

In addition to the system interviews, we conducted one interview with Paul Biggs, Infrastructure Manager, so that we could value the physical assets of the IT Division. That interview lasted one hour. There was one other interview with Paul Damaa, Lead Engineer, to gather background information concerning the Legato unit, a tape backup device used to store data. This interview lasted approximately one hour. We also conducted two group interviews that addressed security issues with the network and passwords; each of these took one hour as well. Besides the interviews, we had weekly progress meetings that lasted an hour and close to one presentation per week that lasted about half an hour. We had five progress meetings and three presentations, for a combined total of about seven hours. The complete list of all of the meetings and interviews that we held can be seen in Appendix P.

#### **6.1.1.2 Council Officer Time**

The amount of time spent by each divisional officer for the risk assessment exercise was not excessive. Each officer spent 30 minutes in the interview, and approximately 30 minutes completing the questionnaire. When each questionnaire was handed out, the employee working on it was asked to write down how much time it took to complete. In all, each officer was only busy for approximately one hour of his time for this exercise. The longest that any interview lasted was 30 minutes, and the amount of time to complete a questionnaire ranged from 20 to 45 minutes. Many times the employee did not return the questionnaire immediately, which forced us to follow up with him or her. If an employee did not return the questionnaire or list the most dangerous threats within a few days, they were sent an email and asked to do so as soon as possible. Often times, the employee was very busy with other work and had forgotten that they were involved in the risk assessment project. Once they were reminded they were very cooperative. In general, the officers of the Council are very busy people, but not so busy that they could not spare an hour or so to help

with the project, and many were interested in the final report as it pertained to their area of work.

Conducting a risk assessment on a larger scale would require much more officer time and cooperation. The people who would be actually conducting the review, as we did, would most likely be officers of the Council, so they would not have to do everything that we did. The officer time on the system side of the review would be about the same, but if there is not an independent contractor or project team completing the review then the total officer time would be considerably higher. The amount of time spent on each system by the officers can be found in Appendix Q.

### **6.1.2 Recommendations**

One way that our efficiency could have been improved would be if we had materials concerning description of CRAMM before we came to London. Much of the work that we did involved becoming familiar with the program, which we had never seen before. CRAMM is a very complex program that was easy to use, but had many hidden parts that it would have been helpful to know about during our preparation phase.

We were rather efficient in the interviewing and data gathering process because we had four group members. Two people conducted each interview, so while the interviews were in process, the other two group members worked with CRAMM, handed out and collected questionnaires, or wrote our report. If our group had consisted of fewer than four members, the project would have been much more difficult to complete.

The expansion of the pilot to a larger project is feasible, but it would take diligent preparation and careful execution. The most important part of conducting the risk assessment is to be familiar with the procedures that are used in assessing risk, as well as the software package that will be used. We recommend that whoever is conducting the review either be experienced with the software, or take some sort of an introductory course so that they will

know what to ask and who to ask for each system assessed. Another option that could be pursued if the organisation was unable to find employees experienced with CRAMM, would be to bring in an outside CRAMM consultant for a one or two day training session. This would be cost effective for the Council and give them the experience necessary to appropriately conduct a review of this nature on their own.

The method that would give the most accurate results would be to determine which threats must be considered individually for each system, and which threats would apply to all systems equally. For example, there are some threats associated with the host or network that are the same for each system and can be answered by one person. In contrast, software or hardware maintenance errors can be different from system to system, so this questionnaire should be completed for each separate system. If the people conducting the risk assessment had more knowledge of how the threats were related to the systems than we did, they would be able to create a more accurate analysis. The method that would give the best representation of data would be to give each questionnaire to all of the interviewees. This would not have been feasible for us due to time constraint, because a single questionnaire containing all the threats would have been over 120 pages. It was not feasible for us to ask the employees to undertake such a task, so instead we used the best method at the time, which was to select the threats that the interviewees felt were most dangerous to their system. These data were difficult to compare at times because there may have only been one system that identified particular threats. One way we could have made the employee's decisions about threats easier was if we had supplied them with a definition of each threat.

One final possibility that might make this project feasible for the Council would be to have one or more WPI project groups complete it, assessing the systems that were outside the scope of our review. This would allow for less officer time to be spent and would be the most cost-effective method of conducting another CRAMM review. In the end, we

determined that the project is feasible and is recommended so that the Council can be aware of threats, vulnerabilities, and risks to all systems that are used. The project would simply be another means of making sure that the information about the people of Merton is stored securely.

## **6.2 Final Thoughts**

For seven weeks we toiled with the task of assessing the risks to eight systems whose proper running is dependent on the IT Division, and finding possible solutions to the risks we identified. We were aided in our task by CRAMM software, created by the UK government for this specific purpose. We walked away with more than just the feeling of accomplishment for completing such a laborious task, however. We left with a better understanding of the costs organisations must pay to keep their systems, their data, and their clients' interests secure. Although often expensive, necessary precautions such as detailed password policies and infallible backup systems can act as insurance against both malicious and random acts that could otherwise destroy an organisation's ability to perform.

Risk analysis is not a tool limited to IT divisions, Merton, or even the United Kingdom. It is a means with which any organisation can find out where its weaknesses lie, and what can be done to strengthen its softest spots. Important as it is, risk assessment has often been overlooked in the past, much to the chagrin of the failing businesses and bankrupt organisations that could have profited by its use. Their reasons for not using this implement of risk identification and repair are probably the time and financial cost required.

Risk assessment is one part of the very large field of project methodology. Since one of our goals at WPI is to become comfortable with project-oriented work, it is fitting that risk is the centre of our IQP. Everyone, at least on some subconscious level, performs some amount of risk analysis in his or her daily life. Running a risk analysis exercise makes these thoughts explicit, and focuses our attention on problems that could hinder us. As we work on and

become comfortable with projects while at WPI, our subconscious project and risk management will improve dramatically; we will learn through repetition. By learning methods to make risks explicit, as we have done these past seven weeks, we will be able to turn our intuitive feel for project management gained at WPI into conscious, accurate decision-making skills.



## Bibliography

- Adams, John. Risk. London: UCL Press, 1995.
- Berg, Bruce L. Qualitative Research Methods for the Social Sciences. Needham Heights, MA: A. Pearson Education, 2001.
- Biggs, Paul. Personal Interview. 19 March 2002.
- Brandt, Josh. Personal Interview. 5 February 2002.
- Brown, Peter. Personal Interview. 21 March 2002.
- Chicken, John C. and Tamar Posner. The Philosophy of Risk. London: Thomas Telford Pub., 1998.
- Damaa, Paul. Personal Interview. 10 April 2002.
- Davey, Geoff. Personal Interview. 8 April 2002.
- Dhillon, Gurpreet. "Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns." Computers & Security. 20 (2001): 165-172.
- Eloff, M. M., and S. H. von Solms. "Information Security Management: An Approach to Combine Process Certification and Produce Evaluation." Computers & Security. 19 (2000): 698-709.
- Everett, David B. Personal Interview. 6 February 2002.
- Glendon, A. Ian and Eugene F. McKenna. Human Safety and Risk Management. London: Chapman & Hall, 1995.
- Hawkins, Tracey. Personal Interview. 28 March 2002.
- Heap, Robert. Personal Interview. 20 March 2002.
- Hernon, Peter and Charles R. McClure. Public Access to Government Information. Norwood: Ablex Pub., 1984.
- Holstein, James A. and Jaber F. Gubrium. The Active Interview. London: Sage Publications, 1995.
- Kahn, Robert L. and Charles F. Cannell. The Dynamics of Interviewing: Theory, Technique, and Cases. New York: John Wiley & Sons, Inc., 1957.
- Key, Steve. Personal Interview. 22 March 2002.
- Kitson, Mark. Personal Interview. 21 March 2002.
- Kiuber, Krystyna. Personal Interview. 3 April 2002.

- Lawrenson, Steve. Personal Interview. 10 April 2002.
- Lopez, Felix M. Personnel Interviewing: Theory and Practice. New York: McGraw-Hill Book Company, 1975.
- Lovatt, Dave. Personal Interview. 10 April 2002.
- Lloyd, Colin. Personal Interview. 25 March 2002.
- Mason, Colin. Personal Interview. 25 March 2002.
- McDowell, Earl E., Interviewing Practices for Technical Writers. Amityville, NY: Baywood Publishing Company, Inc., 1991.
- McInnis, Ray. Personal Interview. 28 March 2002.
- Nice, Chris. Personal Interview. 10 April 2002.
- Neumann, Peter G. Computer-Related Risks. New York: ACM Press, 1995.
- Nosworthy, Julie D. "A Practical Risk Analysis Approach: Managing BCM Risk." Computers & Security. 19 (2000): 596-614.
- Pfleeger, Charles P. Security in Computing. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1989.
- Pounder, Chris. "The European Union Proposal for a Policy Towards Network Security." Computers & Security. 20 (2001): 573-576.
- Pounder, Chris. "The Revised Version of BS7799 – So What's New?" Computers & Security. 18 (1999): 307-311.
- Saris, Willem E., Computer-Assisted Interviewing. London: Sage Publications.
- Schneier, Bruce. Secrets and Lies: Digital Security in a Networked World. New York: John Wiley & Sons, Inc., 2000.
- Schultz, E. Eugene, Robert W. Proctor, Mei-Ching Lien, and Gavriel Salvendy. "Usability and Security: An Appraisal of Usability Issues in Information Security Methods." Computers & Security. 20 (2001): 620-634.
- Stride-Darnley, Felix. Personal Interview. 8 April 2002.
- Sykes, John. Personal Interview. 22 March 2002.
- Thompson, Ben. Personal Interview. 18 February 2002.
- Trompeter, C. M., and J. H. P. Eloff. "A Framework for the Implementation of Socio-ethical Controls in Information Security." Computers & Security. 20 (2001): 384-391.
- United Kingdom. British Standard 7799, British Standards Institute, 1999.

United Kingdom. The Commissioner. Data Protection Act: Legal Guidance. London: 2001.

United Kingdom. CRAMM User Guide, Security Service, 2001.

United Kingdom. Explanatory Notes to the Freedom Of Information Act 2000. London: The Stationary Office Ltd., 2000.

United Kingdom, Office of Government Commerce. Draft Guidelines on Managing Risk. London: OGC, 2001.

von Solms, Basie. "Informational Security – A Multidimensional Discipline." Computers & Security. 20 (2001): 504-508.

von Solms, Basie. "Information Security – The Third Wave?" Computers & Security. 19 (200): 615-620.

Warren, Richard. Personal Interview. 21 March 2002.

Webster, Graeme. Personal Interview. 10 April 2002.

White, Gregory B., Eric A. Fisch and Udo W. Pooch. Computer System and Network Security. New York: CRC Press, 1996.

## Glossary

*Risk* – A risk represents the likelihood of a threat happening/causing a problem

*Threat* – A process which, when active, could destroy or damage things of value, e.g. fire or theft.

*Asset* – Something that is of value to an organisation or individual that could reduce itself when exposed to a threat. Assets can be tangible e.g. skilled staff, a computer system or intangible, e.g. company reputation or goodwill of the company and/or individuals. This differentiation does not detract from the fact that any of these examples still hold a particular value to the company.

*Vulnerability* – A weakness in information controls or a loophole that can be exploited, enabling the threat to occur.

*Impact* – The result of the threat reaching an asset, e.g. destruction or complete loss of any of its assets (direct financial loss, embarrassment, loss of confidentiality, etc).

*Business Impact* – The result of the company following the destruction or complete loss of any of its assets, e.g. direct financial loss, embarrassment, loss of confidentiality etc.

*Controls* – Those measures implemented to counteract the impact from occurring. The severity of the impact will depend on the decisions that companies will make whether to accept, transfer, avoid, or reduce the associated risk by implementing the relevant controls. Controls can be both procedural and technical. Controls fall into the categories of deterrent, preventative, corrective, and detective controls.

*Countermeasures* – See *Controls*.

*Local Authority* – Each London borough has a governing body which is referred to as their Local Authority or Council. The responsibility of a Local Authority is to meet the needs of the citizens that reside in that borough.

*Council* – See *Local Authority*.

*Executive* – The person in charge of any project, who reports back to the company and is a member of the project board.

*Project Manager* – The person who is responsible for the day to day work of any project, such as following the budget or planning the tasks that need to be completed for the week.

*Senior Supplier* – The person that determines what the project will cost and whether or not the organisation has the resources necessary for the completion of the project

*User* – Anybody that uses a system within the Council. All users are Officers of the Council and have different levels of access to their system depending on what they need to complete their duties.

*Senior User* – The manager of each department; in charge of all of the users of their system. The senior user has access to all aspects of the system on the user side and controls the access of all other users.

## Appendix A: Merton IT Services Division

The Information and Communication Technologies organisation within the borough of Merton is primarily focused on supporting all information and communication needs for the council. Therefore the goals and mission of the ICT organisation must directly align with the goals of the council as a whole.

### *The Council's vision and strategic objectives*

Merton's vision is:

***“To make Merton a great place to live, work and learn”***

There are five strategic objectives, which will drive the work of the Council in the coming years:

1. Education Merton - the achievement of standards of excellence in our schools and colleges and inclusive access to learning, the arts and sport for all
2. Safe, Clean and Green Merton - a safe and clean environment in our streets and open spaces to improve sustainability and provide high quality of life for all
3. Caring Merton - support for vulnerable children that equals the standards of the best and support for vulnerable adults that meets their needs while maximising their independence
4. A Thriving Merton - regeneration of town centres and neighbourhoods to provide an attractive environment in which to live, visit and work
5. Equalities Merton - full and equal access to learning, employment, services and cultural life and the celebration of diversity

For the first time Merton has a 'Community Plan'. It is the voice of Merton's Community and sets out the top 20 issues that have been identified by a wide community consultation. The plan will last for 3 years (January 2002 to December 2004) and action to address the top 20 issues will be taken by agencies like the Council, Health Authority, Police, Voluntary Sector organisations and the Chamber of Commerce.

### *Size and Organisation*

#### *Elected Members of Merton Council*

There are 56 Members of Merton Council in 5 political groups plus 1 Independent Member and 1 vacancy. There is a cabinet which comprises 10 councillors including the Leader, Deputy Leader and eight other councillors, each holding Portfolios relating to one or more of the follow policy areas:

Portfolio	Councillor
Care Services	Peter McCabe
Finance & Corporate Support	Geraldine Stanford
Housing	Edith Macauley

Physical Environment	Russell Makin
Primary Education & Children's Services	Maxi Martin
Regeneration	Su Assinen
Secondary Education & Lifelong Learning	Karl Carter
Schools Reorganisation	Danny Connellan (Deputy Leader)

### ***Internal Structure***

The Council is organised into 5 separate departments each headed by a Director who reports to the Chief Executive.

- Housing and Social Services (Director: Rea Mattocks)
- Education, Leisure and Libraries (Director: Sue Evans)
- Environmental Services (Director: Richard Rawes)
- Financial Services (Director: Mike Parsons)
- Chief Executive's Department:  
(Chief Executive: Roger Paine, Asst Chief Executive: Keith Davis)  
[*Legal Services, IT Services, Policy & Scrutiny, Communication & Democratic Services & HR*]

## Appendix B: Legislation and Standards Affecting Information Security

### Data Protection Act

Prior to the Data Protection Act (DPA) there had not been new laws concerning data processing in Great Britain since 1984. Because of the rapid increase in power of computers, and therefore data processing systems, these laws needed to be updated. Although passed in 1998, the DPA allows time for organisations to bring their systems up to date. The final deadline for compliance with the legislation is 24 October 2007. The most important component of the Act is Section Three, in which the eight Data Protection Principles are listed, defined, and described.

The DPA uses some specific terminology to describe processing data. Titles such as data subject, data controller, and data processor have specific definitions, and understanding them is integral to understanding the DPA. The data subject is the person whose data are being processed. The data processor is the person (or group) who actually has the data and does the processing. The data controller is the person (or group) that makes decisions concerning processing the data, and is responsible for ensuring that the data are processed according to the current laws and standards.

#### **Point I: Data Shall be Processed Fairly and Lawfully**

In this Section of the Act, two lists of reasons to process data are given. The first list is for sensitive data and the second list is for non-sensitive data. If the data being processed are considered sensitive, one of the reasons given in the sensitive data list must apply to the situation, and likewise for processing non-sensitive data.

Sensitive data are defined as personal information concerning race, ethnicity, political opinions, religious beliefs, trade union member status, physical and mental health, sexual activity, or allegations concerning criminal activity. The list of reasons for processing sensitive data is quite lengthy; an abridged version is found in Table B-1. The reasons for processing non-sensitive data can be found in Table B-2.

**Table B-1: Reasons for Processing Sensitive Data**

I.	The data subject has given explicit consent
II.	The data needed for reasons of employment
III.	The data is needed for the vital interests of the data subject and explicit consent cannot be given
IV.	The data processing is done within a non-profit organisation (NPO) of which the data subject is a member, and the data will remain within the NPO
V.	The information has already been made public by the data subject
VI.	The data are needed for some legal process, or for the administration of justice
VII.	The data processing is needed for a medical reason
VIII.	The data are used to measure racial equality
IX.	The data are processed in circumstances specified by the Secretary of State



**Table B-2: Reasons for Processing Non-Sensitive Data**

I.	Data subject has given consent
II.	Processing is needed for a contract, or for entering into a contract
III.	Processing is needed to comply with a non-contractual legal obligation
IV.	Processing is needed for some life or death emergency concerning the data subject
V.	Processing is needed for the administration of justice

Point I of the DPA states that the data must be processed both fairly and lawfully. If one of the justifications on the above lists is applicable, then the data are being processed lawfully. However, that does not necessarily mean they are also being processed fairly. There are two main requirements for fair processing. First, the data subject must not be misled about anything concerning the data processing. Second, the data subject also must know the identities of the data processor and data controller.

**Point II: Purposes for Attaining Data**

When a data controller obtains data, he/she must obtain them only for specified lawful purposes. Thereafter, that data cannot be used for anything incompatible with those purposes. Herein lies an important distinction between the DPA and the Act of 1984. In the earlier Act, the data controller could simply notify the subject of a change in purpose after the data were collected, and then continue processing the data for the new purpose. Under the new legislation, this is no longer possible. Once the purposes have been stated, processing data for any reason not in accordance with the original purposes is illegal.

A data controller specifies the purposes of data collection and processing by notifying the data subject in accordance with the rules for fair processing described in Point I.

**Point III: Quantity of Data Shall be Adequate and Relevant**

The data processor is responsible for determining the minimum amount of information required for a given processing situation, and to ensure that only that amount of data are obtained. If there are individual exceptions to this requirement, more data can be collected for those specific individuals. However, extra data cannot be collected simply because the data controller believes that they will be useful or necessary at some point in the future. Only when there is a specific purpose (as per Point II) can data be obtained and held.

Changing circumstances call for constant monitoring of compliance with this point. If circumstances change and what was originally the minimum amount of data required becomes excessive or insufficient, efforts must be made to rectify the situation. Also, as circumstances change, data may become irrelevant. Again, it is the data controller's responsibility to either get rid of or obtain data to be compliant with this point.

**Point IV: Data Shall be Accurate and Current**

Data are considered inaccurate if they are either incorrect or misleading. If the data subject gives false data to the data controller, however, the data controller is not responsible.

Data only needs to be kept current if circumstances require it. For example, if the data are part of a historical database, then changing the historical data to make them current does not make sense. In almost all cases, however, data must be kept up to date.

### **Point V: Data Shall Not be Kept Longer Than Necessary**

In order to comply with this principle, data controllers must regularly review their data and compare them to the stated purposes for which the data were acquired. If the data are no longer needed for the stated purposes, then keeping them must be questioned. Sometimes, however, historical reasons for keeping data can be considered. Although not explicitly stated in the Act itself, keeping data for historical purposes appears to be an exception to Point II. Even if data were not obtained for an explicitly historical purpose, they can sometimes be kept for that reason. For example, if someone is employed at a company, that company will have certain personal data concerning that employee. When the employee leaves, however, some data may be kept for historical records, even though the original purpose for obtaining the data is no longer valid.

### **Point VI: Data Processed in Accordance with Subject's Rights**

The rights of the subject are essentially defined as a right to know who is processing the data, why they are processing them, and how long they will be processing them. The subject's rights are also discussed in the Human Rights Act of 1998. Information concerning that Act can be found in this appendix.

### **Point VII: Unlawful Data Processing**

Point VII says that a data controller is responsible for stopping unlawful data processing, if detected within the organisation. The controller is also responsible for stopping accidental loss of or damage to personal data. Both technical and organisational measures may be required to stop unlawful processing. Under this point, the data controller is responsible for taking reasonable steps to ensure the competency and trustworthiness of the staff processing the data. Topics such as passwords, building access, staff selection, and disposal of old data must be considered compliant with this point.

### **Point VIII: Data Transfer to Other Countries**

Data can legally be transferred to any country within the European Union. However, if a country is outside the European Union, that country must have data protection legislation similar to the United Kingdom's in order to obtain the data.

Exceptions to Point VIII, where the data transfer is acceptable irrespective of the data protection in the country to which the data is being transferred, are summarized in Table B-3.

**Table B-3: Exceptions to Point VIII**

I.	The data subject has given consent
II.	The transfer is necessary for contractual reasons
III.	The transfer is necessary for reasons of substantial public interest
IV.	The transfer is necessary for legal proceedings, or obtaining legal advice
V.	The transfer is necessary in order to protect the vial interests of the subject
VI.	The transfer is authorized by the Commissioner

### **Freedom of Information Act of 2000**

The Freedom of Information Act 2000 received Royal Assent on 30 November 2000. The Act provides a right of access to recorded information held by public authorities; creates exemptions from the duty to disclose information; and establishes the arrangements for

enforcement and appeal. The Act amends the Data Protection Act 1998 and the Public Records Act 1958. The Act has eight parts.

The Act creates new rights of access to information. It is intended to supersede the Code of Practice on Access to Government Information.

### **Part I: Access to information held by public authorities**

This provides for the general right of access to recorded information held by public authorities and specifies the conditions which need to be fulfilled before an authority is obliged to comply with a request.

### **Part II: Exempt information**

This states the circumstances in which information is "exempt information" for the purposes of the Act. Some of the exemptions apply to a class of information; others rely on the application of a prejudice test or other consequences of disclosure.

### **Part III: General functions of Secretary of State, Lord Chancellor and Information Commissioner**

This requires the Secretary of State to issue a code of practice providing guidance to public authorities on various administrative matters, including the practices which authorities should follow when dealing with requests for information. It also requires the Lord Chancellor to issue a code of practice providing guidance to public authorities on the keeping, management and destruction of their records.

Part III places a duty on the Commissioner to promote good practice and public authorities' compliance with the Act, their publication schemes and codes of practice. The Commissioner is also obliged, where he considers it expedient, to disseminate information to the public about the Act. The Commissioner is permitted to charge fees with the consent of the Secretary of State for such services. Part III also enables the Commissioner to make practice recommendations specifying what a public authority should do to comply with the codes of practice and requires the Commissioner to lay annual reports before Parliament.

### **Part IV: Enforcement**

This enables an applicant who is not satisfied with the response by a public authority to a request for information to apply to the Commissioner for a decision on whether the authority has acted in accordance with the provisions of the Act. Subject to certain conditions, for example, the exhaustion of other means of complaint, the Commissioner is under a duty to reach a decision.

This part of the Act also describes the investigative and enforcement powers of the Commissioner. The Commissioner's powers of entry and inspection are set out in Schedule 3. It confirms that the Act does not give rise to any right of action against public authorities for breach of statutory duty. This part also provides for the circumstances in which a certificate may be issued by an accountable person in respect of a decision notice or enforcement notice issued by the Commissioner in respect of the disclosure of exempt

information. The effect of such a certificate is that a public authority need not comply with the Commissioner's notice.

### **Part V: Appeals**

This states the circumstances in which an applicant or a public authority may appeal to the Tribunal when a decision notice, information notice, or enforcement notice has been served. It also states the circumstances in which a party to an appeal to the Tribunal can appeal to the courts on a point of law. It lays down the circumstances in which the Tribunal can hear appeals against the issue of a certificate in national security cases. It also provides for appeal procedures through amendments to the Data Protection Act 1998.

### **Part VI: Historical records and records in Public Record Office or Public Record Office of Northern Ireland**

This effectively replaces the largely discretionary provision for access to public records under the Public Records Act 1958 with a new statutory regime; provides for the access to be enhanced in respect of information contained in records more than thirty years old by disapplying a number of the exemptions in Part II; regulates the relationship between the Lord Chancellor (or appropriate Minister in Northern Ireland) and public authorities in relation to certain information contained in historical records, and makes further provision in relation to decisions relating to certain transferred public records.

### **Part VII: Amendments of Data Protection Act 1998**

With some exceptions and modifications this Part extends the Data Protection Act 1998 provisions about subject access and data accuracy to all personal information held by public authorities. Schedule 6 makes specific provision to extend the 1998 Act to include relevant personal information processed by or on behalf of both Houses of Parliament and makes other minor amendments to that Act.

### **Part VIII: Miscellaneous and supplemental**

This part:

- provides for a power to make provision relating to environmental information;
- provides for a power to repeal or amend existing statutory bars to disclosure;
- provides for disclosure of information between the Commissioner and specified ombudsmen. creates an offence of altering etc. records with intent to frustrate a right of access;
- saves existing powers of public authorities to disclose information;
- makes provision in respect of defamation;
- prevents the extension of the Act to the Scottish Parliament and certain devolved bodies;
- deals with the application of the Act to government departments and to Parliament and the Northern Ireland Assembly;
- defines the way in which orders or regulations can be made under the Act;
- defines various terms used in the Act; and
- gives effect to repeals of existing legislation.

Part VIII also sets out the commencement provisions for the Act. Those provisions in the Act which do not come into effect on, or at the end of the period of two months following, Royal Assent must be brought into force within the following five years unless brought into effect earlier by order of the Secretary of State; meanwhile, the Secretary of State must make annual reports to Parliament on progress towards full commencement.

### **Human Rights Act of 1998**

The Human Rights Act (HRA) of 1998 is very important to citizens of the United Kingdom. The HRA protects the rights citizens of the United Kingdom. There are several sections in the Act, many of which are similar to the Amendments to the Constitution of the United States of America. Most relevant to information security is Article 5: Personal Security.

Article 5 describes the right to liberty and security. Although data protection is not explicitly discussed in the HRA, the security extends to such issues. Personal security extends to personal information. For example, if criminals had access to a person's home address or phone number, they could use that information to commit theft or other crimes. The HRA strengthens the eight points described in the DPA because it creates harsher repercussions for lax data protection when personal security is involved.

### **British Standard 7799**

British Standard 7799 is a detailed document pertaining to information security and risk management that recommends structural changes for organisations. The first version of BS7799 was released in 1995. A second version was released in 1999 following the publication of the Data Protection Act of 1998, and that was the version that we considered. BS7799 no longer specific to the United Kingdom, as it has become an international standard (ISO/IEC 17799.) The fact that BS7799 was adopted as an international standard suggests that it is a reliable and important tool in assessing the overall information security status of an organisation (von Solms 3). There are two parts to BS7799, each part being a separate document. The first consists of a code of practice that should be followed for optimal information security. The second consists of specific measures that are to be taken in implementing an Information Security Management System (ISMS.)

### **Key Sections of BS7799: Part One**

BS7799 contains a detailed set of controls that satisfy information security requirements for most information technology environments. The first part consists of ten major sections that make describe the controls that should be in place to ensure information security.

1. Security Policy
2. Security Organisation
3. Assets Classification and Control
4. Personnel Security
5. Physical and Environmental Security
6. Computer and Network Management
7. System-Access Control
8. Systems Development and Maintenance

9. Business Continuity Planning
10. Compliance

Each of the sections is divided into subsections that detail the controls that are necessary. The second part is much shorter and is not as complex as the first part, but it states how the controls outlined in the first part should be put into place in order to create a successful ISMS. BS7799 does not prescribe the use of particular products to ensure information security; rather it recommends changes that would be beneficial to an organisation (Eloff and von Solms 9).

The ISP followed by the IT Division of the Merton Council ISP is based mostly on Part 2 of BS7799, although it is also based upon Part 2. BS7799 provides a reference point for identifying a wide range of information security that can be applied by many organisations, whether large, medium, or small (von Solms 3-4). There are several companies that have accepted BS7799 as a corporate standard, including Exxon, Shell, Motorola, and IBM. Many countries have also accepted BS7799 as a national standard, including Australia, New Zealand, Holland, Sweden, and Switzerland (von Solms 3-4).

By basing information security on BS7799, an organisation has the confidence that their practices are widely accepted as relevant and important internationally. BS7799 acts as a reference framework and provides the answers to an organisation's question as to whether or not they are missing any part of managing their risk and information security. Through the use of BS7799, an organisation can receive a certificate of compliance assuring E-commerce partners that the organisation is complying with a recognized international standard. This certification of compliance can prove an organisation's conformity to the BS7799 baseline and based on that they can demand the same from other organisations before being allowed into certain IT systems.

### **Information Security Policy Document**

BS7799 itself begins with an introduction that can be very useful in defining the necessity of the document to organisations. The first part of the introduction defines what information security is and why it is needed. The introduction goes on to describe how to establish security requirements and assess security risks. It outlines how to select controls once the security requirements have been identified and also identifies a starting point for an information security policy. There are several controls that are essential from a legislative point of view including data protection and privacy of personal information, safeguarding of organisational records, and intellectual property rights. There are also several controls considered common best practice for information security including the information security policy document, allocation of information security responsibilities, information security education and training, reporting security incidents and business continuity management. The introduction also outlines critical success factors, and how an organisation can develop its own guidelines.

Not all parts of the Standard are relevant for all organisations. It is important to understand what parts of the document are specifically important to the organisation in question. The first part of BS7799 explains to the reader what is to come later on. It goes on to say that the Standard gives recommendations for information security management as well as a common basis for developing organisational security standards and management.

The Standard dictates the contents of the ISP, as well as how it should be documented. The policy should be approved by management, published, and communicated to all employees. There is a minimum guidance requirement of what needs to be in the policy within BS7799. This guidance includes a definition of information security, a statement of

management intent, a brief explanation of the security policies of particular importance to the organisation, a definition of general and specific responsibilities for information security management, and references to documentation that may support the policy. The policy should have an owner who is responsible for its maintenance and review according to a defined review process. This review process should include the policy's effectiveness, the cost and impact of controls on business efficiency, and the effects of changes to technology.

Part One of BS7799 describes in detail the controls that must be implemented for compliance. To describe each of those aspects would be very lengthy, so instead each aspect that is specifically important to our project is briefly summarized below.

### **Organisational Security**

According to BS7799, informational security includes security within the organisation, an information security infrastructure and security of third party access (BS7799, 5). The information security infrastructure should include a management information security forum, information security co-ordination, allocation of information security responsibilities, an authorization procedure for processing facilities, specialist information security advice, co-operation between organisations, and an independent review of information security. Security of third party access includes identification of risks from third party access and security requirements in third party contracts.

### **Personnel Security**

Personnel security includes security in job definition and resourcing, which pertains to security in job responsibilities, personnel screening and policy, confidentiality agreements, and terms and conditions of employment. In order to be compliant with the Standard, organisations must include information security education and training, as well as responses to security incidents and malfunctions. Responses to breaks in information security consist in reporting security incidents and weaknesses, reporting software malfunctions, and learning from the incidents as well as a disciplinary process. Without some sort of a disciplinary process in place, there is no way to prevent multiple acts of personnel security breaches. With measures put into place to correct what has been done wrong, it is less likely that personnel will make the same errors repeatedly.

### **Communications and Operations Management**

Communications management includes operational procedures and responsibilities, system planning and acceptance, housekeeping, network management, media handling and security and exchanges of information and software. It may be important to Merton to know who specifically is having access to their computer system from a remote terminal and from where they have access. It may not be possible to stop this from happening completely, but it can and should be monitored.

### **Systems Development and Maintenance**

Once a system is developed, it must also be maintained. Some aspects of developing a system and making sure that it can be updated are security requirements of systems, security in application systems, security of system files, and security in development and support processes. If the security of the system is not developed, then there is no way to ensure that the files and other information stored in the system are protected. If the system is

not maintained, there is no way to guarantee that those same files are not going to be tampered with in the future. Without a framework that includes testing and re-assessing business continuity, there is no way that an organisation can be sure that their methods are up to date and complying with methods similar organisations are using.

## **Compliance**

The final section the first part of BS7799 that is relevant to our project is the compliance section. It provides guidelines for making sure that organisations comply with the necessary legal requirements, reviews of security policy and technical aspects, and system audits. If the policy of the organisation does not comply with the standards that are set forth, then the policy is not valid. It is imperative that legal requirements are met so that the organisation can avoid being prosecuted. Legal compliance includes identification of applicable legislation, safeguarding of organisational records, data protection and privacy of personal information, prevention of misuse of information processing facilities, regulation of cryptographic controls and the collection of evidence.

Compliance with the security policy and technical compliance checks is also significant. If an organisation has implemented a security policy, but the employees do not comply with it, it cannot be considered valid. A significant part of complying with the policy is performing checks on it to make sure that all aspects are being followed correctly. There are two considerations that must be taken for system audits: controls of the system audit and the protection of the tools necessary for a system audit. System audits must be done on a periodic basis to ensure that the information that being stored or transferred is current, available, and secure. It may be helpful to find an outside consultant to perform the audit since they are not biased.

## **Part Two**

The second part of BS7799 is actually applied when implementing an ISMS, or evaluating an ISP. There are six steps that should be followed in identifying and documenting an ISMS. The six steps are to:

1. Define the policy
2. Define the scope of the information security management system
3. Undertake a risk assessment
4. Manage the risk
5. Select controls and objectives of the controls to be implemented
6. Prepare a statement of applicability

Our project consisted of steps three through six of identifying and documenting the ISMS. BS7799 does not instruct the reader on how to do each of those steps. The reader is told what steps need to be taken, but is not detailed on how to take them. There are many different actions that an organisation may take to complete any of those steps. The second part of BS7799 outlines those actions, but does not include what should be done in any specific manner. It is a document that was produced by the government for organisations so they can use it in order to ensure that they are in compliance with all legislation. For many organisations, Part Two is the more useful of the two parts. It is shorter and easier to read and apply to an organisation than Part One is. Part Two is most influential when any organisation is making an information security policy, as it was in the case with the IT Services Division of the Merton Council.



## Appendix C: CRAMM Methodology

The first data collection operation we had to perform was the initiation phase. In this phase we were required to gather background information for the CRAMM review, and then identify all of our primary interviewees, and interviewers.

In phase two we identified and valued assets. Phase two of the software represents the first stage of any CRAMM exercise. There were three primary operations that had to be completed in order to complete this phase. The first involved modelling the system to be reviewed. We identified the primary assets that would be under review. Assets belong to one of five categories: physical, data, software, location, and end user services.

The second operation in phase one consisted of valuing the assets. We determined the cost and importance of all the assets. Appendices E through F summarise the relationship between cost and importance. The values given were recommended by CRAMM. After the data were collected, we entered them into the CRAMM review.

The final operation in the identification and valuation of assets phase consisted of contingency planning. This operation was mainly comprised of printing the data recovery reports, and then entering data recovery information.

Phase three of the software was the threat and vulnerability assessment phase, and it represents stage two of the CRAMM process. This phase has two primary operations. The first was the identification of threats to specific asset groups. We grouped the assets together by system, and then asked the system managers to identify all potential threats to those asset groups. The second operation involved quantitatively assessing the threat levels. After each system manager had identified the potential threats to their system we were able to print out the appropriate questionnaires for them to answer to gain the data that the CRAMM review needed to analyse the potential threats. This operation also consisted of printing the threat and vulnerability reports and summaries.

The last two phases of the software completed stage three of the CRAMM process. The fourth phase involved the risk analysis. This phase had three primary operations. The first was calculating the measures of the risks involved. This was primarily done by the software itself. The next operation was reviewing the measures of risks that were calculated previously. The third operation consisted of backtracking briefly through stages one and two, and then printing the risk analysis report.

The final phase of operations consisted of the actual risk management for the review. This phase had four major operations that had to be completed in order to make sure that all of the appropriate risks had been managed. The first consisted of identifying all the currently existing assets and entering them into the CRAMM review. We were then able to use the software to analyse, review, and make recommendations on the current situation. The next operation involved generating the risk management reports. Finally we identified all the current security resources in use that needed to be updated and made recommendations as to what should be changed.

# Appendix D: The Merton Information Security Policy

## Contents:

1. Introduction
2. Scope
3. Summary of Policy guidelines
4. Maintaining proper security controls
  - 4.1 Risks from Poor Maintenance of Proper Controls
  - 4.2 Recommended Guidelines
5. Passwords
  - 5.1 Risks from Poor Application of Password Control
  - 5.2 Recommended Guidelines
6. Securing data against accidental loss
  - 6.1 Risks from Accidental Loss
  - 6.2 Recommended Guidelines
7. Virus infection of computers
  - 7.1 Risks from the Introduction of Computer Viruses
  - 7.2 Recommended Guidelines
8. Unauthorised access (hacking)
  - 8.1 Risks from Unauthorised Access
  - 8.2 Recommended Guidelines
9. Deliberate damage to computer hardware and software, and from theft
  - 9.1 Risks from Deliberate Damage
  - 9.2 Risks from Theft
  - 9.3 Recommended Guidelines
10. Misuse of personal data in contravention of the Data Protection Act
  - 10.1 Risks from Misuse of Personal Data
  - 10.2 Recommended Guidelines
11. Misuse of the council's IT equipment
  - 11.1 Risks from Misuse of IT Equipment
  - 11.2 Recommended Guidelines
12. Use of Unlicensed Software
  - 12.1 Risks from Use of Unlicensed Software
  - 12.2 Recommended Guidelines
13. Fraud involving manipulation of computer systems
  - 13.1 Risks from Fraud
  - 13.2 Recommended Guidelines

## 1. INTRODUCTION

The subject of security covers a wide range of topics, and is particularly relevant to the use of Information Technology. This is due to the increasing reliance of organisations everywhere on IT in carrying out all virtually their functions. Information Technology also provides the most scope for breaches of security, as so many of the processes are visible just to those who are actually involved in them.

The Audit Commission carry out periodic surveys on IT fraud and abuse in the public sector, the most recent being published in February 1998. It concludes that despite substantial spending on security in some areas, there will always be scope for breaches to occur, due to poor awareness of the risks, human error and weaknesses in processes which have been put in place. The survey of course covers only known instances - it is still true that the majority of security breaches are discovered by accident rather than by auditing procedures.

This policy addresses the range of aspects of IT security under the headings shown below. It should be emphasised that the Audit Commission found that breaches of security rarely involve sophisticated methods. In most cases it was simply a lack of proper controls for audit, reconciliation and reporting which provided the loopholes.

## 2. SCOPE

The scope of this policy paper is as follows:

- Maintaining proper security controls
- Passwords
- Securing data against accidental loss
- Virus infection of computers
- unauthorised access (hacking)
- deliberate damage to computer hardware and software
- misuse of personal data in contravention of the Data Protection Act
- misuse of the council's IT equipment
- Fraud involving manipulation of computer systems

## 3. SUMMARY OF POLICY GUIDELINES

### **Maintaining Controls:**

1. that managers make time to ensure that all exception and other audit reports produced by computer systems are properly examined and followed up
2. that checks on the work of subordinates are viewed as an essential part of a manager's role, no matter how trusted or reliable the subordinates are
3. that for all new systems and changes to systems, access requirements are specified in full for each individual
4. that processes are put in place to ensure that permissions are removed immediately for employees who leave the council

### **Password security:**

5. the default password for a system should always be changed at the first opportunity

6. system facilities for forcing password changes at regular intervals should be used
7. generated passwords should be used for systems with several users
8. user-defined passwords should be difficult to guess. Names should not be used, neither should birthdays, football teams, or anything you are readily associated with
9. passwords should contain both letters and numbers
10. user-defined passwords should not be left unchanged for more than 2 months
11. passwords should always be changed if they become known to another person
12. if it is really necessary to write down a password, it should be where it won't be found by someone else

**Accidental Loss:**

13. arrange work so that will be possible to re-create inputs to a system for up to a week.
14. save work to the file server rather than on to a PC.
15. if work must be saved to a PC, take regular backups on to diskette.
16. test the ability to recover work from a backup before regarding it as a security asset.

**Virus Control:**

17. all council file servers will be maintained with the latest updates to the installed anti-virus software.
18. guidance will be available regarding the settings applicable to the client end of the software resident on PCs
19. the existing rules concerning the use of games software on council PCs and on the downloading of files from the Internet should be maintained.

**External Unauthorised Access:**

20. wherever possible, dial-up facilities should be supported by a call-back arrangement.
21. Modems within the council which are not part of dial-up facilities should not allow incoming calls.

**Malicious Damage:**

22. grant only the permissions which are needed for an individual's job function
23. ensure that regular and comprehensive backups are taken of data.

**Misuse Of Personal Data:**

24. grant only the permissions which are needed for an individual's job function
25. arrangements for the disposal of computers must include deletion of all data on them.
26. a data protection impact analysis should be included in any proposal to access data held on any information system, including any change to system interfaces.

**Misuse Of IT Equipment:**

27. managers to recognise the risk
28. modem accesses to the Internet are to be justified on business grounds

**Use of Unlicensed Software:**

29. That a policy of not introducing software to any PC or server, except through the approved IT acquisition process, is maintained.
30. That managers make checks on software usage part of their normal supervisory workload.
31. That the council's disciplinary procedure is used where necessary to back up the policy.
32. That software tools are used remotely to monitor the presence of executable programs on servers and PCs against licences, and that any apparently illegal software is reported to senior management.

## **4. MAINTAINING PROPER SECURITY CONTROLS**

### **4.1 Risks from Poor Maintenance of Proper Controls**

The main message to come out of the Audit Commission report is that the lack of proper controls is very often responsible for allowing breaches of security to take place. Instances are quoted where the work of trusted employees is not checked, where exception reports are not properly followed up, and where no check of permissions or accesses takes place. Passwords are an essential part of the controls, as described below, but equally important are the use of the security mechanisms which are built into systems, and regular checks to ensure that the principles of good security are being observed. Ideally, these checks should not be seen as an unwelcome intrusion into the work processes, but an integral part of them.

### **4.2 Recommended Guidelines**

The recommended guidelines for maintaining proper security controls are:

- that managers make time to ensure that all exception and other audit reports produced by computer systems are properly examined and followed up. These reports should be signed by the relevant manager, and the signed copies retained on file.
- that checks on the work of subordinates are viewed as an essential part of a manager's role, no matter how trusted or reliable the subordinates are.
- that for all new systems and changes to systems, access requirements are specified in full for each individual.
- that processes are put in place to ensure that permissions are removed immediately for employees who leave the council. It is proposed that this is achieved through a list to be provided by the Payroll section.

## **5. PASSWORDS**

### **5.1 Risks from Poor Application of Password Control**

The aspect of security most often seen by IT users is password access to systems. Passwords are commonplace and expected, but are liable to be circumvented to save time, particularly where the need for security is not obvious. Different systems have passwords which are either changed centrally or are under the user's control. Some systems force a password change at regular intervals and set down rules to which the password must conform (such as minimum length). User-defined passwords present

more risk than system-generated ones, although the latter are not easy to remember and tend to be written down, sometimes in obvious places. User-defined passwords will often be left unchanged for long periods of time, unless the system forces a change. Leaving a password set to the often-used default of "password" is well known as a risk, but equally important is the use of easily guessed words or names. It has been said that as many as one in 20 passwords are set to "Fred".

The risks associated with lack of password control include:

- fraud, through access to a system to generate or authorise transactions
- unauthorised access to personal or confidential information
- sending abusive or inappropriate e-mail purporting to be from someone else
- the introduction of computer viruses (see section 7).

It is in the interests of each member of staff to maintain the security of their passwords. Proper password security will protect them from allegations of misuse, whereas if they make a password available to someone else they may be liable for the consequences.

## **5.2 Recommended Guidelines**

The recommended policy guidelines for password security are:

- staff need to be made fully aware of their responsibilities for password security, and the consequences of allowing colleagues to use their passwords.
- the default password for a system should always be changed at the first opportunity.
- system facilities for forcing password changes at regular intervals should be used.
- generated passwords should be used for systems with several users.
- user-defined passwords should be difficult to guess. Names should not be used, neither should birthdays, football teams, or anything you are readily associated with.
- passwords should contain both letters and numbers.
- user-defined passwords should not be left unchanged for more than 2 months.
- passwords should always be changed if they become known to another person.
- if it is really necessary to write down a password, it should be where it won't be found by someone else.

## **6. SECURING DATA AGAINST ACCIDENTAL LOSS**

### **6.1 Risks from Accidental Loss**

Whilst this category of security cannot be included under "fraud and abuse", it still represents a significant risk to the council, due to the time and expense which could be involved in re-inputting or recovering data which has not been properly secured. Backup of corporate systems and file servers is provided as a service by the IT Services Division, but this does not cover information stored on PCs or any information held by schools. In these cases it must be the responsibility of the individual officer or department to take any backup copies which are required.

The backup policy for corporate systems is dependent on the needs of each of the systems. In most cases a full copy of the database or files is taken every week, with incremental copies daily. This will normally allow systems to be restored to within 24 hours of any problem occurring, and often a database can be recreated up to the exact point of failure by "rolling forward" using database journals. It will therefore sometimes be necessary for departments using these systems to be able to re-input work, and this may affect the way in which that work is organised.

## **6.2 Recommended Guidelines**

The recommended policy guidelines for securing data against accidental loss are:

- arrange work so that will be possible to re-create inputs to a system for up to a week.
- save work to the file server rather than on to a PC.
- if work must be saved to a PC, take regular backups on to diskette.
- test the ability to recover work from a backup before regarding it as a security asset.

## **7. VIRUS INFECTION OF COMPUTERS**

### **7.1 Risks from the Introduction of Computer Viruses**

Virus infection is becoming a significant aspect of security, and viruses are being introduced to council computers through two main routes. Firstly, the use of diskettes to bring work or games from home PCs which are infected, and secondly the download of infected files from the Internet.

The council's policy of installing anti-virus software on all servers is effective, but only if the software is kept up to date. It is also important that the software on each PC is correctly set to scan all files as they arrive at the machine, and repair any corrupt ones found. The restriction of the circumstances in which officers are allowed to introduce files will also be of benefit if it is properly enforced.

### **7.2 Recommended Guidelines**

The recommended guidelines for computer virus control are:

- all council file servers will be maintained with the latest updates to the installed anti-virus software.
- guidance will be available regarding the settings applicable to the client end of the software resident on PCs
- the existing rules concerning the use of games software on council PCs and on the downloading of files from the Internet should be more strongly enforced.

## **8. UNAUTHORISED ACCESS (HACKING)**

### **8.1 Risks from Unauthorised Access**

The Audit Commission acknowledges that unauthorised access from outside an organisation is rare. Where it occurs, it is usually through a username and password having been identified, combined with the means of connecting to the system concerned over a remote link. The guidelines above in respect of password security are therefore important to limit the risk from hackers.

There are routes available to connect to Merton's network from outside, using dial-up connections, and it is necessary to retain these, for business reasons. The telephone numbers to dial are readily available, but an opportunity for security is provided by the use of call-back facilities. Several modems exist within the council, and are used for Internet or other links. Pending the provision of centralised and controlled network links, modems should be set to enable dial-out, but not dial-in.

## **8.2 Recommended Guidelines**

The recommended guidelines for reducing the risk from external unauthorised access are:

- wherever possible, dial-up facilities should be supported by a call-back arrangement.
- Modems within the council which are not part of dial-up facilities should not allow incoming calls.

## **9. DELIBERATE DAMAGE TO COMPUTER HARDWARE AND SOFTWARE, AND FROM THEFT**

### **9.1 Risks from Deliberate Damage**

There is a risk to the council's computer equipment and systems from malicious damage by those who are aggrieved with Merton in one way or another, or from vandalism. The source of the aggression could be members of the public, or disgruntled employees. In the former case, damage is likely to be limited to hardware, and will be dealt with under the council's insurance policies. Malicious damage from employees, however, could extend to software, depending on the knowledge and access of the person concerned. The key to minimising this lies in taking all possible steps to prevent the occurrences. These will include thinking through the location of equipment in public areas, granting only the permissions which are needed for an individual's job function, and ensuring that regular and comprehensive backups are taken of the council's data.

### **9.2 Risks from Theft**

The high cost of computer equipment presents a real risk from theft, not only of whole items but of components within them. The security aspects include not only the security of the buildings in which the equipment is housed, but also the use of equipment security devices where appropriate, and security marking.

### **9.3 Recommended Guidelines**



The recommended guidelines for reducing the risk from malicious damage and theft are:

- consider the risk of damage when siting equipment in public areas.
- grant only the permissions which are needed for an individual's job function.
- ensure that regular and comprehensive backups are taken of data.
- consider the use of equipment security devices and property marking in areas where these may be useful.

## **10. MISUSE OF PERSONAL DATA IN CONTRAVENTION OF THE DATA PROTECTION ACT**

### **10.1 Risks from Misuse of Personal Data**

The Data Protection Act (DPA) controls the ways in which organisations can use the data they hold. The requirement for organisations to have regard to the protection of personal data is increasing - new focus is imposed by the European Data Protection Directive 95/46/EC which must be enforced by 24 October 1998. Staff may take available opportunities to access systems to find out personal information about friends or relatives, which is outside their usual job function. If it is within correctly defined access permissions it could still amount to a breach of confidentiality. It is also possible for data accesses to contravene the DPA inadvertently, if the requirements of the Act are overlooked.

There is also a risk of libel action in respect of something which is stated in an E-mail message. Whilst the risk is small, it needs to be borne in mind when sending messages of a controversial nature.

### **10.2 Recommended Guidelines**

The recommended guidelines for reducing the risk from misuse of personal data are:

- grant only the permissions which are needed for an individual's job function
- arrangements for the disposal of computers must include deletion of all data on them.
- a data protection impact analysis should be included in any proposal to access data held on any information system, including any change to system interfaces.
- Maintain a professional approach to using E-mail, and never include statements which may be interpreted as libellous.

## **11. MISUSE OF THE COUNCIL'S IT EQUIPMENT**

### **11.1 Risks from Misuse of IT Equipment**

This section refers to other ways in which staff may be able to use IT equipment in a way which is not in keeping with their job function. This can include the use of the facilities for private work, the playing of computer games in work time, and the use of Internet access facilities to download unsuitable material. This last type of misuse in

particular can become a security issue, as the risk of introducing computer viruses is greatly increased.

There are plans to route Internet accesses through a central firewall, which will be able to provide the necessary level of security. The guidelines below relate to the current situation, where modem access occurs in several different places within the authority.

## **11.2 Recommended Guidelines**

The recommended guidelines for reducing the risk from misuse of IT equipment are:

- managers to recognise the risk
- modem accesses to the Internet are to be justified on business grounds

## **12. USE OF UNLICENSED SOFTWARE**

### **12.1 Risks from Use of Unlicensed Software**

It is Merton's policy only to use software which has been acquired and licensed through the correct official channels. The availability of software on the Internet, and the ease with which it can be downloaded and sent to other computer users makes it difficult to control without a firm policy backed up by punitive action where necessary. The use of illegal software could:

- cause financial penalties for the council following investigation
- bring the name of the Council into disrepute following investigation
- encourage misuse of officers' time, especially where games are concerned
- cut across work to set and maintain standards.

It would be impossible to prevent all ways of loading illegal software, and to prevent all usage of it too. Therefore there needs to be a firm control on both the importing and the use of any illegal software.

### **12.2 Recommended Guidelines**

Other sections of this policy have already made reference to the need to control access to the Internet by restricting it to areas which have a recognised business need. The remaining recommended guidelines for reducing the risk from use of unlicensed software are:

- That a policy of not introducing software to any PC or server, except through the approved IT acquisition process, is maintained.
- That managers make checks on software usage part of their normal supervisory workload.
- That the council's disciplinary procedure is used where necessary to back up the policy.
- That software tools are used remotely to monitor the presence of executable programs on servers and PCs against licences, and that any apparently illegal software is reported to senior management.

## **13. FRAUD INVOLVING MANIPULATION OF COMPUTER SYSTEMS**

### **13.1 Risks from Fraud**

The Audit Commission survey identified that most fraud cases are discovered by accident, rather than by use of checks and inspections. It also found that staff in managerial positions were responsible for nearly a third of all fraud instances detected.

IT-related frauds are classified under four headings:

- those involving fraudulent input of data
- those involving the alteration of data held on computer
- the fraudulent use of output, and
- alteration of programs.

### **13.2 Recommended Guidelines**

The recommendations to reduce the risk of fraud are included in the section "Maintaining Proper Security Controls", above.

## Appendix E: Physical Asset Valuation Report

Name	Class	Number	Scale	Cost
<b>Cashiers Office</b>				
Cash Office Server	Host, Application Server	1	2	£30,000
Cash Office User Workstations	Fixed Location Intelligent Workstation	12	2	£9,600
<b>Cashiers Office Sub Total:</b>				<b>£39,600</b>
<b>Microsoft Exchange</b>				
Administration Workstations	Fixed Location Intelligent Workstation	4	2	£3,200
Best Value Workstations	Fixed Location Intelligent Workstation	2	2	£1,600
DSG Workstations	Fixed Location Intelligent Workstation	7	2	£5,600
Head of IT Workstation	Fixed Location Intelligent Workstation	1	2	£1,200
Portable Workstations	Workstation, Portable	5	2	£7,500
Service Desk Workstations	Fixed Location Intelligent Workstation	5	2	£4,000
Strategy and Quality Workstations	Fixed Location Intelligent Workstation	4	2	£3,200
System & Projects Workstations	Fixed Location Intelligent Workstation	18	3	£14,400
Exchange 1	Host, Application Server	1	3	£30,000
Exchange 2	Host, Application Server	1	3	£30,000
Exchange 3	Host, Application Server	1	3	£30,000
<b>Exchange Sub Total:</b>				<b>£130,700</b>
<b>Financial Accounting</b>				
FMIS User Workstation	Fixed Location Intelligent Workstation	60	4	£48,000
FMLS	Host, Database Serve, Application Server	1	4	£100,000
<b>Financial Account Sub Total:</b>				<b>£148,000</b>
<b>Mainframe Systems</b>				
HBIS User Workstations	Fixed Location Intelligent Workstation	50	4	£40,000
Council Tax User Workstations	Fixed Location Intelligent Workstation	40	4	£32,000
SOSCIS User Workstations	Fixed Location Intelligent Workstation	100	4	£80,000
ICL VME	Host, Database, Application Server	1	5	£250,000
<b>Mainframe Systems Sub Total:</b>				<b>£402,000</b>
<b>Housing Rents and Repairs</b>				
HRR User Workstations	Fixed Location Intelligent Workstation	70	4	£56,000
Thresh Live	Host, Database, Application Server	1	4	£100,000
<b>Housing Rents and Repairs Sub Total:</b>				<b>£156,000</b>
<b>Payroll System</b>				
HR User Workstations	Fixed Location Intelligent Workstation	25	3	£20,000
HR Server	Host, Database, Application Server	1	3	£30,000
<b>Payroll System Sub Total:</b>				<b>£50,000</b>

**TOTAL REPLACEMENT COST: £926,300**

## Appendix F: Data Asset Valuation Report

<b><i>Cashiers Office</i></b>		
<b>Impact</b>	<b>Guideline</b>	<b>Scale Value</b>
Unavailability - 12 Hours	Disruption to Activities	4
Unavailability - 1 Week	Disruption to Activities	4
Total Destruction (including backups)	Disruption to Activities	2
Unauthorized disclosure (service providers)	Loss of goodwill	1
<b><i>Council Tax</i></b>		
<b>Impact</b>	<b>Guideline</b>	<b>Scale Value</b>
Unavailability - 3 hours	Disruption to Activities	1
Unavailability - 1 day	Disruption to Activities	2
Unauthorised disclosure to outsiders	Legal and Regulatory Obligations	1
Wide-spread errors	Disruption to Activities	4
Deliberate modification	Financial Loss	1
<b><i>Microsoft Exchange</i></b>		
<b>Impact</b>	<b>Guideline</b>	<b>Scale Value</b>
Unavailability - less than 15 minutes	Disruption to Activities	1
Unavailability - 3 hours	Disruption to Activities	2
Unavailability - 1 day	Disruption to Activities	2
Unavailability - 2 day	Disruption to Activities	3
Unavailability - 1 week	Disruption to Activities	4
Total destruction including back-ups	Disruption to Activities	1
Wide-spread errors	Disruption to Activities	1
Deliberate modification	Security and Intelligence	1
<b><i>Financial Accounting</i></b>		
<b>Impact</b>	<b>Guideline</b>	<b>Scale Value</b>
Unavailability - 1 hour	Disruption to Activities	1
Unavailability - 1 day	Disruption to Activities	2
Unavailability - 1 week	Disruption to Activities	4
Destruction since last successful backup	Management and Business Operation	6
Total destruction including back-ups	Policy and Operations of Public Service	7
Unauthorised disclosure to outsiders	Personal Information	3
Deliberate Modification	Policy and Operations of Public Service	4
<b><i>Housing Rents and Repairs</i></b>		
<b>Impact</b>	<b>Guideline</b>	<b>Scale Value</b>
Unavailability - 3 hours	Disruption to Activities	1
Unavailability - 1 week	Disruption to Activities	3
Total destruction including back-ups	Disruption to Activities	4
Wide-spread errors	Financial Loss	3

**Housing Benefits**

<b>Impact</b>	<b>Guideline</b>	<b>Scale Value</b>
Unavailability - less than 15 minutes	Disruption to Activities	1
Unavailability - 1 hour	Loss of goodwill	1
Unavailability - 1 day	Disruption to Activities	2
Unavailability - 1 week	Loss of goodwill	2
Total destruction including back-ups	Management and Business Operations	4
Unauthorised disclosure to outsiders	Personal Information	1
Small scale errors	Loss of goodwill	1
Wide-spread errors	Legal and Regulatory Obligations	3
Deliberate modification	Financial Loss	1
Non-delivery	Legal and Regulatory Obligations	1

**Payroll System**

<b>Impact</b>	<b>Guideline</b>	<b>Scale Value</b>
Unavailability - 1 hour	Disruption to Activities	1
Unavailability - 1 day	Disruption to Activities	2
Unavailability - 1 week	Disruption to Activities	3
Destruction since last successful backup	Management and Business Operation	5
Total destruction including back-ups	Management and Business Operation	6
Unauthorised disclosure to outsiders	Personal Information	4
Small scale errors	Disruption to Activities	2
Wide-spread errors	Management and Business Operation	5
Deliberate modification	Financial Loss	1

**SOSCIS**

<b>Impact</b>	<b>Guideline</b>	<b>Scale Value</b>
Unavailability - 1 day	Disruption to Activities	1
Unavailability - 2 days	Disruption to Activities	2
Unavailability - 2 weeks	Disruption to Activities	3
Total destruction including back-ups	Disruption to Activities	2
Unauthorised disclosure to outsiders	Personal Safety	1

## Appendix G: Software Asset Valuation Report

Software Asset: **Cashiers Office Software**  
 Type of Software: Package Financial  
 Annual Contract Cost: £10,500

Impact	Guideline	Scale
Unavailability - 12 Hours	Disruption to Activities	4
Unavailability - 1 Week	Disruption to Activities	4

Software Asset: **Council Tax Software**  
 Type of Software: Package Financial  
 Annual Contract Cost: £16,800

Unavailability - 3 hours	Disruption to Activities	1
Unavailability - 1 day	Disruption to Activities	2
Unavailability - 1 week	Disruption to Activities	4

Software Asset: **Housing Benefits Software**  
 Type of Software: Package Financial, Funds Transfer, Personal Information  
 Annual Contract Cost: £12,900

Unavailability - 15 minutes or less	Disruption to Activities	1
Unavailability - 1 hour	Loss of goodwill	1
Unavailability - 1 day	Disruption to Activities	2
Unavailability - 1 week	Loss of goodwill	2

Software Asset: **Housing Rents and Repairs Software**  
 Type of Software: Package Financial, General, Personal Information  
 Annual Contract Cost: £13,100

Unavailability - 3 hours	Disruption to Activities	1
Unavailability - 1 week	Disruption to Activities	3

Software Asset: **Microsoft Exchange**  
 Type of Software: Package General, Personal Information  
 Annual Contract Cost:

Unavailability - 15 minutes or less	Disruption to Activities	1
Unavailability - 3 hours	Disruption to Activities	2
Unavailability - 1 day	Disruption to Activities	2
Unavailability - 2 day	Disruption to Activities	3
Unavailability - 1 week	Disruption to Activities	4

Software Asset: **PS Enterprise**  
 Package Financial, Funds Transfer, Personal Information, Safety  
 Type of Software: Critical  
 Annual Contract Cost: £80,000

Unavailability - 1 hour	Disruption to Activities	1
Unavailability - 1 day	Disruption to Activities	2
Unavailability - 1 week	Disruption to Activities	3

Software Asset: **SOSCIS**  
 Type of Software: Package Personal Information  
 Annual Contract Cost: £44,500

Unavailability - 1 day	Disruption to Activities	1
Unavailability - 2 days	Disruption to Activities	2
Unavailability - 2 weeks	Disruption to Activities	3



## Appendix H: Definition of Threats

1. *Masquerading of User Identity by Insiders* – This threat covers attempts by authorised users to gain access to information to which they have not been granted access. These users may attempt to gain access to that information by posing as another user.

2. *Masquerading of User Identity by Contracted Service Providers* – This threat covers attempts by people working for a contracted service provider to obtain unauthorised access to information by posing as another person.

3. *Masquerading of User Identity by Outsiders* – This threat covers attempts by outsiders to obtain unauthorised access to information by posing as an authorised user.

4. *Unauthorised Use of an Application* – This threat covers the possibility of someone using an account that they have been granted access to, but for unauthorised purposes. For example, a pay clerk using the payroll application to make unauthorised increase in his/her own pay

*Introduction of Damaging or Disruptive Software*

6. *Misuse of System Resources* – This threat covers people using the organisation's facilities for non-work related activities, such as:

- using word processing facilities for personal correspondence
- using development facilities to create programs for external organisations
- using access to the Internet to browse non-work related sites.

7. *Communications Infiltration* – This threat covers the following types of events:

- Hacking into a system using, for example, buffer overflow attacks
- Masquerading as a server
- Masquerading as an existing user of an e-commerce application
- Masquerading as a new user of an e-commerce application
- Denial of service (deliberate)
- Flaming attacks
- Spamming.

8. *Communications Interception* – This threat covers:

- Passive interception
- Traffic monitoring

The ease of interception is determined by two basic factors:

- The medium of the transmission
- The type of protocols being used

Interception of some types of traffic on the Internet is relatively easy. It can be achieved by attackers sending messages to target systems instruction them to send traffic via specific (hostile) machines.

9. *Communications Manipulation* – This threat covers:

- Active interception
- Insertion of false messages
- Deliberate delivery out of sequence
- Deliberate delay of delivery
- Deliberate mis-routing

If an attacker can force a message to be sent via a hostile host, the attacker may be in a position to intercept, alter and the forward the message.

10. *Repudiation* – This threat covers:

- People denying that they sent a message (repudiation of origin)
- People denying that they received a message (repudiation of receipt).

11. *Communications Failure* – This threat covers:

- Unavailability of Service Provider
- Failure of data link
- Non-delivery of message
- Accidental delivery out of sequence
- Accidental delay in delivery
- Accidental denial of service.

The Internet does not provide a service level agreement. There are no guarantees on how long it will take for a message to get to a recipient, or even that it will get there eventually.

12. *Embedding of Malicious Code* – This threat covers: - e-mail viruses  
- hostile mobile code (ex: hostile Active X applets)

E-mail viruses are now more common than disk viruses. Once on a network they can quickly infect many machines causing significant disruption. Java and Active X raise a range of new security concerns. Users are now running code written by people from outside of the organisation, sometimes from unknown sources. This code has often not been tested by the organisation. There are concerns that hostile code written using these types of techniques could inflict damage on systems and networks.

13. *Accidental Mis-routing* – This threat covers the possibility that information might be delivered to an incorrect address when it is being sent over a network.

14. *Technical Failure of Host* – This threat identifies the factors that increase the likelihood of failure of a host. The vulnerability to host failure depends on the ease of resuming service following such a failure.

15. *Technical Failure of Storage Facility* – This threat identifies the factors that increase the likelihood of failure of a storage facility. The vulnerability to storage facility failure depends on the ease of resuming service following a failure.

16. *Technical Failure of Print Facility* – This threat identifies the factors that increase the likelihood of failure of a print facility. The vulnerability to print facility failure depends on the ease of resuming service following a failure.

17. *Technical Failure of Network Distribution Component* – This threat identifies the factors that increase the likelihood of failure of such a component. The vulnerability to network distribution component failure depends on the ease of resuming service following a failure.

18. *Technical Failure of Network Gateway* – This threat identifies the factors that increase the likelihood of failure of a gateway. The vulnerability to network gateway failure depends on the ease of resuming service following a failure.

19. *Technical Failure of Network Management of Operation Host* – This threat identifies the factors that increase the likelihood of failure of such a component. The vulnerability to network management host or operations failure depends on the ease of resuming service following a failure.

20. *Technical Failure of Network Interface* – This threat of failure of a network interface identifies the factors that increase the likelihood of failure of a network interface. The vulnerability to network interface failure depends on the ease of resuming service following a failure.

21. *Technical Failure of Network Service* – This threat of failure of a network service identifies the factors that increase the likelihood of failure of a network service. The vulnerability to network service failure depends on the ease of resuming service following a failure.

22. *Power Failure* – This threat covers the possibility that the power supply to the building may fail.

23. *Air Conditioning Failure* – This threat covers the possibility that work may have to be suspended because temperatures in the location fall outside of acceptable parameters, due to the failure of air conditioning units.

24. *System and Network Software Failure* – This threat covers the possibility that the system or network software might fail, causing not just a loss of service, but also potentially weakening other security mechanisms.

25. *Application Software Failure* – This threat covers the possibility of errors being contained in application programs.

26. *Operations Error* – This threat covers the possibility that the people responsible for operating the host system might make mistakes when carrying out their work.

27. *Hardware Maintenance Error* – This threat covers the possibility that those people responsible for maintaining the hardware might make mistakes when carrying out their work.

28. *Software Maintenance Error* – This threat covers the possibility that those people or organisations responsible for maintaining software might make mistakes when carrying out their work.

29. *User Error* – This threat covers the possibility that the users might make mistakes when using an application.

30. *Fire* – This threat covers the possibility of fire affecting any of the physical assets that make up a system including documentation and magnetic media. The vulnerability of a building or room to fire depends on the extent to which a fire would spread once it had started and the extent to which it would affect the business processes.

31. *Water Damage* – This threat covers the possibility of water affecting any of the physical assets that make up a system including documentation and magnetic media. The vulnerability of a building or room to water damage depends on the extent to which water could enter the room and damage the equipment in it and the extent to which it would affect the business processes.

32. *Natural Disaster* – This threat covers the possibility of either a natural event, or man made (such as traffic accidents), causing physical damage to the location or surrounding area. The vulnerability of the area/ location depends on the extent to which a disaster would affect the business processes.

33. *Staff Shortage* – The threat of staff shortage covers the possibility of the absence of key personnel for whatever reason and the ease with which they could be replaced. The vulnerability to staff shortage depends on the extent to which shortage of staff would affect the business processes.

34. *Theft by Insiders* – This threat covers documentation, which incorporates information, as well as physical assets. This questionnaire relates to thefts by insiders. This would include anybody who had a legitimate reason to be working in the building such as cleaners, contractors etc. The level of the threat derives mainly from the number of previous incidents, the type of theft i.e. petty or not, if the theft was carried out by insiders and the morale of staff. The vulnerability is primarily dependent on the effect on business processes and the time it would take to replace the equipment.

35. *Theft by Outsiders* – This threat covers the theft of documentation, which incorporates information as well as physical assets. The questionnaire relates to thefts by outsiders i.e. where there has been a break in. The vulnerability to theft depends on the ease to which assets can be removed and the time it takes to replace them.

36. *Wilful Damage by Insiders* – This threat covers acts of vandalism and other cases where physical damage is caused to IT systems or their supporting environment by people who have been granted access to the building.

37. *Wilful Damage by Outsiders* – This threat covers acts of vandalism and other cases where physical damage is caused to IT systems or their supporting environment by people who have not been granted access to the building.

38. *Terrorism* – The threat of terrorism has been separated from the more general act of wilful damage by outsiders. It covers the actions of organised groups seeking to pursue political objectives by force.

# Appendix I: Sample CRAMM Questionnaire

CRAMM V4.0  
Questionnaires

Blank Threat and Vulnerability  
Review: Merton IT RA

Merton IT Services Risk Assessment

## Threat: Technical Failure of Host

This threat of failure of a host identifies the factors that increase the likelihood of failure of a host.

The vulnerability to host failure depends on the ease of resuming service following such a failure.

### Threat Questionnaire

- |   |   |    |
|---|---|----|
| 1 | Is the network host between 1 and 6 years old?  |    |
|   | Possible Answer   |    |
| a | Yes   | 0  |
| b | No  | 10 |
| 2 | Is the network host of a new and innovative design that is, as yet, not widely proven?  |    |
|   | Possible Answer   |    |
| a | Yes   | 10 |
| b | No  | 0  |
| 3 | Has the network host been specially adapted for the installation?   |    |
|   | Possible Answer   |    |
| a | Yes   | 10 |
| b | No  | 0  |
| 4 | Is the network host used in a non-standard manner, or in a manner for which it was not intended?  |    |
|   | Possible Answer   |    |
| a | Yes   | 15 |
| b | No  | 0  |
| 5 | Is the network host operated in an environment outside of the manufacturer's recommended environmental specification (e.g. temperature, power, humidity, dust)? |    |
|   | Possible Answer   |    |
| a | Yes   | 35 |
| b | No  | 0  |
| 6 | Is the network host operated close to the limits of its expected capabilities?  |    |
|   | Possible Answer   |    |
| a | Yes   | 30 |
| b | No  | 0  |

110

7 How many incidents of technical failure of a network host have occurred in the last 3 years?

Possible Answer

- |   |                                  |    |
|---|----------------------------------|----|
| a | None                             | 0  |
| b | One or two                       | 15 |
| c | On average, one a year           | 25 |
| d | On average, more than one a year | 35 |
| e | Unknown                          | 15 |

8 What is the trend in the number of failures of the network host?

Possible Answer

- |   |                              |     |
|---|------------------------------|-----|
| a | Increasing                   | 10  |
| b | Remaining constant / Unknown | 0   |
| c | Decreasing                   | -10 |

### Vulnerability Questionnaire

1 Would the failure of any single component result in loss of service to the users?

Possible Answer

- |   |                   |    |
|---|-------------------|----|
| a | Yes, total loss   | 30 |
| b | Yes, partial loss | 10 |
| c | No                | 0  |

2 Is it possible to reconfigure the system to overcome technical failure of the network host to prevent the above effect?

Possible Answer

- |   |     |   |
|---|-----|---|
| a | Yes | 0 |
| b | No  | 5 |

3 Could replacement assets be provided in timescales that would prevent the above effect, e.g. via a maintenance contract?

Possible Answer

- |   |     |   |
|---|-----|---|
| a | Yes | 0 |
| b | No  | 5 |

4 Is it likely that a technical failure of the network host could be repaired within 15 minutes?

Possible Answer

- |   |  |    |
|---|--|----|
| a | Could not be repaired within this timeframe          | 75 |
| b | Unlikely to be fixed                                 | 50 |
| c | Normally fixed                                       | 25 |
| d | The failure could always fixed within this timeframe | 0  |

5 Is it likely that a technical failure of the network host could be repaired within 1 hour?

Possible Answer

- |   |  |    |
|---|--|----|
| a | Could not be repaired within this timeframe          | 75 |
| b | Unlikely to be fixed                                 | 50 |
| c | Normally fixed                                       | 25 |
| d | The failure could always fixed within this timeframe | 0  |

- 6 Is it likely that a technical failure of the network host could be repaired within 3 hours?  
Possible Answer
- |   |  |    |
|---|--|----|
| a | Could not be repaired within this timeframe          | 75 |
| b | Unlikely to be fixed                                 | 50 |
| c | Normally fixed                                       | 25 |
| d | The failure could always fixed within this timeframe | 0  |
- 7 Is it likely that a technical failure of the network host could be repaired within 12 hours?  
Possible Answer
- |   |  |    |
|---|--|----|
| a | Could not be repaired within this timeframe          | 75 |
| b | Unlikely to be fixed                                 | 50 |
| c | Normally fixed                                       | 25 |
| d | The failure could always fixed within this timeframe | 0  |
- 8 Is it likely that a technical failure of the network host could be repaired within 1 day?  
Possible Answer
- |   |  |    |
|---|--|----|
| a | Could not be repaired within this timeframe          | 75 |
| b | Unlikely to be fixed                                 | 50 |
| c | Normally fixed                                       | 25 |
| d | The failure could always fixed within this timeframe | 0  |
- 9 Is it likely that a technical failure of the network host could be repaired within 2 days?  
Possible Answer
- |   |  |    |
|---|--|----|
| a | Could not be repaired within this timeframe          | 75 |
| b | Unlikely to be fixed                                 | 50 |
| c | Normally fixed                                       | 25 |
| d | The failure could always fixed within this timeframe | 0  |

## Appendix J: Employee Identified Threats

Ray McInnis (Central Postroom Manager) – Cashier’s Office

- Introduction of Damaging or Disruptive Software
- Technical Failure of Print Facility
- System and Network Software Failure
- Fire
- Theft by Outsiders

Tracey Hawkins (Senior User) – Housing Benefits

- Masquerading of User Identity by Outsiders
- Unauthorized Use of an Application
- System and Network Software Failure
- Application Software Failure
- Operations Error

Krystyna Kiuber (Analyst Programmer) – Housing Benefits

- Technical Failure of Network Service
- System and Network Software Failure
- Hardware Maintenance Error
- Natural Disaster

Colin Mason (Analyst Programmer) – Housing Rents and Repairs

- Misuse of System Resources
- Technical Failure of Host
- Technical Failure of Network Service
- Power Failure
- System and Network Software Failure

John Sykes (ISS HSG Team Leader) – Housing Rents and Repairs

- Introduction of Damaging or Disruptive Software
- Communications Failure
- Technical Failure of Host
- Technical Failure of Network Service
- Application Software Failure

Peter Brown (Analyst Programmer) – Council Tax

- Communications Failure
- Technical Failure of Network Host
- Air Conditioning Failure
- Operations Error
- Hardware Maintenance Error
- Staff Shortage

Colin Lloyd (Systems Control Manager) – Council Tax

- Air Conditioning Failure

- Hardware Maintenance Error
- Software Maintenance Error
- User Error
- Staff Shortage

Steve Key (Payroll Manager) – Payroll System

- Technical Failure of Host
- Application Software Failure
- Software Maintenance Error
- User Error
- Staff Shortage

Felix Stride-Darnley (ISS Team Leader) - SOSCIS

- Technical Failure of Storage Facility
- System and Network Software Failure
- Application Software Failure
- Fire
- Terrorism

Robert Heap (Analyst Programmer) – Financial Accounting

- Masquerading of User Identity by Insiders
- Unauthorised Use of an Application
- Technical Failure of Host
- Power Failure
- Application Software Failure
- User Error

Mark Kitson (Desktops & Servers Engineer) – Microsoft Exchange

- Masquerading of User Identity by Contracted Service Providers
- Masquerading of User Identity by Outsiders
- Misuse of System Resources
- Communications Infiltration
- Communications Manipulation
- Theft by Outsiders



## Appendix K: Threat and Vulnerability Report

Threats and Systems Affected	Threat Level	Vulnerability Level
<b>Masquerading of Identity by Insiders</b>		
Financial Accounting	<i>Very High</i>	<i>High</i>
<b>Masquerading of Identity by Contractors</b>		
Exchange and Outlook	<i>Very Low</i>	<i>High</i>
<b>Masquerading of Identity by Outsiders</b>		
Housing Benefits	<i>Very High</i>	<i>Medium</i>
Exchange and Outlook	<i>Very High</i>	<i>Medium</i>
<b>Unauthorised Use of an Application</b>		
Housing Benefits	<i>Medium</i>	<i>High</i>
Financial Accounting	<i>Medium</i>	<i>Medium</i>
<b>Introduction of Damaging Software</b>		
Housing Rents and Repairs	<i>Low</i>	<i>High</i>
Cashier's Office	<i>Low</i>	<i>High</i>
<b>Misuse of System Resources</b>		
Exchange and Outlook	<i>Low</i>	<i>Medium</i>
Housing Rents and Repairs	<i>Medium</i>	<i>Medium</i>
<b>Communications Infiltration</b>		
Exchange and Outlook	<i>Very Low</i>	<i>Medium</i>
<b>Communications Manipulation</b>		
Exchange and Outlook	<i>Very Low</i>	<i>High</i>
<b>Communications Failure</b>		
Council Tax	<i>Very High</i>	<i>High</i>
Housing Rents and Repairs	<i>High</i>	<i>High</i>
<b>Technical Failure of Host</b>		
Council Tax	<i>Medium</i>	<i>Low</i>
Financial Accounting	<i>Low</i>	<i>Low</i>
PS Enterprise	<i>Medium</i>	<i>High</i>
Housing Rents and Repairs	<i>Medium</i>	<i>High</i>
<b>Technical Failure of Storage Facility</b>		
Housing Benefits	<i>Medium</i>	<i>High</i>
SOSCIS	<i>Medium</i>	<i>High</i>
<b>Technical Failure of Print Facility</b>		
Cashier's Office	<i>Medium</i>	<i>Low</i>
<b>Technical Failure of Network Service</b>		
Housing Benefits	<i>Low</i>	<i>High</i>
Housing Rents and Repairs	<i>High</i>	<i>Medium</i>
<b>Power Failure</b>		
Financial Accounting	<i>Low</i>	<i>Low</i>
Housing Rents and Repairs	<i>High</i>	<i>Medium</i>

<b>Air Conditioning Failure</b>		
Council Tax	<i>Very High</i>	<i>Medium</i>
<b>System and Network Software Failure</b>		
Housing Benefits	<i>Medium</i>	<i>High</i>
Housing Rents and Repairs	<i>Very High</i>	<i>High</i>
Cashier's Office	<i>Very High</i>	
SOSCIS	<i>Medium</i>	<i>High</i>
<b>Application Software Failure</b>		
Housing Benefits	<i>Very High</i>	<i>High</i>
Financial Accounting	<i>Very High</i>	<i>High</i>
PS Enterprise	<i>Very High</i>	<i>High</i>
Housing Rents and Repairs	<i>Very High</i>	<i>High</i>
SOSCIS	<i>Low</i>	<i>High</i>
<b>Operations Error</b>		
Council Tax	<i>Medium</i>	<i>High</i>
Housing Benefits	<i>Medium</i>	<i>High</i>
<b>Hardware Maintenance Error</b>		
Council Tax	<i>Very High</i>	<i>High</i>
Housing Benefits	<i>Very High</i>	<i>High</i>
<b>Software Maintenance Error</b>		
Council Tax	<i>Very Low</i>	<i>Medium</i>
PS Enterprise	<i>Medium</i>	<i>Medium</i>
<b>User Error</b>		
Council Tax	<i>Very High</i>	<i>High</i>
Financial Accounting	<i>Very High</i>	<i>High</i>
PS Enterprise	<i>Very High</i>	<i>High</i>
<b>Fire</b>		
Cashier's Office	<i>Low</i>	<i>High</i>
SOSCIS	<i>Medium</i>	<i>High</i>
<b>Natural Disaster</b>		
Housing Benefits	<i>Very Low</i>	<i>High</i>
<b>Staff Shortage</b>		
Council Tax	<i>Low</i>	<i>Low</i>
PS Enterprise	<i>Very Low</i>	<i>High</i>
<b>Theft by Outsiders</b>		
Exchange and Outlook	<i>Medium</i>	
Cashier's Office	<i>Very Low</i>	<i>Low</i>
<b>Terrorism</b>		
SOSCIS	<i>Very Low</i>	<i>High</i>

## Appendix L: Measure of Risk (MoR) Report

<b>Asset: Cashier's Office</b>	<b>Threat</b>	<b>Vulnerability</b>	<b>Impact</b>	<b>MOR</b>
<b>Threat: Introduction of Damaging Software</b>				
UNAVAILABLE – 12 HOURS	L	H	4	3
UNAVAILABLE – 1 DAY	L	H	4	3
UNAVAILABLE – 2 DAYS	L	H	4	3
FULL DESTRUCTION	L	H	2	2
<b>Threat: Technical Failure of Print Facility</b>				
UNAVAILABLE – 12HOURS	M	L	4	3
<b>Threat: Fire</b>				
PHYSICAL DESTRUCTION	L	H	3	3
UNAVAILABLE – 12 HOURS	L	H	4	3
UNAVAILABLE – 1 DAY	L	H	4	3
UNAVAILABLE – 2 DAYS	L	H	4	3
UNAVAILABLE – 1 WEEK	L	H	4	3
UNAVAILABLE – 2 WEEKS	L	H	4	3
UNAVAILABLE – 1 MONTH	L	H	4	3
UNAVAILABLE – 2 MONTHS	L	H	4	3
<b>Threat: Theft by Outsiders</b>				
PHYSICAL DESTRUCTION	VL	L	3	1
UNAVAILABLE – 12 HOURS	VL	L	4	2
UNAVAILABLE – 1 DAY	VL	L	4	2
UNAVAILABLE – 2 DAYS	VL	L	4	2

<b>Asset: Council Tax</b>	<b>Threat</b>	<b>Vulnerability</b>	<b>Impact</b>	<b>MOR</b>
<b>Threat: Communications Failure</b>				
UNAVAILABLE – 15 MINUTES	VH	H	1	3
UNAVAILABLE – 1 HOUR	VH	H	1	3
UNAVAILABLE – 3 HOURS	VH	H	1	3
UNAVAILABLE – 12 HOURS	VH	H	1	3
UNAVAILABLE – 1 DAY	VH	H	2	4
UNAVAILABLE – 2 DAYS	VH	H	2	4
NON-DELIVERY	VH	H	1	3
<b>Threat: Technical Failure of Host</b>				
UNAVAILABLE – 15 MINUTES	M	L	1	1
UNAVAILABLE – 1 HOUR	M	L	1	1
UNAVAILABLE – 3 HOURS	M	L	1	1
UNAVAILABLE – 12 HOURS	M	L	1	1
UNAVAILABLE – 1 DAY	M	L	2	2
UNAVAILABLE – 2 DAYS	M	L	2	2
<b>Threat: Air Conditioning Failure</b>				
UNAVAILABLE – 15 MINUTES	VH	M	1	2
UNAVAILABLE – 1 HOUR	VH	M	1	2
UNAVAILABLE – 3 HOURS	VH	M	1	2
UNAVAILABLE – 12 HOURS	VH	M	1	2
UNAVAILABLE – 1 DAY	VH	M	2	3
<b>Threat: Operations Error</b>				

UNAVAILABLE – 15 MINUTES	M	M	1	1
UNAVAILABLE – 1 HOUR	M	L	1	1
UNAVAILABLE – 3 HOURS	M	L	1	1
UNAVAILABLE – 12 HOURS	M	L	1	1
FULL DESTRUCTION	VL	L	4	2
DISCLOSURE OF DATA TO OUTSIDERS	VL	M	2	1
SMALL SCALE MODIFICATION	VL	M	1	1
WIDE-SPREAD MODIFICATION	VL	L	4	2
<b>Threat: Hardware Maintenance Error</b>				
UNAVAILABLE – 15 MINUTES	VH	H	1	3
UNAVAILABLE – 1 HOUR	VH	H	1	3
UNAVAILABLE – 3 HOURS	VH	H	1	3
UNAVAILABLE – 12 HOURS	VH	L	1	2
UNAVAILABLE – 1 DAY	M	L	2	2
DISCLOSURE OF DATA TO OUTSIDERS	M	L	2	2
NON-DELIVERY	M	L	1	1
<b>Threat: Software Maintenance Error</b>				
UNAVAILABLE – 15 MINUTES	VL	M	1	1
UNAVAILABLE – 1 HOUR	VL	M	1	1
UNAVAILABLE – 3 HOURS	VL	M	1	1
UNAVAILABLE – 12 HOURS	VL	L	1	1
SMALL SCALE MODIFICATION	VL	L	1	1
WIDE-SPREAD MODIFICATION	VL	L	4	2
NON-DELIVERY	VL	L	1	1
<b>Threat: User Error</b>				
UNAVAILABLE – 15 MINUTES	M	L	1	1
DISCLOSURE OF DATA TO OUTSIDERS	M	H	2	3
SMALL SCALE MODIFICATION	VH	M	1	2
NON-DELIVERY	M	L	1	1
<b>Threat: Staff Shortage</b>				
UNAVAILABLE – 15 MINUTES	L	L	1	1
UNAVAILABLE – 1 HOUR	L	L	1	1
UNAVAILABLE – 3 HOURS	L	L	1	1
UNAVAILABLE – 12 HOURS	L	L	1	1
UNAVAILABLE – 1 DAY	L	L	2	1
UNAVAILABLE – 2 DAYS	L	L	2	1

<b>Asset: Exchange and Outlook</b>	<b>Threat</b>	<b>Vulnerability</b>	<b>Impact</b>	<b>MOR</b>
<b>Threat: Masquerading of Identity by Contractors</b>				
UNAVAILABLE – 15 MINUTES	VL	H	1	1
UNAVAILABLE – 1 HOUR	VL	H	1	1
UNAVAILABLE – 3 HOURS	VL	H	2	2
UNAVAILABLE – 12 HOURS	VL	H	2	2
UNAVAILABLE – 1 DAY	VL	H	2	2
UNAVAILABLE – 2 DAYS	VL	H	3	2
DATA MODIFICATION – DELETION	VL	H	1	1
<b>Threat: Masquerading of Identity by Outsiders</b>				
UNAVAILABLE – 15 MINUTES	H	M	1	2
UNAVAILABLE – 1 HOUR	H	M	1	2

UNAVAILABLE – 3 HOURS	H	M	2	3
UNAVAILABLE – 12 HOURS	H	M	2	3
UNAVAILABLE – 1 DAY	H	M	2	3
UNAVAILABLE – 2 DAYS	H	M	3	3
DATA MODIFICATION – DELETION	VH	M	1	2
<b>Threat: Misuse of System Resources</b>				
UNAVAILABLE – 15 MINUTES	L	M	1	1
UNAVAILABLE – 1 HOUR	L	M	1	1
<b>Threat: Communications Infiltration</b>				
UNAVAILABLE – 15 MINUTES	VL	M	1	1
UNAVAILABLE – 1 HOUR	VL	M	1	1
UNAVAILALBE – 3 HOURS	VL	M	2	1
UNAVAILABLE – 12 HOURS	VL	M	2	1
UNAVAILABLE – 1 DAY	VL	M	2	1
UNAVAILABLE – 2 DAYS	VL	M	3	2
DATA MODIFICATION – DELETION	VL	M	1	1
<b>Threat: Communications Manipulation</b>				
WIDE-SPREAD MODIFICATION	VL	H	1	1
DATA MODIFICATION – DELETION	VL	H	1	1

<b>Asset: Financial Accounting</b>	<b>Threat</b>	<b>Vulnerability</b>	<b>Impact</b>	<b>MOR</b>
<b>Threat: Masquerading of Identity by Insiders</b>				
UNAVAILABLE – 15 MINUTES	H	H	1	2
UNAVAILABLE – 1 HOUR	H	H	1	2
UNAVAILABLE – 3 HOURS	H	H	2	3
UNAVAILABLE – 12 HOURS	H	H	2	3
UNAVAILABLE – 1 DAY	H	H	2	3
UNAVAILABLE – 2 DAYS	H	H	3	4
PARTIAL DESTRUCTION OF DATA	H	H	6	5
DATA MODIFICATION – DELETION	VH	H	4	5
<b>Threat: Unauthorised Use of an Application</b>				
UNAVAILABLE – 15 MINUTES	M	M	1	1
UNAVAILABLE – 1 HOUR	M	M	1	1
UNAVAILABLE – 3 HOURS	M	M	2	2
UNAVAILABLE – 12 HOURS	M	M	2	2
UNAVAILABLE – 1 DAY	M	M	2	2
UNAVAILABLE – 2 DAYS	M	M	3	3
PARTIAL DESTRUCTION OF DATA	M	L	6	4
DISCLOSURE OF DATA TO OUTSIDERS	M	L	3	2
DATA MODIFICATION – DELETION	M	L	4	3
<b>Threat: Technical Failure of Host</b>				
UNAVAILABLE – 15 MINUTES	L	L	1	1
UNAVAILABLE – 1 HOUR	L	L	1	1
UNAVAILABLE – 3 HOURS	L	L	2	1
UNAVAILABLE – 12 HOURS	L	L	2	1
UNAVAILABLE – 1 DAY	L	L	2	1
UNAVAILABLE – 2 DAYS	L	L	3	2
PARTIAL DESTRUCTION OF DATA	L	L	6	3
<b>Threat: Power Failure</b>				

UNAVAILABLE – 15 MINUTES	L	L	1	1
UNAVAILABLE – 1 HOUR	L	L	1	1
UNAVAILABLE – 3 HOURS	L	L	2	1
<b>Threat: Application Software Failure</b>				
UNAVAILABLE – 15 MINUTES	VH	H	1	3
UNAVAILABLE – 1 HOUR	M	M	1	1
UNAVAILABLE – 3 HOURS	M	M	2	2
UNAVAILABLE – 12 HOURS	L	M	2	2
PARTIAL DESTRUCTION OF DATA	VL	L	6	3
DISCLOSURE OF DATA TO OUTSIDERS	VL	L	3	1
WIDE-SPREAD MODIFICATION	VL	L	1	1
<b>Threat: User Error</b>				
UNAVAILABLE – 15 MINUTES	VH	H	1	3
PARTIAL DESTRUCTION OF DATA	M	L	6	4
DISCLOSURE OF DATA TO OUTSIDERS	H	M	3	3

<b>Asset: Housing Benefits</b>	<b>Threat</b>	<b>Vulnerability</b>	<b>Impact</b>	<b>MOR</b>
<b>Threat: Masquerading of Identity by Outsiders</b>				
UNAVAILABLE – 15 MINUTES	H	M	1	2
UNAVAILABLE – 1 HOUR	H	M	1	2
UNAVAILABLE – 3 HOURS	H	M	2	3
UNAVAILABLE – 12 HOURS	H	M	2	3
UNAVAILABLE – 1 DAY	H	M	2	3
UNAVAILABLE – 2 DAYS	H	M	3	3
DISCLOSURE OF DATA TO OUTSIDERS	H	M	2	3
DATA MODIFICATION – DELETION	VH	M	1	2
<b>Threat: Unauthorised Use of an Application</b>				
UNAVAILABLE – 15 MINUTES	M	H	1	2
UNAVAILABLE – 1 HOUR	M	H	1	2
UNAVAILABLE – 3 HOURS	M	H	2	3
UNAVAILABLE – 12 HOURS	M	H	2	3
UNAVAILABLE – 1 DAY	M	H	2	3
UNAVAILABLE – 2 DAYS	M	H	3	3
DISCLOSURE OF DATA TO OUTSIDERS	M	L	2	2
DATA MODIFICATION – DELETION	M	L	1	1
<b>Threat: Technical Failure of Storage Facility</b>				
UNAVAILABLE – 15 MINUTES	M	H	1	2
UNAVAILABLE – 1 HOUR	M	M	1	1
UNAVAILABLE – 3 HOURS	M	M	2	2
UNAVAILABLE – 12 HOURS	M	M	2	2
UNAVAILABLE – 1 DAY	M	M	2	2
UNAVAILABLE – 2 DAYS	M	L	3	2
<b>Threat: Technical Failure of Network Service</b>				
UNAVAILABLE – 15 MINUTES	L	H	1	1
UNAVAILABLE – 1 HOUR	L	H	1	1
UNAVAILABLE – 3 HOURS	L	H	2	2
UNAVAILABLE – 12 HOURS	L	H	2	2
NON-DELIVERY	L	H	1	1
<b>Threat: System and Network Software Failure</b>				

UNAVAILABLE – 15 MINUTES	M	H	1	2
UNAVAILABLE – 1 HOUR	M	L	1	1
UNAVAILABLE – 3 HOURS	VL	L	2	1
UNAVAILABLE – 12 HOURS	VL	L	2	1
DISCLOSURE OF DATA TO OUTSIDERS	VL	M	2	1
SMALL SCALE MODIFICATION	VL	L	1	1
WIDE-SPREAD MODIFICATION	VL	L	4	2
NON-DELIVERY	VL	L	1	1
<b>Threat: Application Software Failure</b>				
UNAVAILABLEABLE – 15 MINUTES	M	H	1	2
UNAVAILABLEABLE – 1 HOUR	H	L	1	1
UNAVAILABLEABLE – 3 HOUR	VH	L	2	3
UNAVAILABLEABLE – 12 HOUR	M	L	2	2
DISCLOSURE OF DATA TO OUTSIDERS	M	L	2	2
SMALL SCALE MODIFICATION	M	L	1	1
WIDE – SPREAD MODIFICATION	M	L	4	3
NON – DELIVERY	M	L	1	1
<b>Threat: Operations Error</b>				
UNAVAILABLEABLE – 15 MINUTES	VH	M	1	2
UNAVAILABLEABLE – 1 HOUR	VH	M	1	2
UNAVAILABLEABLE – 3 HOURS	VH	L	2	3
UNAVAILABLEABLE – 12 HOURS	VH	L	2	3
FULL DESTRUCTION OF DATA	M	L	4	3
DISCLOSURE OF DATA TO OUTSIDERS	M	L	2	2
SMALL SCALE MODIFICATION	M	H	1	2
WIDE – SPREAD MODIFICATION	M	H	4	4
<b>Threat: Hardware Maintenance Error</b>				
UNAVAILABLEABLE – 15 MINUTES	VH	H	1	3
UNAVAILABLEABLE – 1 HOUR	VH	H	1	3
UNAVAILABLEABLE – 3 HOURS	VH	H	2	4
UNAVAILABLEABLE – 12 HOURS	VH	L	2	3
UNAVAILABLEABLE – 1 DAY	M	L	2	2
DISCLOSURE OF DATA TO OUTSIDERS	M	L	2	2
NON – DELIVERY	M	L	1	1
<b>Threat: Natural Disaster</b>				
PHYSICAL DESTRUCTION	VL	H	5	3
UNAVAILABLEABLE – 15 MINUTES	VL	H	1	1
UNAVAILABLEABLE – 1 HOUR	VL	H	1	1
UNAVAILABLEABLE – 3 HOURS	VL	H	2	2
UNAVAILABLEABLE – 12 HOURS	VL	H	2	2
UNAVAILABLE – 1 DAY	VL	H	2	2
UNAVAILABLE – 2 DAYS	VL	H	3	2
UNAVAILABLE – 1 WEEK	VL	H	4	3
UNAVAILABLE – 2 WEEKS	VL	H	4	3
UNAVAILABLE – 1 MONTH	VL	H	4	3
UNAVAILABLE – 2 MONTHS	VL	H	4	3

<b>Asset: Housing Rents and Repairs</b>	<b>Threat</b>	<b>Vulnerability</b>	<b>Impact</b>	<b>MOR</b>
<b>Threat: Introduction of Damaging Software</b>				

UNAVAILABLE – 15 MINUTES	L	M	1	1
UNAVAILABLE – 1 HOUR	L	M	1	1
UNAVAILABLE – 3 HOURS	L	M	2	2
UNAVAILABLE – 12 HOURS	L	M	2	2
UNAVAILABLE – 1 DAY	L	M	2	2
UNAVAILABLE – 2 DAYS	L	M	3	2
FULL DESTRUCTION OF DATA	L	H	4	3
WIDE-SPREAD MODIFICATION OF DATA	L	M	3	2
MODIFICATION OF DATA – DELETION	L	H	1	1
<b>Threat: Misuse of System Resources</b>				
UNAVAILABLE – 15 MINUTES	M	M	1	1
UNAVAILABLE – 1 HOUR	M	M	1	1
<b>Threat: Communications Failure</b>				
UNAVAILABLE – 15 MINUTES	H	H	1	2
UNAVAILABLE – 1 HOUR	H	H	1	2
UNAVAILABLE – 3 HOURS	H	H	2	3
UNAVAILABLE – 12 HOURS	H	H	2	3
UNAVAILABLE – 1 DAY	H	H	2	3
UNAVAILABLE – 2 DAYS	H	H	3	4
<b>Threat: Technical Failure of Host</b>				
UNAVAILABLE – 15 MINUTES	M	H	1	2
UNAVAILABLE – 1 HOUR	M	M	1	1
UNAVAILABLE – 3 HOURS	M	M	2	2
UNAVAILABLE – 12 HOURS	M	M	2	2
UNAVAILABLE – 1 DAY	M	M	2	2
UNAVAILABLE – 2 DAYS	M	M	3	3
<b>Threat: Technical Failure of Network Service</b>				
UNAVAILABLE – 15 MINUTES	H	M	1	2
UNAVAILABLE – 1 HOUR	H	M	1	2
UNAVAILABLE – 3 HOURS	H	M	2	3
UNAVAILABLE – 12 HOURS	H	M	2	3
<b>Threat: Power Failure</b>				
UNAVAILABLE – 15 MINUTES	H	M	1	2
UNAVAILABLE – 1 HOUR	M	L	1	1
UNAVAILABLE – 3 HOURS	L	L	2	1
<b>Threat: System and Network Software Failure</b>				
UNAVAILABLE – 15 MINUTES	VH	H	1	3
UNAVAILABLE – 1 HOUR	VH	H	1	3
UNAVAILABLE – 3 HOURS	VH	L	2	3
UNAVAILABLE – 12 HOURS	M	L	2	2
WIDE-SPREAD MODIFICATION OF DATA	L	L	3	2
<b>Threat: Application Software Failure</b>				
UNAVAILABLE – 15 MINUTES	VH	H	1	3
UNAVAILABLE – 1 HOUR	H	H	1	2
UNAVAILABLE – 3 HOURS	H	H	2	3
UNAVAILABLE – 12 HOURS	H	L	2	2
WIDE-SPREAD MODIFICATION OF DATA	L	L	3	2



<b>Asset: PS Enterprise</b>	<b>Threat</b>	<b>Vulnerability</b>	<b>Impact</b>	<b>MOR</b>
<b>Threat: Technical Failure of Host</b>				
UNAVAILABLE – 1 HOUR	M	H	1	2
UNAVAILABLE – 3 HOURS	M	H	1	2
UNAVAILABLE – 12 HOURS	M	M	1	1
UNAVAILABLE – 1 DAY	M	M	2	2
UNAVAILABLE – 2 DAYS	M	M	2	2
PARTIAL DESTRUCTION OF DATA	M	M	5	4
<b>Threat: Application Software Failure</b>				
UNAVAILABLE – 1 HOUR	H	H	1	2
UNAVAILABLE – 3 HOURS	L	H	1	1
UNAVAILABLE – 12 HOURS	VL	H	1	1
PARTIAL DESTRUCTION OF DATA	VL	L	5	2
DISCLOSURE OF DATA TO OUTSIDERS	VL	L	4	2
SMALL SCALE MODIFICATION OF DATA	VL	L	2	1
WIDE-SPREAD MODIFICATION OF DATA	VL	L	5	2
<b>Threat: Software Maintenance Error</b>				
UNAVAILABLE – 1 HOUR	VL	M	1	1
UNAVAILABLE – 3 HOURS	M	L	1	1
UNAVAILABLE – 12 HOURS	M	L	1	1
PARTIAL DESTRUCTION OF DATA	VL	L	5	2
SMALL SCALE MODIFICATION OF DATA	M	L	2	2
WIDE-SPREAD MODIFICATION OF DATA	M	L	5	3
<b>Threat: User Error</b>				
PARTIAL DESTRUCTION OF DATA	M	L	5	3
DISCLOSURE OF DATA TO OUTSIDERS	M	L	4	3
SMALL SCALE MODIFICATION OF DATA	VH	H	2	4
<b>Threat: Staff Shortage</b>				
UNAVAILABLE – 1 HOUR	VL	H	1	1
UNAVAILABLE – 3 HOURS	VL	H	1	1
UNAVAILABLE – 12 HOURS	VL	H	1	1
UNAVAILABLE – 1 DAY	VL	H	2	2
UNAVAILABLE – 2 DAYS	VL	H	2	2

<b>Asset: SOSICIS</b>	<b>Threat</b>	<b>Vulnerability</b>	<b>Impact</b>	<b>MOR</b>
<b>Threat: Technical Failure of Storage Facility</b>				
UNAVAILABLE – 15 MINUTES	M	H	1	2
UNAVAILABLE – 1 HOUR	M	M	1	1
UNAVAILABLE – 3 HOURS	M	M	1	1
UNAVAILABLE – 12 HOURS	M	M	1	1
UNAVAILABLE – 1 DAY	M	M	2	2
UNAVAILABLE – 2 DAYS	M	L	2	2
<b>Threat: System and Network Software Failure</b>				
UNAVAILABLE – 15 MINUTES	M	H	1	2
UNAVAILABLE – 1 HOUR	M	L	1	1
UNAVAILABLE – 3 HOURS	M	L	1	1
UNAVAILABLE – 12 HOURS	VL	L	1	1
DISCLOSURE OF DATA TO OUTSIDERS	VL	M	2	1
SMALL SCALE MODIFICATION OF DATA	VL	L	1	1

WIDE-SPREAD MODIFICATION OF DATA	VL	L	4	2
NON – DELIVERY	VL	L	1	1
<b>Threat: Application Software Failure</b>				
UNAVAILABLE – 15 MINUTES	L	H	1	1
UNAVAILABLE – 1 HOUR	VL	H	1	1
UNAVAILABLE – 3 HOURS	VL	H	1	1
UNAVAILABLE – 12 HOURS	VL	L	1	1
DISCLOSURE OF DATA TO OUTSIDERS	VL	L	2	1
SMALL SCALE MODIFICATION OF DATA	L	L	1	1
WIDE-SPREAD MODIFICATION OF DATA	VL	L	4	2
NON – DELIVERY	VL	L	1	1
<b>Threat: Fire</b>				
PHYSICAL – DEST	M	H	5	4
UNAVAILABLE – 15 MINUTES	M	H	1	2
UNAVAILABLE – 1 HOUR	M	H	1	2
UNAVAILABLE – 3 HOURS	M	H	1	2
UNAVAILABLE – 12 HOURS	M	H	1	2
UNAVAILABLE – 1 DAY	M	H	2	3
UNAVAILABLE – 2 DAYS	M	H	2	3
UNAVAILABLE – 1 WEEK	M	H	4	4
UNAVAILABLE – 2 WEEKS	M	H	4	4
UNAVAILABLE – 1 MONTH	M	H	4	4
UNAVAILABLE – 2 MONTHS	M	H	4	4
<b>Threat: Terrorism</b>				
PHYSICAL DESTRUCTION	VL	H	5	3
UNAVAILABLE – 15 MINUTES	VL	H	1	1
UNAVAILABLE – 1 HOUR	VL	H	1	1
UNAVAILABLE – 3 HOURS	VL	H	1	1
UNAVAILABLE – 12 HOURS	VL	H	1	1
UNAVAILABLE – 1 DAY	VL	H	2	2
UNAVAILABLE – 2 DAYS	VL	H	2	2
UNAVAILABLE – 1 WEEK	VL	H	4	3
UNAVAILABLE – 2 WEEKS	VL	H	4	3
UNAVAILABLE – 1 MONTH	VL	H	4	3
UNAVAILABLE – 2 MONTHS	VL	H	4	3

## Appendix M: Controls Suggested by CRAMM

ID	Controls	Implemented	Recommended
1	User Ids should ensure that activities can be traced to individuals	<b>x</b>	
2	Passwords should be sufficiently long so that they are difficult to guess or determine from the encrypted form.		<b>x</b>
3	Passwords should be stored in a form that no one, not even the system administrator, may see the password chosen by the user	<b>x</b>	<b>x</b>
4	Passwords should be pronounceable but not valid English words		
5	The system should ensure that users follow good security practice in the selection of passwords		
6	Users should follow good security practice in the selection and use of passwords		
7	Passwords should be changed whenever they have been compromised		<b>x</b>
8	Passwords should be changed regularly	<b>limited</b>	<b>x</b>
9	The confidentiality of passwords should be maintained when the passwords are being distributed		
10	Access to the identification facilities should be controlled	<b>x</b>	
11	All workstations attached to the host should be identified	<b>limited</b>	<b>x</b>
12	The responsibility for decided who may be granted access to a file should rest with the file's owner	<b>x</b>	
13	Unattended workstations should be protected against an unauthorised person taking the opportunity to use the workstation	<b>x</b>	
14	Users should be restricted to using the system at specific times	<b>limited</b>	
15	All major information assets should be accounted for		<b>x</b>
16	Access to a multi-user information system should be subject to a formal user registration and de-registration process	<b>x</b>	
17	The use of privileged functions should be controlled	<b>x</b>	
18	User access rights should be reviewed at regular intervals		<b>x</b>
19	The business requirement for access control should be defined	<b>x</b>	
20	Highly sensitive application systems should be run on a dedicated computer		
21	Access to application system files should be controlled	<b>x</b>	
22	Access to audit trails should be controlled		
23	The amount of data to be recorded should be configurable		

24	The events that need to be accounted for should be configurable		
25	System clocks should be synchronized	<b>x</b>	
26	Accounting should be carried out by trusted facilities		
27	The Accounting Log should be retained to enable investigations to be carried out when necessary	<b>x</b>	
28	Accounting should be operation at all times	<b>x</b>	
29	A range of facilities for analysing accounting logs should be provided		
30	The types of events that need to be inspected should be specified	<b>x</b>	
31	The frequency with which the account log should be reviewed should be specified		
32	All suspected or detected attempts to breach security should be investigated	<b>limited</b>	<b>x</b>
33	Audit requirements and activities should be planned to minimise the risk of disruption to the business	<b>x</b>	
34	Access to system audit tools should be safeguarded to prevent any possible misuse of compromise	<b>x</b>	
35	Acceptance criteria should be specified for security testing	<b>x</b>	
36	Security tests should be conducted against the security requirements, using agreed acceptance criteria		<b>x</b>
37	Breaches of software integrity should be detected and prevented		
38	The potential for the introduction of malicious software into the IT system should be minimised	<b>x</b>	<b>consider</b>
39	The system should be monitored for potential malicious software activity	<b>x</b>	
40	Any malicious software should be identified, isolated, and removed	<b>x</b>	
41	Teleworking should only be authorised if the appropriate security arrangements are in place		<b>x</b>
42	Regardless of ownership, any equipment used for information processing should be authorised by management		<b>x</b>
43	All changes to software should be authorised before the change is implemented	<b>x</b>	
44	A record should be maintained of all changes made to the software		
45	Changes to software which have to be made before the authorisation can be granted should be controlled		
46	All incoming software should be checked to ensure that no unauthorised amendments have been made in transit		
47	Software that is being exported should be sent in a manner that ensures that no unauthorised amendments are made in transit		
48	All input/output devices should be uniquely identified	<b>x</b>	

49	Users should be informed that e-mail facilities should not be misused	<b>x</b>	
50	The application should be identified to the system	<b>x</b>	
51	Unauthorised access to remote access ports should be prevented	<b>x</b>	
52	Users should be informed of actions to take if they are subject of unwanted or Spam e-mail		
53	Operator procedures should be produced covering all operator actions	<b>x</b>	
54	Faults should be reported and corrective action taken	<b>x</b>	
55	Operational activity should be monitored		
56	The risks in using an external contractor to manage information processing facilities should be identified and managed		
57	Changes to IT facilities should be controlled		
58	Changes to the Operating System should be authorised	<b>x</b>	
59	The security impact of a change to Operation System should be reviewed		
60	Access to the System Administration accounts should be strictly controlled	<b>limited</b>	<b>x</b>
61	Changes to packaged software should be carried out in such a manner that the change will not introduce further problems	<b>x</b>	
62	Control should be provided for the implementation of software on operational systems	<b>x</b>	
63	Test data should be protected and controlled	<b>x</b>	
64	Only authorised software maintenance personnel should carry out maintenance tasks	<b>x</b>	
65	The quality of all software maintenance work should be checked		
66	All key equipment should be supported by a maintenance contract	<b>x</b>	
67	There should be measures to safeguard against user error		
68	The application should check the overall consistency of the information once it has been entered	<b>x</b>	
69	Data output from an application should be validated to ensure that processing of stored information is correct	<b>x</b>	
70	Hardcopy Outputs should show the classification of the information being printed		
71	It should be possible to check that print-outs are complete		
72	A stand-by Host should be available to take over processing in the event of a disaster or other incident		<b>x</b>
73	Where appropriate it should be possible to revert to a manual process	<b>x</b>	

74	Emergency spares should be available		
75	Business Continuity Plans should be produced		
76	The business continuity strategy should be based on a risk assessment		
77	The business continuity plans should enable the restoration of business operations within the required timescales following an interruption to a business process		
78	Business Continuity Plans should be subject to regular tests		
79	The Business Continuity Plans should be maintained	<b>x</b>	
80	Back-ups should be taken of all essential business data	<b>x</b>	<b>consider</b>
81	Back-ups should be taken of all software applications	<b>limited</b>	<b>x</b>
82	All data should be backed-up using suitable technology	<b>x</b>	
83	It should be possible to re-create data lost since last back-up		<b>x</b>
84	The system should be resilient to the failure of individual storage disks		
85	The manufacturer's specifications should be observed for operational areas	<b>x</b>	
86	Maintenance support should be provided	<b>x</b>	
87	In the even of equipment failure, disruption should be minimised	<b>x</b>	
88	A Data Controller should be formally identified and named		
89	A Data Protection Officer should be appointed		
90	Data Processors to be identified and named		
91	The Data Protection Officer should ensure that the Data Protection Commissioner is informed of required details about the processing of personal data by means of the Notification Process		
92	The Data Protection Officer should ensure that all further amendments to the processing of personal information are notified to the Data Protection Commissioner		
93	Information systems handling personal data should comply with the principles of the data protection legislation		<b>x</b>
94	The Data Subjects' rights should be enforced		<b>x</b>
95	Data Subjects to be able to control what happens to their personal information		
96	Regular data protection awareness training to be undertaken within the organisation		
97	Regular reviews of the register entry should be undertaken		

## Appendix N: Meetings and Interviews Report

Date of Occurrence	Title of Meeting	Start Time	End Time
14-Mar-02	WPI Scope and Progress Meeting 1	14:00	15:00
Meeting Head	Meeting Recorder	Primary Attendee	
John Duell	Casey Whicher	Steve Weininger	
All Other Attendees			
Aziza Dar, Laura Menides, Jeff Kimball, Josh Coakley			
Description			
To evaluate the scope of the E-Government Information Security project in terms of the sponsor's expected results and WPI expected results. We also talked about the format of the end report.			

Date of Occurrence	Title of Meeting	Start Time	End Time
14-Mar-02	PRINCE Overview and System Asset Briefing	12:00	13:30
Meeting Head	Meeting Recorder	Primary Attendee	
Steve Lawrenson	All	Steve Lawrenson	
All Other Attendees			
Josh Coakley, Jeff Kimball, John Duell, Casey Whicher, Aziza Dar			
Description			
To familiarize Information Security project team with PRINCE methodology, and to gather a list of key system / software resources to focus the risk analysis on. We received a thorough briefing from Steve concerning PRINCE, and then compiled a list of around seven key systems spanning a variety of operating systems used within IT.			

Date of Occurrence	Title of Meeting	Start Time	End Time
19-Mar-02	Server Asset Information Gathering	10:30	11:30
Meeting Head	Meeting Recorder	Primary Attendee	
Jeff Kimball	Casey Whicher	Paul Biggs	
Description			
To discuss physical asset information in regards to servers for four specific systems: Council Tax, Housing Benefits, Housing Rents and Repairs and Financial Accounting.			

Date of Occurrence	Title of Meeting	Start Time	End Time
20-Mar-02	Interview with Rob Heap	14:30	15:00
Meeting Head	Meeting Recorder	Primary Attendee	
John Duell	Josh Coakley	Robert Heap	
All Other Attendees			
Casey Whicher			
Description			
Interview concerning Financial Accounting System			

Date of Occurrence	Title of Meeting	Start Time	End Time
21-Mar-02	WPI Scope and Progress Meeting 2	15:00	16:00
Meeting Head	Meeting Recorder	Primary Attendee	
Josh Coakley	Jeff Kimball	Professor Weininger	
All Other Attendees			
Casey Whicher, John Duell, Aziza Dar, Professor Menides			
Description			
Progress meeting to go over where we are in our research with our advisors and liaison. It seems that we have made good progress and should keep up the good work.			

Date of Occurrence	Title of Meeting	Start Time	End Time
21-Mar-02	Interview with Peter Brown	10:00	10:30
Meeting Head	Meeting Recorder	Primary Attendee	
Josh Coakley	Jeff Kimball	Peter Brown	
Description			
Interview concerning Council Tax System			

Date of Occurrence	Title of Meeting	Start Time	End Time
21-Mar-02	Interview with Richard Warren & Mark Kitson	11:00	11:30
Meeting Head	Meeting Recorder	Primary Attendee	
Casey Whicher / Jeff Kimball	John Duell	Richard Warren	
All Other Attendees			
Josh Coakley, Mark Kitson			
Description			
Interview concerning the Outlook/Exchange email system			

Date of Occurrence	Title of Meeting	Start Time	End Time
22-Mar-02	Housing Rents / Repairs System Interview	10:00	10:20
Meeting Head	Meeting Recorder	Primary Attendee	
Josh Coakley	Casey Whicher	John Sykes	
Description			
Interview to gather information concerning the Housing Rents and Repairs system, and potential threats.			

Date of Occurrence	Title of Meeting	Start Time	End Time
22-Mar-02	Payroll System Interview	10:00	10:25
Meeting Head	Meeting Recorder	Primary Attendee	
Jeff Kimball	John Duell	Steve Key	
Description			
Interview to discuss Payroll System (PS Enterprise), and to talk about potential threats.			



Date of Occurrence	Title of Meeting	Start Time	End Time
25-Mar-02	Council Tax Senior User Interview	14:30	15:00
Meeting Head	Meeting Recorder	Primary Attendee	
Jeff Kimball	Casey Whicher	Colin Lloyd	
Description			
Interview of Colin Lloyd who is a senior user of the Council Tax system to gain a better understanding of the data that is stored and other assets.			

Date of Occurrence	Title of Meeting	Start Time	End Time
25-Mar-02	Review of scope meeting with Aziza	15:00	16:00
Meeting Head	Meeting Recorder	Primary Attendee	
John Duell	Jeff Kimball	Aziza Dar	
All Other Attendees			
Casey Whicher, Josh Coakley			
Description			
Project is on schedule and the scope is fine at the moment. We think that we will be able to complete all tasks necessary for project completion			

Date of Occurrence	Title of Meeting	Start Time	End Time
27-Mar-02	Interview with Colin Mason	14:30	15:00
Meeting Head	Meeting Recorder	Primary Attendee	
Jeff Kimball	John Duell	Colin Mason	
Description			
Interview concerning Housing Rents and Repairs System			

Date of Occurrence	Title of Meeting	Start Time	End Time
28-Mar-02	Cashiers Office System Interview	10:30	11:00
Meeting Head	Meeting Recorder	Primary Attendee	
Josh Coakley	Casey Whicher	Ray McInnis	
Description			
Interview used to gather asset and threat information concerning the Cashier's Office System.			

Date of Occurrence	Title of Meeting	Start Time	End Time
28-Mar-02	Housing Benefits System Interview	11:30	12:00
Meeting Head	Meeting Recorder	Primary Attendee	
Casey Whicher	Josh Coakley	Tracey Hawkins	
Description			
Interview used to gather Senior User side data concerning potential threats, and asset information on the Housing Benefits system.			

Date of Occurrence	Title of Meeting	Start Time	End Time
28-Mar-02	WPI Scope and Progress Meeting 3	2:30	3:15
<b>Meeting Head</b>	<b>Meeting Recorder</b>	<b>Primary Attendee</b>	
Casey Whicher	Josh Coakley	Steve Weininger	
<b>All Other Attendees</b>			
Aziza Dar, Laura Menides			
<b>Description</b>			
To review project status, potential risks, and next steps			

Date of Occurrence	Title of Meeting	Start Time	End Time
03-Apr-02	Interview concerning Housing benefits system	14:00	14:30
<b>Meeting Head</b>	<b>Meeting Recorder</b>	<b>Primary Attendee</b>	
Jeff Kimball	John Duell	Krystyna Kiuber	
<b>Description</b>			
Interview used to learn about the housing benefits system based upon the IT aspects			

Date of Occurrence	Title of Meeting	Start Time	End Time
03-Apr-02	Progress meeting	15:45	16:15
<b>Meeting Head</b>	<b>Meeting Recorder</b>	<b>Primary Attendee</b>	
John Duell	All	Aziza Dar	
<b>All Other Attendees</b>			
Casey Whicher, Josh Coakley, Jeff Kimball			
<b>Description</b>			
Discussed the project, some of our findings as of yet and some preliminary reports from the CRAMM software.			

Date of Occurrence	Title of Meeting	Start Time	End Time
04-Apr-02	WPI Scope and Progress meeting 4	14:30	15:30
<b>Meeting Head</b>	<b>Meeting Recorder</b>	<b>Primary Attendee</b>	
Jeff Kimball	John Duell	Steve Weininger	
<b>All Other Attendees</b>			
Laura Menides, Aziza Dar, Casey Whicher, Josh Coakley			
<b>Description</b>			
Review of progress and scope of the project with the advisors and liaison. Not much to report on since there has only been two days of work since last meeting.			

Date of Occurrence	Title of Meeting	Start Time	End Time
08-Apr-02	SOSCIS Interview	14:00	14:45
<b>Meeting Head</b>	<b>Meeting Recorder</b>	<b>Primary Attendee</b>	
John Duell	Casey Whicher	Felix Stride - Darnley	
<b>All Other Attendees</b>			
Geoff Davey			
<b>Description</b>			
Learned about the SOSCIS system and Social Services, what they are responsible for and what type of a system it is.			

Date of Occurrence	Title of Meeting	Start Time	End Time
09-Apr-02	Group Interview with Systems & Projects	14:30	15:30
<b>Meeting Head</b>	<b>Meeting Recorder</b>	<b>Primary Attendee</b>	
John Duell	Casey Whicher	Steve Lawrenson	
<b>All Other Attendees</b>			
Josh Coakley, Jeff Kimball, Chris Nice, Graeme Webster			
<b>Description</b>			
Group interview to discuss network logon issues, password use and control, external logon, and use of personal workstations			

Date of Occurrence	Title of Meeting	Start Time	End Time
09-Apr-02	Group interview with DSG	15:30	16:30
<b>Meeting Head</b>	<b>Meeting Recorder</b>	<b>Primary Attendee</b>	
John Duell	Jeff Kimball		
<b>All Other Attendees</b>			
Josh Coakley, Casey Whicher, Paul Damaa, Dave Lovatt			
<b>Description</b>			
Group interview to discuss network logon issues, password use and control, external logon, and use of personal workstations			

Date of Occurrence	Title of Meeting	Start Time	End Time
11-Apr-02	WPI Scope and Progress Meeting #5	14:30	15:30
<b>Meeting Head</b>	<b>Meeting Recorder</b>	<b>Primary Attendee</b>	
Josh Coakley	Jeff Kimball	Steve Weininger	
<b>All Other Attendees</b>			
Laura Menides, Paul Davis, Aziza Dar, Casey Whicher, John Duell			
<b>Description</b>			
Last meeting to review the progress of the project, good progress; have to work harder to reach goals since laptop is back and in working order.			

Date of Occurrence	Title of Meeting	Start Time	End Time
11-Apr-02	Steve Key follow-up Interview	16:00	16:20
<b>Meeting Head</b>	<b>Meeting Recorder</b>	<b>Primary Attendee</b>	
John Duell	Josh Coakley	Steve Key	
<b>Description</b>			
To gather additional information on the Payroll System in regards to asset valuation.			

Date of Occurrence	Title of Meeting	Start Time	End Time
11-Apr-02	Rob Heap follow-up Interview	11:30	11:45
<b>Meeting Head</b>	<b>Meeting Recorder</b>	<b>Primary Attendee</b>	
John Duell	Josh Coakley	Rob Heap	
<b>Description</b>			
To gather a little more information in regards to the Financial Accounting systems and asset valuation.			

<b>Date of Occurrence</b>	<b>Title of Meeting</b>	<b>Start Time</b>	<b>End Time</b>
12-Apr-02	LEGATO Tape Backup System	10:30	11:15
<b>Meeting Head</b>	<b>Meeting Recorder</b>	<b>Primary Attendee</b>	
Jeff Kimball	John Duell	Paul Damaa	
<b>Description</b>			
To discuss and gather crucial information concerning the Legato tape backup system in regards to the NT systems.			

## Appendix O: Interviews at WPI

**Interviewee:** Josh Brandt

**Job Title:** WPI UNIX Systems Administrator [been employed for 2 yrs]

**Date:** February 5<sup>th</sup>, 2002

**Time:** 2:00PM - 2:45PM

**Interviewer:** Jeff Kimball

**Note Taker:** Casey Whicher

**Note Taker:** Josh Coakley

1. *What (if any) are some relevant standards in the United States that compare with the British Standard 7799 in regards to information security? Specifically how do these apply to WPI?*

The largest and most relevant standard that has a connection to institutes or universities is called FERPA. It is primarily concerned with medical records and other personal information. Particularly FERPA lays out guidelines by which all sensitive information of this type must be protected. State controlled universities and schools have greatly many more regulations and controls placed on them because they are controlled by the government. "I am not sure specifically what these additional regulations are; I just know that they are stricter."

2. *Does WPI have a specific policy written down anywhere on what types of information can be released?*

Human resources will have that kind of information.

3. *Are WPI student medical records held at the CCC?*

Not sure. I don't believe so but you should consult Ben Thompson.

4. *What information is stored on site through the CCC?*

A wide range of school related, and personal information. Everything from your name, contact information, class, home address, advisor, phone number, home phone number, and email address to your grades, which are stored in the Banner system. However, that system is only accessible by certain faculty and administration. "Even I don't have access to Banner."

5. *Does WPI use any security management software?*

At WPI and other schools we are allowed to give out email addresses over the web, but not addresses and phone numbers. Other personal information of that sort also remains confidential. At WPI you might be familiar with the White Pages campus directory. This system dispenses this contact information out over the web. It utilizes what is called an

LDAP (light weight database access protection) system to store and dispense personal information. LDAP allows certain people access to certain information based upon the user's login name and password. The information is layered with different security levels, and based upon the user's level of clearance only information at that specific layer is deployed.

“There is a new LDAP version 2.0 that has been introduced to the system that has more security checks than the new one. LDAP is an open standard, needs someone skilful to set it up, but once it is set up it is easy to maintain.”

Besides the LDAP system the only other major Information System on campus that stores and handles personnel/student data is the Banner system. It runs off from an Oracle database and is updated by five employees whose primary function consists only with keeping the system up, and updated.

*6. Are there any other things that WPI does to prevent the breakdown of information security?*

The CCC discourages the use of Telnet due to its lack of password encryption when it sends and receives requests. The CCC recommends that students and employees utilize a SSH terminal utility. SSH opens up an encrypted channel before transmitting data. SSH uses the new Kerberos MIT Encryption technique to secure the channel with over 4 layers of encryption. This prevents “hackers” utilizing “packet sniffing” techniques from simply acquiring your password. It is important to note that even though most students don't practice this almost the entire faculty does.

Another method that the WPI CCC employs to protect your password information is that it stores the user id and personal information in a separate location from the UNIX password list. The two directories are located in separate places so that if one is taken the other isn't compromised. Also the password list is heavily encrypted.

Two cases have been seen where unauthorised access has been seen. One case is a girl told someone else her password. The other case was a male student that had his UNIX password shared on the network in a plain text file. 9 times out 10 the cases in which a password might be compromised are due to “Social Engineering”, and not outright hacking.

WPI will only release information to government officials and police departments when provided with a subpoena. Family must be mother/father for student information, or closing living relative for alumni. Certificate of death is needed for passed away alumni.

*7. What kinds of protections does WPI have against people stealing identities or faking password resets?*

Need SSN (WPI ID) and PIN to reset your UNIX password.  
Need SSN (WPI ID) and UNIX Password to reset your PIN.

If you lose all of your required ID numbers then you would have to go to the Help Desk and physically show a form of valid ID in order to have your UNIX password rest. Due to the fact that the white pages database has your SSN on it because it is your WPI student id number

security needs to be taken in this area. In order to have your ID pulled up you need to present ID also. If you request it the registrar's office can give you a student id number that is not your SSN. In order to get a UNIX account you need to be in the white pages. White pages are updated by the Banner system daily. This is a recent development, as Banner and white pages use to be totally separate.

8. *Does WPI take any steps with risk management/policies?*

It depends on the situation in specific. There are no formal policies. No specific risk management procedures that they have to follow. "I run the public UNIX systems so there is not that much secure information under my control"

9. *What is Social engineering?*

Social engineering is a slang term for the process of "socially" acquiring someone's password. It isn't an actual form of engineering, but more of a "hacker" slang term for conning someone out of personal information. If only an individual student's ID is compromised than this has very little impact on the WPI system as a whole. Faculty accounts are obviously more sensitive, and if an administrator's password was taken then the system would be in Jeopardy.

10. *Is there anything else we may have missed?*

- Talk to Sean O'Connor for legal information
- Ben Thompson for Admin systems
- John Bartelsem for Admin systems
- Definitely look into FERPA.
- Do a web search for MIT security camp.
- UMASS contacts: IT Department  
Christopher Misra  
Network Analyst  
V: 413.545.9721  
F: 413.545.3203  
Email: [cmisra@oit.umass.edu](mailto:cmisra@oit.umass.edu)

**Interviewee:** David B. Everitt

**Job Title:** Associate Director of Human Resources WPI – Benefits Administration

**Date:** February 6<sup>th</sup>, 2002

**Time:** 2:00PM - 2:45PM

**Interviewer:** Jeff Kimball

**Note Taker:** John Duell

**Note Taker:** Casey Whicher

1. *Does WPI use a formal Information Security Policy?*

a. *If so, can we receive a copy of the document, or could you tell us more about it?*

No, although there are some federal government regulations that we follow concerning retention records. Nothing can be released without authorised signature from the employee. Situations where this arise include when a bank is looking for salary info – we need signed authorisation from employee. It also occurs for a reference call – we can only give hire date, termination date – not salary, reason for termination, unemployment information  
Two exceptions include attorney privileges and deceased employees

2. *Do you know of any steps WPI takes in the direction of Risk Management in terms of managing its information? (i.e. How it is collected, entered, processed, viewed, and or who has access to it)*

The Resume goes to the hiring supervisor, which is outside the department. That person can give it to anyone, however. The person is not an employee at this point. As soon as they sign on, then the information is confidential, and everything stored on paper, including resume and application, go into their file. Only HR has access to that file. We try to get resumes back from hiring supervisor and anyone to whom they gave it. Performance evaluations, salary, personal info, progressive discipline memo, promotion info, etc., also goes into file

3. *Are there any other methods that you are aware of that the school uses to protect employee, and student data?*

There are various levels of security in Banner. For example, if someone wants an HR page, they need to get signed up, and there are different levels of security for different people as to what you can see. Employees who have varying levels of access include the alumni office, admissions, and HR. Banner holds student, employee, and alumni information. Banner is post-employment – emergency info, home address, phone number etc., are found here. If someone calls asking for information concerning a person, they would not be able to get things such as someone's phone number, age, birth date, or SSN. Currently the SSN is the identifier of the system, which is a big deal. However, we would not move away from that, because banner dictates it. It can be changed by people using it though.

4. *Could you give us some further information on FERPA?*

Nickie Andrews in registrar – lots of info on FERPA  
[www.Personalinfomediadiary.com/ferpa](http://www.Personalinfomediadiary.com/ferpa)



Other contacts:

Roger Donahue - Banner

Ben Thompson – Banner

Gina Patterson – 5610 vp's secretary

**Interviewee:** Ben Thompson

**Job Title:** Director of Computing Services

**Date:** February 18<sup>th</sup>, 2002

**Time:** 2:00PM - 2:45PM

**Interviewer:** Jeff Kimball

**Note Taker:** John Duell

*1. What functions does Banner perform? What is stored in Banner in terms of Data?*

Banner holds inquiry admissions, accounts receivable, general ledger, payroll, alumni development, ERP...pretty much everything. There are a few things outside of the banner system. One example is the system for summer sports. A couple other things are not in it. But essentially everything is in it for running the campus

It holds approximately 15 gigabytes of information.  
3500-4000 tables of information

*2. Who has access to Banner and what are the varying levels of access people can have?*

Everyone, including students, faculty, staff, and even alumni, have some access to the banner system. There are a few different levels at which you can access the system.

One is the web interface, which gives individual access. Everyone has this (employee, student, faculty.) What is available is dependant on what and who you are – you can only look at data that is somehow attached to you.

Examples:

Student – not much

Advisor – gain access to auditing all your advisees

The next way to access Banner is the client – only employees can have this access. You access through user classes, which define form group (inquiry or update access.) A person can have an unlimited # of user classes, and when you look at the form, you look at it under the best level of access that you have.

Usually it is the staff more than the faculty that have access to this.

Registrars, admissions, advising, campus police – FAT client

Budgeting, accounting, treasury – are all separate entities

The last is the FAT client – log in as user name and password (not id# and pin#) to Oracle – when logged in you have access to user classes you are members of and that decides what forms you can get to, and whether it is update or inquiry. Within each module we use value-based security. Example: A department head can see all of students who major in your dept but not other students. Or you can see information concerning all funds and orgs that you manage but not other ones. Some don't have value based security – for example Financial aid – if you work there you look at all of the students, and if you don't work there you cant get anything

Raw Data Access – access directly to the tables, instead of viewing tables – value based security – this is not given out too much – odbc/sql connection – access oracle giving user name and password.

Rolls are collections of views (or tables) that you have access to  
User could have multiple rolls

what forms and what records you have access to are two different security systems  
ex FOAPL – you have access to certain ones based on your log in –

### *3. What kind of security measures does Banner utilize in an attempt to secure data?*

Web client – packages that pull out data, and these are restricted based on how you log in (id# and pin# currently – eventually network name and password) once you are in, it tracks you, it tracks how long you've been there. Knows what page it last gave you, tracks when you go to the next page, where you are going to – if you attempt to go to a web page where you shouldn't have a link to, it wont let you do it.

Network encryption on both levels sql net – and secure socket on web.

### *4. What does WPI use for an information security policy?*

– acceptable use policy (ASP)  
- Buckley amendment – FERPA  
- extend FERPA regulations to all information, even though FERPA is technically only for students while at school - cant give other employees the info – cant answer questions on phone (where does he live? No what are his grades? No) It is important to note that any information that WPI created (box # etc.) can be given out.

Owners of data – look at request to make sure they are reasonable – if there is a question then it goes back to the owners to double-check it to make sure it is a valid request.

Release statement- we have one, and it has been approved by lawyers, but it is not currently in use. They are in handbooks and you have to sign that you received it, so you sign it, in a sense

### *5. FOLLOW UPS*

*Who runs banner?*

10 people total

Team of people – database admin, project manager, developers and support people

Access is controlled by Ben and DB admin

Applications development, general management, and like CCC helpdesk – all run by Ben Thompson

Can write report and give it to someone and the user, who doesn't have access, can use the report that does have access and you get that limited access.

One objective of the current Banner system – departmental key users – primary contact in the dept to train and develop with more focus – easier because you don't have to train as many people and it gives someone within the dept to go to for help.

# Appendix P: Interviews in Merton

Paul Biggs (Technical Support Manager)

19 Mar 02

## Interview for Server Information

UNIX and VME Mainframe physical asset information:

System 1: Council Tax

1. Name: ICL VME server mainframe
2. Quantity: 1
3. Type – Database / Application / File Server (limited capabilities)
  - IDMS database stored locally on server
  - Two primary database regions
    - Development
    - Production
4. Cost per unit / Replacement costs
  - Hardware, Support, Upgrade, and Software Package
    - 800,000 per/year for VME mainframe
  - Paul will try and get a better breakdown of the costs for us and get back to us later this afternoon.
5. Systems it runs
  - Council Tax
  - Housing Benefits (HBS)
  - Misc. other systems not in scope for this project
6. Hardware integral to server system
  - Central UPS in the machine room
  - Air conditioning
  - Master Console for direct connection to Mainframe during network downtime
  - 2 Xerox Laser Print Room Printers
    - 40,000 Cost
    - Does not include SW and maintenance
  - Print Server – FUNASSETT
    - VME runs batch print jobs
    - Around 5,000 to replace system
  - Form Design Server / General – REDTITAN
    - Takes in batch print jobs
    - Sorts based on form requirement
    - Applies template
    - Sends back to print server
7. Hardware not located on local floor
  - Document imaging system for council tax and housing and benefits.
    - Documents scanned in on second floor
    - Use PC's to view them as a backup of all documents
    - NT server running an Oracle database
    - Stored on two optical disk drives
    - Approximately 16 gigabyte database
    - Three months of information stored on disk
    - Every night copied off onto optical disks

- Cost of about 100,000
9. Is data stored locally on server
    - Local IDMS database on VME mainframe
    - Backups made to tape
    - Batch work done at night with three months worth of data.
  10. Controls currently implemented
    - Integrity check every week on the server, checks all the pointers pointing between points of the data, errors are not a good thing at all. Back up complete system once a week as well on VME, tape sent off site on Legato tape backups, 70 gigabyte per tape

#### System 2: Housing Rents and Repairs

1. Name: TreshLive
  - ICLUNS UNIX system
  - Threshold system
  - Currently in the process of switching to UNIX server > Sun Server V880
  - Runs INGRIS database, size is about 8 gigabyte. Currently being changed to a new operating system and new hardware, UNIX server, SUN server, V880
  - Currently holds the operating system and the application software. NT server used to get to the server, different servers, but looking to put them through the same one, nothing major in losing this server, two databases, two versions of INGRIS, development and production. All backups follow the same procedure. DSG has the backup plan for all NT and UNIX systems because Legato tape backup is used.
2. Quantity: 1
3. Type - Database / Application / File server (limited applications)
  - INGRIS 8 Gigabyte database
4. Cost per unit
  - 100,000 for complete package
  - currently replacing system, will become “Academic” instead of “Threshold”
5. Data stored locally on server: yes

#### System 3: Financial Accounting

1. Name: Sequent IBM UNIX server
2. Quantity: 1
3. Type – Database / Application / File Server (limited functionality)
  - There are three regions to the INGRIS database. Those three regions are live, test and development sections. This allows developers to make changes to the system, and then test the system before actually implementing the changes into the live region.
4. Cost per unit / Replacement costs:
  - 100,000 (upgraded six months ago)
5. Other hardware integral to these server systems:
  - Consoles inside, as a direct connection so if network went down there would still be access to the server
7. Any hardware not on this floor: no
8. Multiple applications on same server: no
9. Data stored locally on server:
  - Data is stored on the server but is backed up by Legato system nightly
10. Controls currently implemented:

- Cardkey swipe, only authorised people can go in, this is the case for all of the systems.
- Each system has a boot access list, so nobody can do any damage to the system
- Passwords are changed on a regular basis, about monthly.
- Similar principles on all the systems. Users have to change own password for application access, different systems have different password protections. VME.

11. What exactly is the role that tech support plays in the management and care of those physical assets that our study is focused on?

Look after the operating systems and the application software. Ensure that the software has patch levels, integrity of databases, backed up regularly, sort out hardware failures, configuration of additional things, such as installation, or if a new printer is added, UNIX box must be configured. Help out other departments with what they want, advice, and guidance

12. How does tech support division differ from DSG, and why do they control the NT servers?

The NT servers were looked after by tech support, but there was a restructuring about six months ago because the overlap between what the PC guys were doing and the NT server guys were doing was getting bigger because they needed passwords and such. There was more and more work compressing the differences between the two teams, decision was made to move them back out. Didn't really know what to do when there were problems with the servers. Procedures were put into place because there is such a large quantity of NT servers. They then started doing things such as putting forth standard software, anti-virus, etc. Talk to Richard Warren about that he will help a lot. A lot of software coming in was client based, so that the software was installed on the server as well as the PC client / server based software.

Structure:

Paul has been here seven years, been restructured five times. Always looking to do things differently to change and comply with the technology.

Printing for council tax is all done centrally, separate print server. VME runs batch work, sends to Funasset system, which is the printer server. Council tax comes out as VCL file, this is then transferred to the Red Titan formatting server which takes the ASCII information from the mainframe and inputs it into predefined standardised forms.

- Not expensive to set it up, maybe 20,000 but would be time consuming.
- Xerox printers cost about 40,000 for the pair of them.
- Everything going to the Xerox printers goes through Funasset.
- Printed about 250,000 council tax bills, which were completed well ahead of time.

One other thing we should be aware of on the systems, they are all separate servers, but send files to each other the threshold system sends files to VME either through ftp, or ftf, the VME equivalent. There is no file server; the systems just do it themselves VME can act as a file server because it can transfer files to other places that need it

- Physical information about other systems will come from Richard warren.

Payroll is SQL system, probably cashiers office will be as well, may direct us to someone else who has been here longer.



### Interview for Financial Accounting

#### *1. What responsibilities does the financial accounting system have?*

There is a legal requirement that the authority maintains accounts for inquiry purposes. It keeps track of the fiscal information within the Council, ledgers, accounts receivable, accounts payable. The system holds no individual information.

If a constituent overpays their council tax, the Council make refunds. The system doesn't know the background behind why a refund is needed, they just process it.

#### *2. What types of data, particularly personal data of the constituents of Merton, does financial accounting need?*

The system holds no personal information for employees. For residents, it holds personal information if they are receivers of housing or social benefits. It holds names of addresses of business within and without the borough. For those within, it is because they may have to pay certain taxes. For businesses outside Merton, the system holds information because the council orders supplies through them.

#### *3. Is that data shared with any other systems within or without the IT department?*

There are two outside organisations, one of which is the Central Government. They require information concerning Value Added Tax (VAT.) We sometimes have to send them money for VAT we collected in order to keep balance with Central Government. Also, some Ad Hoc groups require information, and the Internal Revenue (IR) needs some information. We give IR a monthly summary of information concerning the types of expenditures

There are many interfaces within the Council. We share information with:

- Check reconciliation
- Cash office – payments received, bills
- Housing system – invoice details from contractors
- Monthly interface for payroll system
- 2 weekly interfaces – council tax, business rates

#### *4. How many people?*

There are 700 users known to the account system throughout borough. Approximately 100-150 users have it as their primary job function, and use it all day. Most of these are in the Civic Centre, but there are some elsewhere as well. The peak concurrent usage of the system is about 60 people. This is lower than the 100-150 number because people get booted off the system after 20 minutes of inactivity, and no one needs to access the system all the time.

*5. What control mechanisms are in place for various risks to the system*

As mentioned, there is a timeout after 20 minutes. There is also a logon and password. The password is changed every 28 days. We also give each user a security profile, which defines how much each person can see, and which functions they are allowed to do. There are less than ten people who have full control of everything in the entire system.

*6. How would the organisation be impacted if the system was unavailable for 15 min, 1 hr, 3 hrs, 12 hrs, 1 day, 1 week, 1 month, or destroyed?*

If it was down for a short amount of time, it would not have a large impact, but if it was down for more than a day, there would start to be very big problems. More than that and we would not deliver money that we need to by contract and by law. If it was destroyed, that would be a very serious problem. We would have no record of what was paid when and where.

*7. How would the organisation be impacted if data was disclosed to people within the organisation, contracted service providers, or outsiders?*

Since a lot of our data is financial, much of it is disclosed anyway.

**Interview for Council Tax**

*1. What responsibilities does the Council Tax system have?*

Council Tax is the revenue generating system for the council.  
Council Tax / Business Rates / Housing Benefits.  
Business Rate generates high revenue for the size of the system.  
Housing Benefits is negative revenue because it pays out.

We are currently in the main billing cycle until the end of March end of the year. All the bills have gone out. Need to get the bills out in order to start generating revenue in April

*2. What types of data, particularly personal data of the constituents of Merton, does it need? Have?*

The system holds property based accounts, one per household. Personal Information:  
Name, Address, Phone, Properties Address...  
What they owe, what they have paid, how much they have outstanding...

*3. Is that data shared with any other systems within or without the IT department?*

Information is shared with the Housing Benefits system. Twice a week we pass data to make sure data is the same on both database systems  
Document Imaging System- Both Housing Benefits and Council Tax link to this NT system. Directly populated with VME system, used to actually visually see the document on the screen. Actual server is located on the 2<sup>nd</sup> floor. Plans to move it back to the machine room, where it would be more secure and in a cleaner environment.

*4. How many people use the system?*

50 Users on the 2<sup>nd</sup> Floor  
40-50 Housing Benefits  
100 For both.

*5. What control mechanisms are in place for various risks to the system?*

VME is a tight and secure database, very difficult to change data on the database due to its age. From an IT perspective can only access a development region. TP system impacts the actual data, and only authorised users of that system can log in and change data, and only on certain portions of that. Changes made in development, and then moved up to the Live. Users have SysAdmins that control and manage user level access

Limited Life Span- Tentative replacement date of within 2 years, it will be replaced by an NT based system (SQL) Current system is way to expensive. Security is very good on the old mainframe, fast and easy to use for expert users, but cumbersome for management and newer

users. Bigger risks with newer NT systems in terms of security. Even Physical access security. Procedures haven't matured as much for newer systems. Old perspective was IT bought and controlled access to the systems, modern thought is that the User drive the control, use, and support of new systems. Process can be risky as more and more people have higher level access to these newer systems.

Peter has been in Merton IT Services for 5 Years

## Interview for Council Tax

*1. What responsibilities does the Council Tax system have?*

The council tax system handles pretty much everything in terms of assessing liability. For example, the billing process has just finished, now they are tying up the process. Can close one liability and open another liability for another person or property. For each property there is a record, each one is put into a banding, and determine the liability, the system knows the charge based on the banding. An account that is attached to each property and will come up with a charge and certain discounts that are based on the living arrangements and who reside there.

*2. What types of data, particularly personal data of the constituents of Merton, does it need? Have?*

Stores the property and records when someone moves into or out of the property. There are 76,000 council tax properties; each one gets a bill about April 1. Not everyone pays when they should, reminders are sent out, if don't respond, then a summons is sent out and system tells when each should be done. Everything is done using the council tax system or a document imaging system. They have a series of interfaces so it can be transferred back and forth. The document imaging system can store images of what comes in, depending on what action is a result of that, may generate a new document to go back to the person that sent it, another copy of the letter is stored. The third thing it does is that if one of the documents is scanned in, it will know that there are documents outstanding in the council tax system

Does not store a lot of personal data, basically the name, and whatever random information that is in the notebook and financial data that is stored for that person, social security number is not stored.

*3. Is that data shared with any other systems within or without the IT department?*

No

*4. How many people use the system?*

About forty people in the office are the only ones that have the control over the data. There are some people who have access to view but not update the information. About 70-80 with viewing capabilities, IT has nothing to do with it. Within the second floor there are about 35 workstations, standard facilities, nothing special on most.

*5. How would the organisation be impacted if the system was unavailable for 15 min, 1 hr, 3 hrs, 12 hrs, 1 day, 1 week, 1 month, or destroyed?*

If they know it will be down, there is a copied version of the latest dump. You cannot make any changes, but you can look at stuff to answer basic enquiries. If there is a failure or over

run of jobs, find out how long it will be down for and if more than an hour, get them to load the copy of the latest dump, if not then not a big deal. System has an availability of about 98%. When the bills were produced, the system was down for a week. People tend to take leave, so impact is lessened. They know about it so it is not really a problem, it happens every year. Not much can be done, it is dead time. If it was unplanned, it wouldn't be a huge problem but wouldn't be able to change things, so money wouldn't be lost, but there would be a delay of any work that needed to be done. See IT for backup procedures

*6. How would the organisation be impacted if data was disclosed to people within the organisation, contracted service providers, or outsiders?*

Wouldn't be a problem to the actual council, but would be in terms of data protection. If it did become general knowledge, didn't really know the implications, but not extremely dangerous. The data that is stored is not very sensitive, only if your neighbours knew how much you paid, or if someone was receiving a discount and it made people unhappy. Lying could cause a problem if it was reported. The council tax department is required to check once a year that discounts apply but changes may be made and are not always reported. Do not usually impose a penalty, just take away the discount. Bank account details are held for people who pay using direct debit. Probably the most sensitive data, about 40% of people pay that way. Nobody is primarily responsible for data protection within the department.

### Interview for Exchange and Outlook

#### 1. *What responsibilities does the Windows Exchange / Outlook system have?*

It handles email and exchange. Currently, there are still approximately 150 people still using MS Mail, but we are in the process of moving them over. There are between 2000 and 2500 accounts on Outlook right now.

#### 2. *What servers does it use?*

There are 3 exchange servers on the 6<sup>th</sup> floor named exchange 1, exchange 2, and exchange 3. In the future we want to consolidate into two servers, one on site and one elsewhere, for redundancy protection. ETA: 3yrs. Estimated replacement cost is £30,000 per server

The information is not shared with any other systems. It controls MyDiary, to-do list, email system. These are core corporate applications – very important

#### 3. *What sort of protection is there?*

The Exchange server is buffered from internet by a firewall. There is also an SMTP server. Anything going into or out of outlook goes through SMTP, which checks for anything bad (ex. Viruses) The SMTP server is hidden behind the firewall, so its IP address is not what is seen from outside. Every morning and evening we sit down and go through what has been stopped by the SMTP server (ex flags are size, content, key words, viruses.) We can either attempt to clean them and send them through, or refuse them

Also, every exchange account is locked into an NT account. Therefore each person should be logged in as themselves when they are on Outlook, and no one else can have access unless permission is given. An example of the permission is that Maggie has access to Gurmel's mail because he has given her access. Also, you can give access to calendar but not email. All people can view other people's calendars.

There is also Outlook web access. To log on, you need your NT user name and password. It is encrypted but it is not secure encryption

There are approximately 100 Outlook accounts that are not individuals, but rather groups. For example, Housing Benefits has an email address that everyone in the borough emails in order to contact the department, but it is not directly affiliated with a person and NT logon.

#### 4. *What kind of personal information is stored?*

Whatever a person wants as the signature of their email. Ex. Name, job title. This is entirely up to the person.

We store very little personal information ourselves. We only store names and telephone numbers.

*5. Who can we talk to about other NT-based systems?*

You can talk to Steve Key for Payroll Services Enterprises. You can talk to me at a later date about the Legato back-up system.

You can also talk to Mark Thomas about our plans to change exchange servers.



**Interview for Housing Rents and Repairs***1. What responsibilities does the Housing Rents and Repairs system in question have?*

There are two main systems, Academy housing which is the main one which manages rents, repairs, allocations, and voids. Prelude manages lease hold management. Those two systems do all housing needs.

*2. What types of data does the system need?*

On the academy housing, you have all of the property details of every property, as well as all of the people who are tenants, waiting lists, etc. All repairs are logged onto the system. Huge database, 500+ tables probably holding eight million rows of data. Everything you can imagine. The main data for academy is based on the core menu which has all the people who have been on the waiting list or have been tenants. Full list, nothing on the system is ever deleted. On top of that is the property database, includes all property stock. The database contains details of stock that have been transferred to a housing association as long as that property still exists. Within that there are various things such as repairs, down to types of bricks and cements, whether the toilet system is one meter or one and a half meters from the floor. The database is very detailed. Live tenancies and past tenancies are kept track of. In terms of allocations to housing, there is a waiting list where properties are offered. Once tenancy is set up, there is the rent module which manages rent and all adjustments to it. There is the history of the rent account as well. Start of tenancy to present. Payments, housing benefits and all other information are held on it. The rent charges screen keeps information on how the rent is constructed. Repairs is the other major area, all repairs made to the property have been logged and the stage that they are at can be viewed...target dates of completion, when it was completed, breakdown of all components of the job, parts, man hours etc. There is an interface with council's financial system where the actual payment is made. Voids area, for when property is vacant, void period carried out to make the property acceptable for someone else to move into.

*3. What types of software or hardware does the system need?*

Academy is an Ingris 2 database, which has just been renamed advantage, on a UNIX platform. ICL Trimetra is a hardware system that has three different operating systems, NT, UNIX and VMS partitions. All located in central IT where the servers are managed.

*4. Is the data shared with any other systems?*

Interface with housing benefits, no link, simply a transfer of relevant data two ways done by a batch process. One way interface to the financial accounting system.

5. *What control mechanisms are in place for information security?*

Each user has an individual logon and password protected that is changed every 28 days. Within each person's logon are set permissions which each individual maintains. His team has full access to manage the system, IT services has more access to maintain the database, the infrastructure team has more control over the servers, there is a tiered system

6. *Who are the users of the system?*

140 registered users, about 80 concurrent users at one time. Many are infrequent users. Only three people have full access to the system. All others have limited access to their main part of it.

**Interview for Housing Rents and Repairs**

*1. What responsibilities does the Housing Rents and Repairs system have?*

The database within the Housing Rents and Repairs system contains council houses – ones owned by council and let out, also garages, and other properties. It holds basic property data, rents chargeable, rents paid, and repairs to the property. Each property is its own record, there are several hundred tables

*2. What types of software or hardware does the system need?*

Unix – Ingris, Trimetro machine – in the process of moving it to a Sun box (ThreshLive)  
The test one is in already  
The live one coming in next week

Client front end – launcher sits on every PC, and that connects to other software. There are 4 district offices for housing around borough

Having a network connection is crucial – if a line goes down, they get kicked off.

The system stores data for people who reside in properties, as well as people on waiting list – only financial data stored involves rent payments. No income or anything like that is stored by the system.

All the clients are windows-based.

*3. Is the data shared with any other systems?*

Payments of rent are sent to the Financial Accounting system (FMIS.)  
Repair bills go to threshlive to check to see if it should be paid...once cleared it goes to masterpiece (FMIS)

There is a 2 way interface with housing benefits system – send in rent details, and the renter may receive housing benefits  
The amount of rent paid goes to the benefits department and benefits figures out how much \$ they get according to certain criteria.  
Rent gets paid at cashier's office and then the information is sent to the system.

*4. What control mechanisms are in place for information security?*

Security layers at user end, permissions can be granted to any screen, can be either read or updated.  
Above that is the System administrator – housing in 3<sup>rd</sup> floor – they grant permissions to all users.  
Above that is Colin – can destroy system with one command.

Backup?

There is a backup to the system done every night using the legato system – talk to Paul Damaa about legato system.

The Database is check-pointed to disk with journal running on it, so if system crashes during the day, it will automatically go through journal and redo everything from the previous day's backup.

Roll forward – flag with time – do all transactions before that time.

5. *Who are the users of the system, and how many are there?*

The majority of the users are housing officers in district offices – deal with problems tenants may have, deal with repairs, get them to pay rent, threaten them if necessary.

There are a few users in the civic centre.

There are approximately 70 concurrent users of system – 150 to 200 people – housing people are not good at updating us with employee lists

6. *How would business be impacted if the system was down for 15m, 1hr, 1wk, or 1month?*

15 minutes – happens often, no big deal.

1 hr – not a serious impact, would hold work up, annoyance.

1 week – almost a year ago, the system disk went bang, and it took a week, including Easter holiday, and that caused chaos – repairs done manually, and then put in later once system was back up.

-only \$ lost would be due to overtime payments.

Last summer they had to go back and then roll forward, by the time Ingris was up, database was corrupt, and they had to go back to checkpoint.

**Interview for Payroll System**

*1. What are the responsibilities of this system?*

The payroll and HR system has the following modules and responsibilities: recruitment, job applications, training module, employees training needs and history, absence module – only records sickness absence at moment, payroll system for employees and other contracts, pure HR module – peoples personal details, appraisals, disagreements and disciplinaries, health and safety module, allows information to be put on the internet. This is provided by an outside contractor named REBUS HR.

*2. What kind of data is held within the system?*

It holds, among other things, names, addresses, and phone numbers. There are over 450 tables of information in all, so there is a lot of information.

*3. What kind of information is shared?*

General Ledger, FMIS, annual extract goes to pensions. Tax system info from central government.

*4. What kind of hardware/software is used?*

There is an NT server on 6<sup>th</sup> floor called HR\_server. The replacement cost is about 30,000 pounds. It is an application / data server. Network, PC's (client-server)

*5. What kind of control mechanisms are in place?*

Only people within HR have access to the server. There are security profiles for each different user, and access is divided up by module. A person must log into central NT domain to have access.

The following divisions use the PS Enterprise system: human resources, payroll, health and safety, and miscellaneous users. There are currently 70 users – the system is about 9 months old. Once it goes live on intranet, there will be approximately 400 users. We are working on phased implementation. By September or October of this year we will be on intranet. Currently most users are inside civic centre. After the intranet is implemented, up to 15-20% of the users will be outside civic centre.

Prior to PS enterprise, we were using VME mainframe.

REBUS HR is the leading payroll supplier, so there is minimum risk. We pretty much had no choice because we do not have the resources to develop the system on our own. It is newest system of PS Enterprise, so there might be a slight risk – it isn't 'tried and tested.' – not quote from interviewee

We do have a support contract with them.

One possible risk is due to the general movement away from mainframe to unix and NT. PS Enterprise is Merton's 1<sup>st</sup> large NT system, and it is also doing a lot of processing – very complex. There might be a shortage of support personnel because they have mainframe background in IT and maybe not 100% on NT

Supplier info: REBUS HR – over 5 yrs, 400,000 pounds – including support and everything

6. What would happen if the system was down for...

15 minutes? Very little.

1 hour? Depends on the time of day, could be slightly disruptive

1 day? Again, depends on the day, but would be disruptive

1 week? Severe problems

Partial destruction of data? Major problems, such as not paying staff, returns to government agencies would be missed, we would incur penalties and fines.

Full destruction? Everything of partial destruction but much worse

Disclosure? Data Protection Act violations, fraud, destruction of Council's reputation

Modification? Small scale – minor

Widespread – As bad as partial destruction

Deliberate – Fraud, but not very serious

**Interview for Cashier's Office**

1. *What responsibilities does the Cashier's Office system have?*

Cash receipting, give out receipts, report the data and end of day Cash & Cheque Balance.

2. *What types of data, particularly personal data of the constituents of Merton, does it need? Have?*

Codes represent money paid into the Cash Office and what it is for. Whenever there is any money paid in, it has to be paid against a code. References refer to reference or account numbers; each council tax payer has a reference number so it can be referenced. Funds refer to different accounts for the various sections that take payments of cash. Pay types are different ways of paying in money, eg Cash, Credit Card, Debit Card, Cheque and Postal order and debits from the accounts are also recorded.

3. *What types of software or hardware does the system need?*

The application is Microsoft based and called Radius Icon. It is a SQL server.

4. *Is that data shared with any other systems within or without the IT department?*

It is shared with council tax, housing benefits, parking, education, Leisure, Libraries and housing rents and repairs

5. *How many people use the system?*

There are about 12 people that use the system, just people in the cash office that use it. At the moment, all access is through the cash office. Nobody outside of the cash office has access to the system.

6. *What control mechanisms are in place for various risks to the system?*

There are security codes which gives staff different access levels, logins, passwords. There is also a firewall. Certain users have more access than others. The Manager's access is level 15; the supervisor is level 10 and Cashiers are level 5.

7. *How would the organisation be impacted if the system was unavailable for 15 min, 1 hr, 3 hrs, 12 hrs, 1 day, 1 week, 1 month, or destroyed?*

Big effect because it would be difficult to give people information. Every time there is a transaction, a receipt is given, and if the system is down then the receipts have to be given out

manually. A few hours would probably be ok, but any longer than that would most likely be a problem.

If there was a power cut, they have a manual procedure for receipting transactions, but they could not process the payments to the accounts. They would simply take the payments, receipt them and bank them.

*8. What would happen if part of the systems data became corrupt or was permanently damaged?*

If the data was lost or corrupted, there would be a delay in the transactions reaching the accounts. There is an IT backup on the server on a daily basis, therefore they can use that to retrieve any lost data.



**Interview for Housing Benefits**

*1. What responsibilities does the system in question have?*

Housing Benefits helps people pay their rent and helps people pay council tax.  
Holds all information regarding: Housing Benefits, to assess and pay claim, and figures.

*2. What types of data does the system need?*

To assess claims, you need to input, name, address, date of birth, insurance numbers, income, capital, etc. (personal information)  
Details of how much rent they pay  
Every aspect of their claim is included.  
Financial details – sensitive information

*3. What types of software or hardware does the system need?*

Mainframe system, ANITE software  
Everyone has software on PC  
Hosing offices can view details if have access

*4. Is the data shared with any other systems?*

No, but other departments can have access to it.  
No personal data shared, only people that have access to it are within the Housing Rents Department.

*5. What control mechanisms are in place for information security?*

Certain access for certain users, depending on job title, description. When a new person enters the department, there are several people involved when creating a new user's ID.  
Lots of logons, password changes once a month

*6. Who are the users of the system, and how many are they?*

50 people – have update access  
Other officers (50-70) have view only access  
Council tax officers (40-50) has view only access

In all there are about 150 total users of the system.

*7. How would business be impacted if the system was down for 15m, 1hr, 1wk, or 1month?*

The officers would have nothing to do if the system was down even 10 minutes. Any longer than that could be disastrous, the officers would have no work to do. The longest unplanned down time that HAS occurred was less than a day, there were no major problems, just not much could be done on the system.

8. *What would happen if part of the systems data became corrupt or was permanently damaged?*

Don't know, but there are weekly backups done by the Legato system.

**Interview for Housing Benefits**

*1. What responsibilities does the system in question have?*

Tracy Hawkins is in charge of the system.

VME has limited access from IT, we just support the system to ensure it is running smoothly and maintain it. It is a package bought from ICL, extract data from database through ICL tools.

Data would be extracted in order to perform a Query.

*2. What kind of maintenance and upkeep is involved with the system?*

Initially, there was a lot, because we had to do checkups, but it has been running for a while and there have been hardly any changes to the system. It is a pretty stable system without many problems. One addition has been through bank accounts, so we had to implement that interface. It is a very secure system.

*3. Is the data shared with any other systems?*

Council Tax and Housing rents and repairs talk to each other and communicate with housing benefits, but they do not share data. There is an interface with those two.

*4. What control mechanisms are in place for information security?*

There is a full database dump everyday. There is an integrity check once a week to make sure nothing has been corrupted. The system has never have had to be restored from backup.

*5. Who are the users of the system, and how many are they?*

See Interview summary of Tracey Hawkins.

*6. How would business be impacted if the system was down for 15m, 1hr, 1wk, or 1month?*

15 min – users would be upset. The system is politically sensitive so it must be working in order for business to go on.

The response from IT would be to find out what happened.

The system would only go down if the network was down or if there was a batch failure during the night – that would be probably due to human error.

If the development environment is slightly different than the live environment a problem may arise. The system has flags that go up as soon as one thing goes down, and it stops any other things from happening so that the problem can be fixed. If there is something wrong because of ICL it is their responsibility to fix it.

*7. What would happen if part of the systems data became corrupt or was permanently damaged?*

I have no idea what would happen

Manual adjustments would be made because the system must work because the people getting benefits HAVE to get paid.

### Interview for SOSCIS

*1. What responsibilities does the system in question have?*

SOSCIS stands for Social Service Client Index, holds information on vulnerable adults and children with various situations, part of social services practices confidentiality. The job of it is to maintain the client index and assessments and proposals to deal with the clients on the assessments and to record information on high sensitivity groups. Paper files exist to store all sensitive information. The old system about to be replaced with a new system that will hold information on clients, mostly basic, by certain groups of people. Mostly paper records at the case level. Management of case workers is done by the system.

*2. What types of data does the system need?*

Name, address, client grouping for mental health client, ethnicity, date of birth, when referred to them, what the problem was, assessments, who did the assessment and some basic notes. Children are covered by a more frigid framework, about 200 children in care in system at one time, council is in effect their parents. Subsidiary information about the children in care, keyed off the main system.

*3. What types of software or hardware does the system need?*

Proprietary IDMS Database, not a relational database ICL mainframe system on the sixth floor.

*4. Is the data shared with any other systems?*

Very little data is shared with other systems. There is a reference number in SOSCIS, but none of the personal data goes outside the council. All data is protected by the Data Protection Act. Nothing in operation with the NHS, but have had pilot programs. There is no direct link; they would have to phone here. Need to find out what sharing can be done, a project needs to be done on that, sometime in the future.

*5. What control mechanisms are in place for information security?*

Access is only granted on request from a manager. There is quite a high staff turnover and there is a mechanism for new users, giving them new user service. IDMS lay down some basic procedures. There is a standard computer misuse warning when it is started up, not to share passwords or logins with anybody. It is a multi level login to the system, anyone using a VME mainframe gets a standard screen, section name is specified, etc...similar to all the other systems, payroll number is number used for access. Everyone has their own user ID and password, does not force them to change that password, SOSCIS is changed every month automatically from ICS.

6. *Who are the users of the system, and how many are they?*

80-90 concurrent users, but new system will have 300-400 workstations. About 60 in here, other ones in district offices in other establishments, those who deal with the people face to face with the clients. The new system is called Care First and those are estimates for the new one. Different phases in place so that the

7. *How would business be impacted if the system was down for 15m, 1hr, 1wk, or 1month?*

There was an outage at the end of the old year, there was a power supply problem and systems were out for two days. Could not sustain the outage for two days because information is held about clients, safety information, it is a high risk safety issue that meant people need access to the system to record or view information held by the system. Anything much more than a day and the risk levels start to go really high. Very much a matter of chance...short periods are not a problem, a few hours people start worrying about it. It's a fairly reliable system, the incident where there was a power failure has not happened very often. This would cause a problem with Care First because they want more information in it so they can stop recording information on paper files. Raises the risk factor more than what it is now by not having a paper backup file.

8. *What would happen if part of the systems data became corrupt or was permanently damaged?*

If it is beyond recovery, they would be unable to report to government...there are statutory requirements to report how they are doing and what they are doing. They wouldn't be able to get all the information back in, be a black mark but nothing much else. Could be recreated but it would cost money. Failed safe services to children, not sure of outcome, re inspection and joint review to inspect the whole department, not sure what the outcome will be but in that context it will be less good to not be able to do the returns. Pretty drastic scenario, chances of losing the data are not very high. Backup recovery systems are there for a reason.

**Interview for Legato tape backup system**

*1. What is the origin of the name 'Legato'?*

Legato is a French company – the actual product is called Networker, but it is referred to by all the employees as Legato.

The company ICL installed the system for us and they basically support any problems that we have. One of my guys, Mike, looks after it. If there are any problems, he first will look at website, and if there isn't an update to the software that could solve the problem, he calls ICL and they respond within a couple hours. They might RAS in, or come down with some replacement part.

*2. What does legato do, in detail?*

It backs up most of our servers. A client needs to be installed on each server, the Legato network client. Basically you can set up different groups on the servers (about 80 servers on legato) and you can schedule the different groups to be kicked off Legato at certain times, and schedule backups by group

On the weekend we tend to do the full backups. Most of the servers are set to differential backups daily, with full backup on weekend

On Monday you back up level one, Tuesday, do changes from Monday and Tuesday, Wednesday do 3, so by Friday you have the week's changes, then the weekend you do everything. There are a few systems that do a full backup during the week, but for the most part this does not happen.

Monday morning – the full back-up tapes are ejected and taken off site

*3. Can you give us any particulars on the specific systems?*

Talk to Paul Biggs for the mainframe ones...they use the same robot but its not Legato tape. In the machine room you've got a robot, with 2 Legato tape drives, and the other is VME – they work independently, although use the same robot. They are two separate systems. Legato backs up Unix and NT servers. If we have a new server, put it in a group. But the VMA has tapes but need to talk to Paul Biggs.

We back up all of the NT and UNIX systems you are interested in. There are special clients for exchange that are more expensive. The legato exchange client is a couple grand, whereas the normal one is a few hundred. Backup SQL client and exchange client costs more

Part of the entire rental from ICL, includes mainframe robot and legato

It is very uneconomical, because I am sure we could put our own system in. In fact, when the lease expires in a few years, we want to do it ourselves, and we are looking into it. It is very expensive, and it is all rented off ICL

*4. What if the backup system failed to work?*

We have got a multi change dle tape drive, which we could use, and schedule backups on most critical stuff...legato itself is being backed up itself onto a DAT tape drive....if legato went down, we could restore that. Critical files necessary to quickly rebuild legato are dumped off every night to a server. It is important to keep all the indexes of what we need to do to restore the system.

*5. Say legato failed to work, and there were no legato backup working, what would happen?*

If the server went down, the worst case scenario would be ICL comes in, gives us a new server, we restore files...it depends on what goes wrong, but the hardware bits are covered by ICL, and we could quickly rebuild the legato system with one or 2 days

Weve got the tapes off of site anyway, so the worst case scenario would be that they lose one week's worth of work...worst case scenario, robot malfunctions and melts all tapes on Friday, so we lose a weeks worth of work, but have everything off site  
Its only taken off site once a week

*6. Do you check the Legato system to make sure it works??*

No, but we do 2 to 3 restores every day, so we know it is working...that is probably a good enough check with me, but it might be important to do a little more checking.

*7. Has legato failed big-time?*

Yeah, we have had some big problems, but we have got them sorted out by now – We had our daily backups working alright, but the weekend ones were having some problems – Legato was trying to back up the systems at the same time, a network problem. So the weekend ones were touch and go, but that was months ago and we haven't had any problems since then. ICL doesn't have the skills you would think they ought to have. The problem, which we ended up solving, should have been solved easily by the ICL support team. We were staggering the full backups weekly to do that.

*8. How long have we had legato system?*

Since end of 1999 – everything was working fine, then remote sites were not backing up, which stumped us for a few months, but then we got around that, so we backed some onto the old dat tapes – and then sometime last year we ran into the problem I mentioned before

*9. Could ICL's lack of skills be a problem in the future?*

Yes – each tape had a parallel setting – all we needed to do was change that, essentially they should have known that



We have for years been an ICL site – but it is very expensive and it is a lot of money.

We may have to rethink our backup strategy

Large scale restores – build one of the servers – 3 or 4 weeks ago – ran out of space so we had to go out buy new hard drives, and restore 30 Gigabytes – took a long time – almost the entire weekend

*10. Would it take a while to restore a few systems if a few servers went down and needed a complete rebuild?*

Well, it did take the better part of the weekend for 60 Gigabytes.

Group Interview for Systems and Projects

1. *Network logon issues*

- a.) How often do you encounter problems with network access?
- b.) Does it affect work substantially?

GW: Not too often, but find individual servers do.

SL: Sometimes permissions take a while so you think you have access but don't really.

GW: Sometimes servers are temperamental.

CN: That's been the email server recently, the problem today, it's been a high risk because they don't really know about the fault if the email is not working.

SL: Appears to be a problem with exchange

CN: Service desk is at fault in this case.

SL: Very secure, so secure nobody knows the password.

SL: It's been bad today, but not too bad usually.

CN: This peculiar combination has been real bad since they can't get emails from the helpdesk.

GW: Network doesn't really have responsibility for the problem, usually down to the servers rather than a network problem.

CN: When exchange has its problems, its bad, but once its solved its solved for good, not very frequent problems.

SL: Doesn't happen very often, but when it does, there is a severe problem.

2. *Password use and control*

- a.) How many passwords do each of you have?
- b.) How often are you required to change them?
- c.) Can they remain the same at all?
- d.) Is it possible to use the same password for multiple accounts, and do you?
- e.) What types of passwords do you use (ex. Complex, simple, names, etc.)?
- f.) Where do you store your passwords (on paper, memorize, etc.)?

CN: Depends on whether they are live or development, don't have passwords to most live systems.

SL: Access to almost every development system because they are developed here. GW: If someone calls in then I log in as myself and fix the problem, have dozens of passwords.

SL: Mainframe is very secure and many disciplines. They allow the permissions; they have access but can't see live systems. Not much control on UNIX systems, no direct accessing.

CN: Could fiddle with the UNIX, but so disciplined by mainframe that they still use a third party.

SL: NT servers are becoming more widely used, don't have many procedures as of yet, but procedures will come into effect. In DSG they have administrator passwords, above that are databases, have most permissions, with applications there are different tiers of users that can be requested by the users and controlled by the senior users. There are about four levels of them.

CN: Users have control over who has access to what within the system.

CN: All the mainframe passwords are changed once a month by a program, the people that need them get them in sealed envelopes.

GW: Depends on the system

SL: Once a month once you're in the system, only has a rollover of two passwords. Different systems have different rules.

CN: computer generated passwords create a problem because they are so difficult to remember.

GW: I have a little notebook where they are hidden, but that's secret

CN: I have mine memorized, but there's a way that I have it remembered. It can be a pain sometimes, but depends from system to system.

SL: One place I worked did not allow any words from a dictionary, difficult to remember, but secure until you have to write it down until you remember it.

### 3. *External logon (i.e. from home or field office)*

a.) Do people log on from outside the main office? How often?

b.) Do you use RAS?

c.) If/when you connect to RAS, are you connected to anything else?

d.) Any problems with that?

e.) Should remote logon be more accessible?

GW: Does not at all

CN: Every other week, to make sure everything works right.

SL: Uses it to look at emails while on leave, use the internet to get the email, but direct connection to network through dial up.

GW: If you were logged on to the intranet could you connect to anything else? CN: access to internal email as well as intranet.

SL: Most of the permissions can be granted, but some things are too slow so they aren't done.

CN: System log to see which system is up or down, versatility to different things. I have broadband, so broadband can be used and dialup can be used too, so that someone can look at that and log on to the network. I have mine fire walled so it does not really matter.

SL: The program he used was too secure so that he couldn't get on himself. Broadband is not too widely used, but it might be in the future and there are a lot more exposure risks present with broadband. There are six users of VPM, being developed, Gurmel has it but doesn't really need it.

### 4. *Use of portable workstations (i.e. laptops)*

a.) Does the division have laptops available to borrow?

b.) What kinds of procedures are there when you borrow a laptop?

c.) Do you store any information written within the case, such as passwords, etc.?

d.) How many employees use portable workstations?

e.) What would happen if one was lost or stolen?

CN: Each team has a laptop and mobile with it, whoever is on standby gets the laptop and mobile phone.

SL: Each team has a laptop assigned to it; nobody can just take one home whenever they want.

CN: Each one is configured for the team so it will only be good for that team.

CN: No passwords within the cases that are known of.

SL: No passwords that are specific to the laptop, so not really any in cases or could be found anywhere. There are three laptops that go out in systems and projects.

CN: Aware of not leaving it in an unlocked car, it has been made aware that they have to be careful.

SL: Everyone knows what the thing is, but they really have no use for the laptop.

CN: Hard disks are not used very much because there is not any kind of a backup. No reason for data to be held on the laptop itself.

SL: If a laptop were missing, no security issues, only the property loss.

CN: The passwords would all be changed for anybody that may use the machine.

##### 5. *Anything else?*

SL: An auditor asked Steve once if they had a list of signatures so that when there is a request, they could check and see if it was authentic. They really did not, so it appears that at times procedures are not in place that well. Most of the issues are procedural, rather than issues pertaining to actual information security. There are some issues of social engineering that must be considered.

Group Interview for Desktop Support Group

1. *Network logon issues*

- a.) How often do you encounter problems with network access?
- b.) Does it affect work substantially?

DL: Very rarely

PD: Agrees, users have more problems than people here.

DL: Users don't quite understand how to logon, simple to IT people not so simple to other people, can't get in and get frustrated. It is more of a user error than a failure.

2. *Password use and control*

- a.) How many passwords do each of you have?
- b.) How often are you required to change them?
- c.) Can they remain the same at all?
- d.) Is it possible to use the same password for multiple accounts, and do you?
- e.) What types of passwords do you use (ex. Complex, simple, names, etc.)?
- f.) Where do you store your passwords (on paper, memorize, etc.)?

PD: A lot of the servers have similar passwords or the same passwords, about forty passwords in all. Each server has a local administrator password, about 100 servers that have some the same and some different.

DL: Passwords for applications that they use. By and large, many are coded into the login so they don't have to be remembered anyways. There are about ten more for additional systems. They use around ten passwords on a day to day basis. There are no requirements system-wide to change administrator passwords, maybe something that should be done.

PD: Some users do not have forced password changes. There are some groups with thin client users that you can type your username and password and they can just let you in.

DL: Don't change them unless there is an unusual circumstance. Most are changed every few months if they are used often. Nothing in place to change them should be something in place. They are allowed to put the server passwords in themselves, mixture of numbers and letters, not extremely complex, but reasonably complex. Other passwords are less than complex. CRN system had passwords allocated to them, can't change them at all, only person that could change it is the system administrator. Some passwords are very important and some are not at all. None of the systems that have simple passwords are low level security and low priority. All passwords are kept in a secure area.

PD: Kept in a database which is password protected.

DL: The problem would be the physical location of the paper copy of passwords.

PD: Should be protected better, they should have to sign it in and out.

DL: May be a problem having all of the passwords on one sheet, but it is not a likely problem. A different method should be used, always arguing about what is the best way to be doing this.

PD: Should probably change them more often.

### 3. External logon (i.e. from home or field office)

- a.) Do people log on from outside the main office? How often?
- b.) Do you use RAS?
- c.) If/when you are connected to RAS, are you connected to anything else?
- d.) Any problems with that?
- e.) Should remote logon be more accessible?

DL: Use RAS once a week.

PD: Doesn't use it very often, uses outlook web access from home instead. It has been decided that all RAS servers will have to have some sort of VPM software.

DL: On paper the problem with broadband is a high risk, but in actuality isn't so bad. PD: Someone can hack into your machine, then copy your password when you RAS in, then they can RAS in as the worker whose machine they hacked into.

DL: Not that big of a risk for people who don't use it too often.

### 4. Use of portable workstations (i.e. laptops)

- a.) Does the division have laptops available to borrow?
- b.) What kinds of procedures are there when you borrow a laptop?
- c.) Do you store any information written within the case, such as passwords, etc.?
- d.) How many employees use portable workstations?
- e.) What would happen if one was lost or stolen?

DL: Laptops are used, approximately six within the DSG group. About three of them go back and forth, the others stay here, aren't transported very often. Laptops are assigned to given individuals, do not have to ask to take them out. They could ask to borrow one from another one of the individuals with a laptop. Not an official procedure for that. The machines are for work, if someone needs to use one for work at home then that is a possibility. Work takes precedent over other uses. The people working with laptops do not have access to confidential data, they are support engineers, do not have actual data that can be sensitive. Not like someone working for social services or the department of defence losing a laptop. If a laptop was stolen or lost, it would be reported to the service desk, get in touch with admin who would put in an insurance claim and notify the police. Could crack the local administrator passwords and gain access to the Merton system, could be a minor security breach, but only allow them onto an individual computer at a time, not a server or system.

## Appendix Q: Officer Time by System

<i>Employee</i>	<i>System</i>	<i>Officer Time (min)</i>
	<b>Council Tax</b>	
Peter Brown	Interview IT	30
Colin Lloyd	Interview Senior User	30
	Questionnaire	45
	Questionnaire	24
	<b>Housing Benefits</b>	
Krystyna Kuber	Interview IT	30
Tracey Hawkins	Interview Senior User	30
	Questionnaire	25
	Questionnaire	10
	<b>Housing Rents and Repairs</b>	
Colin Mason	Interview IT	20
John Sykes	Interview Senior User	30
	Questionnaire	25
	Questionnaire	20
	Questionnaire	20
	<b>Exchange and Outlook</b>	
Richard Warren	Interview IT	30
Mark Kitson		
	Questionnaire	25
	<b>Financial Accounting</b>	
Rob Heap	Interview IT	30
	Questionnaire	30
	<b>SOSCIS</b>	
Felix Stride-Darnley	Interview Senior Users	45
Geoff Davey		
	Questionnaire	5
	Questionnaire	25
	Questionnaire	45
	<b>Payroll System</b>	
Steve Key	Interview Senior User	25
	Questionnaire	20
	<b>Cashiers Office</b>	
Ray McInnis	Interview Senior User	30
	Questionnaire	30

# Appendix R: Project Timeline

ID	Task Name	Mar 10, '02					Mar 17, '02					Mar 24, '02					Mar 31, '02					Apr 7, '02					Apr 14, '02					Apr 21, '02				
		S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S
1	Orientation to Agency	■																																		
2	CRAMM Orientation		■	■	■	■																														
3	Updating Methodology		■	■	■	■																														
4	Schedule Interviews							■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	
5	Interview Process							■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	
6	Asset Identification							■	■	■	■	■	■	■																						
7	Asset Valuation																																			
8	Threat Identification							■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	
9	Threat and Vulnerability Valuation							■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	
10	Outline Final Chapters																																			
11	Conduct CRAMM Risk Analysis																																			
12	Complete Gap Analysis																																			
13	Final Draft																																			
14	Final Presentations																																			