Walton Centre

Risk Assessment

Document History

Date	Version	Author	Changes
01/10/2004	1.0	A Cobain L Wyatt	

Table of Contents

1. Introduction

Information and information systems are important corporate assets and it is essential to take all the necessary steps to ensure that they are at all times protected, available and accurate to support the operation and continued success of the Trust.

The Trust acknowledges that we must demonstrate to third parties our expertise in security technology and implementing it. To achieve this it is recognised that we must protect our own assets as well as the environment.

The aim of the Trust Security Policy, Security Standards and Work Instructions Manual is to maintain the confidentiality, integrity and availability of information stored, processed and communicated by and within the Trust. These standards, procedures and policies are used as part of the information security management system (ISMS) within the Trust.

2. Responsibilities Within This Standard

Particular responsibilities within the standard are defined as:-

Review and Maintenance	Information Security Officer
Approval	Information Security and Governance Group
Local adoption	Line Managers (in scope)
Compliance	All staff and contractor (in scope)
Monitoring	Information Security Officer Information Security Auditor

3. Methodology

3.1 Risk Identification

The levels of risk for the identified systems are determined by combining the following:

- The values of assets (data, physical and software);
- The levels of threat to these assets;
- The levels of vulnerability to these threats.

Data assets are valued by carrying out interviews with staff who can speak authoritatively about the way in which the data is used, considering such incidents as unavailability, destruction, disclosure and modification. In the case of the Walton Centre, where relevant, the System Administrator and System Owner were identified as interviewees for providing information on the value of data assets.

In each of these areas a 'realistic worst-case scenario' was identified and qualitatively assessed by looking at the possible resulting impacts. For example the scenario of the data being unavailable for an hour.

The threat and vulnerability assessment followed on from the impact analysis and considered many potential problem areas, each of which may affect different parts of the system in different ways, potentially causing different impacts.

The threat categories are grouped into the following areas:

- Logical threats;
- Communications threats;
- Failures of equipment;
- Errors;
- Physical threats.

The level of the threat acknowledges not only the actions of Trust staff but also the actions of legitimate third parties and outsiders.

These levels, together with the value of assets assessed during Stage 1 of the review, were then combined to give a measure of risk. A high asset value combined with a high threat or vulnerability rating would lead to a high measure of risk, whereas a lower asset value with a lower threat or vulnerability rating would result in a lower or baseline level of risk.

3.2 Maintenance of the Risk Assessment

All organisations are subject to change brought about by modifications to the operational and technical environments. These in turn change the risks presented to the organisations, resulting in a requirement to review any previously conducted Risk Assessments.

Consequently, this Risk Assessment should be subject to regular maintenance by an appropriate person to be nominated within Informatics Services Department. Such an individual would need to have some knowledge of CRAMM and risk assessment methodology.

Although a generic model has been created, the levels of threat and vulnerability can be altered to reflect any such changes. The use of the toolkit will considerably simplify such maintenance.

It is recommended that a formal review of this Risk Assessment be conducted at least annually, and also following major changes to The Walton Centres infrastructure or the purposes for which it is used.

4. Asset Valuation

4.1 Introduction

To value data assets, a set of established guidelines within CRAMM are used. This will then drive the highest impact value in a given scenario.

In order to determine the severity of these impacts, CRAMM provides a series of guidelines. The worst-case scenarios outlined by the interviewees are compared against these guidelines to determine where on a scale, which ranges from 1 (Very Low) to 10 (Very High), each of the impacts appears.

For example, the unavailability of the Network system and/or data, even for a short period could, in the worst case scenario, result in the inability to provide an appointment on any of the Trust systems. *This could result in the death of more than one individual*.

The CRAMM data valuation guideline in this case would therefore be (*Personal Safety)*. The worst scenario would be that this is likely to lead to (*the life of an individual or group of individuals being threatened, therefore the rating given was 8*).

The loss of different types of data would have different impacts. For example the unavailability of administration data for a short period would not result in patient safety being compromised. For this scenario the guideline used was Policy and Operations of a Public Service. The disruption caused by staff not being able to access administration data for 1 day would result in the inefficient operation of one part of the organisation.

4.2 Assets

The assets are valued by conducting interviews with personnel who are able to speak authoritatively about the way the data is used. In each case this was the system administrator and/or system owner. Staff were asked to outline the realistic worst case scenarios that could arise from the following impacts:

- Unavailability of the data;
- Disclosure of the data;
- Accidental or deliberate modification of the data;
- Destruction of the data.

Whenever possible during asset valuation existing countermeasures are ignored to avoid making incorrect assumptions about their effectiveness and a baseline is used.

5. Threat and vulnerability assessment

5.1 Introduction

This section describes the assessment of threats to, and the vulnerabilities of, the assets that comprise the systems described in the report.

Stage 1 of the CRAMM review looked at the potential impacts (i.e. unavailability, destruction, disclosure and modification) to evaluate the possible effects of a failure, disaster or breach in security. Stage 2 assesses the potential threat types that could cause these impacts to occur and the vulnerability of the system to these threats.

These threat and vulnerability assessments, together with the values assessed during Stage 1, allow the measures of risk to the system to be calculated, as detailed in Chapter 7.

5.2 Process Description

The Threat and Vulnerability Assessments were obtained by the completion of questionnaires with appropriate staff. This utilised their experience, technical expertise and knowledge of the systems being reviewed. The assessment of the threat and vulnerability levels was then calculated from the answers given by CRAMM.

The threats were assessed on the following scale:

- Very Low (considered to be unlikely to ever occur);
- Low (considered to be likely to occur only in unusual circumstances);
- Medium (considered to be likely to occur occasionally);
- High (considered to be likely to occur regularly);
- Very High (considered to be likely to occur very frequently).

The vulnerabilities were assessed on the following scale:

- Low (if the threat did occur, it is felt unlikely that it would damage or disrupt the system);
- Medium (if the threat did occur, it is felt it could damage or disrupt the system);

- High (if the threat did occur, it is felt it would definitely damage or disrupt the system).

The following sections set out an overview of each of the threats, an assessment of its likelihood and the type of measures that can be taken to combat the threat.

The threat and vulnerability analysis looks at many potential problem areas, each of which may affect different parts of the system. The threat types fall into the following categories:

- Logical threats;
- Communications threats;
- Failures (of equipment, services and software);
- Errors;
- Physical threats.

5.3 Threats

Individual threats were investigated in some detail against each of the assets. For example the threat of masquerading of user identity was looked at in respect of all the systems. The results were therefore different for each asset and impossible to summarise.

The descriptions below represents an overview of the types of threat considered.

Threat	Description
Masquerading of User Identity by Insiders	The threat of masquerading of user identity by insiders covers attempts by authorised users to gain access to information to which they have not been granted access or carry out unauthorised actions. These users may attempt to gain access to that information by posing as another user by guessing their password, seeing it being typed in, or in a number of other ways.
Masquerading of User Identity by Contracted Service Provider	The threat of masquerading of a user identity by service providers covers attempts by people working for a contractor; for example a hardware maintenance engineer, attempting to obtain unauthorised access to information.

Threat	Description
Masquerading of User Identity by Outsiders	The threat of masquerading of a user identity by outsiders covers attempts by outsiders to obtain unauthorised access to information by posing as an authorised user.
Unauthorised Use of an Application	Unauthorised use of an application refers to the possibility of an authorised person using the facilities to which they have been granted access for unauthorised purposes. This covers the possibilities of people committing frauds or looking up information for personal rather than business reasons.
Introduction of Damaging or Disruptive Software	Damaging and disruptive software covers viruses, trojan horses, worms or other such examples of software that have been deliberately developed to cause damage or disruption to the work of the system.
Mis-use of System Resources	Mis-use of resources refers to people using facilities for personal purposes rather than the ones for which they were originally developed. It covers, for example, the possibility of people playing games on IT systems, setting up their own databases, or using facilities for personal correspondence.
Communications Infiltration	Communications infiltration covers the following types of event: ➢ Hacking into a system using, for example, buffer overflow attacks; ➢ Denial of service attacks; ➢ Flaming attacks; ➢ Spamming.
Communications Interception	Communications interception covers: ➢ Interception of messages being passed over a network; ➢ Monitoring the levels of traffic on a network link.
Communications Manipulation	Communications manipulation covers:

Threat	Description
	➢ Interception and alteration of a message ➢ Insertion of false messages ➢ Deliberately causing messages to be delivered out of sequence ➢ Deliberately delaying the delivery of a message Deliberately mis-routing a message to an unintended recipient
Communications Failure	This threat covers such incidents as: ➢ failure of the communications link; ➢ the unavailability of the network service provider; ➢ non-delivery of messages; ➢ accidental denial of service.
Embedding of Malicious Code	This threat covers e-mail viruses, and hostile code incorporated into e-mails or Active-X applets
Accidental Mis-routing	This threat covers the possibility that information might be delivered to an incorrect address when being sent over the network.
Technical failure of Host	The failure of a host or server refers to hardware faults such as failures of the CPU or hard disk.
Technical Failure of Storage Facility	This threat covers hardware failure of tape and disk storage facilities.
Technical Failure of Print Facility	This threat covers the failure of printers whether local or networked.
Failure of Network Distribution Components	This type of failure includes failures of network components, such as the gateways, bridges and routers that make up the wide area network. It also includes physical damage to the network connection.

Threat	Description
Technical Failure of the Network Gateway	This threat covers the failure of the network gateway resulting in a loss of network access.
Technical Failure of Network Management or Operation Host	This threat covers the failure of those hosts used to manage or operate the network.
Technical failure of the Network Interface	This covers the failure of the interface between the Trust's communications equipment and the network infrastructure.
Technical failure of Network Service	This threat examines the factors that increase the likelihood of a failure of the network service
Power Failure	This threat covers the failure of the power supply to Trust premises
Air Conditioning Failure	This threat covers the possibility that work may need to be suspended because temperatures fall outside acceptable limits, caused by air conditioning unit failure.
Failure of System and Network Software	The failure of the system / network software refers to faults and failures in the operating system and networking software that is used by the Trust.
Failure of Application Software	The failure of the application software refers to faults and failures in the applications used to provide network management.
Operations Error	The threat of an operator error covers the possibility that the staff responsible for operating the IT systems might make mistakes when carrying out their work. This could include setting up the security of the system incorrectly or failing to make or test back-ups.
Maintenance Errors	Maintenance error covers the possibility of mistakes by those people responsible for maintaining both the hardware and software of the system. It covers the work of both members of staff and people working for third party companies who have

Threat	Description
	been contracted to perform these duties.
User Error	This threat covers the possibility that users may make mistakes when using applications.
Fire	The threat of fire covers the possibility of a fire affecting the physical assets that support or make up the systems. This includes documentation and storage media.
Water Damage	There have been incidents in the past where water damage has occurred. This has been caused by excessive rainfall on flat roof premises and the fact that water pipes serving central heating systems pass over key assets.
Natural Disaster	This covers the possibility of either a natural or man-made event causing physical damage to the location or surrounding area.
Staff Shortage	This covers the staffing resources in terms of both quantity and skill sets.
Theft	This covers the possibility of theft either by employees (insiders) or members of the public (outsiders).
Wilful Damage	This covers any act of vandalism on equipment that might be carried out by employees (insiders) or members of the public (outsiders).
Terrorism	This covers the actions of organised groups seeking to pursue political objectives by force.

6. Measures of risk

Stage 1 of the CRAMM review looked at the potential business impacts (unavailability, destruction, disclosure and modification) to evaluate the possible effects of a failure, disaster or breach in security. Stage 2 assessed the potential threat types that could cause one of these impacts to occur and the vulnerability of the system to these threats. These threat and vulnerability assessments, together with the values assessed during Stage 1, allow the measures of risk to the system to be calculated.

The measure of risk (MOR) for each asset group is established by combining the asset values with the threat and vulnerability ratings. Within CRAMM, the measures of risk are represented on a scale of 1 - 7.

These measures of risk are used to select the appropriate security countermeasures to counteract the risk. A measure of risk of 1 or 2 indicates that only baseline countermeasures are required. Conversely, a value of 7 implies that a very high level of security should be implemented.

The results of the risk assessment are included within ISMS 05: Risk Assessment & Management.

7. Compliance

7.1 Responsibility

It is the responsibility of all users to ensure that they have read, understood and abide by this standard.

7.2 Review and Monitoring

The Walton Centre has in place routines to regularly audit compliance with this and other standards.