NHS
Greater Manchester Shared Services

GMSS Information Risk Policy

Review Date: February 2022

Document Control

Title / Reference:	Information Risk Policy
Status:	Approved
Version:	V2.1
Date Issued / Ratified:	March 2020
Originator of Document and Job Role:	IG Team
File Classification:	Official Data
Retention:	Life of the organisation plus 6 years (place of deposit)
Target Audience:	All GMSS staff & 3rd party partners
Links to other strategies, policies, procedures etc:	• Data Security, Protection & Confidentiality Policy • Data Security, Protection & Confidentiality Framework • Confidentiality Audit Procedure • Data Security Breach & Incident Reporting Policy • Secure Transfer of Data Policy • Acceptable Use of IT / Information Systems Policy • Information Classification Policy • Records Management Policy • Risk Management Policy • Information Risk Policy • Subject Access Request Policy • Registration Authority (Smart Card) Procedure • Data Security, Protection & Confidentiality Staff Handbook **This list is not exhaustive**

Change History

Summary of Changes	Name	Date	Version
Recommend approval by the IG Group	IG Group	Nov 16	0.1
Recommend approval after some amendments	FPG	Jan 17	0.1
Amendments needed	SMT	Jan 17	0.1
Amendments to accommodate GDPR	IG Group	Aug 17	1
Standard review and amendments to link in with updated Risk Management Policy	IG Team	Feb 20	2.1

Review

Name	Role	Date	Version
K Rigden	SMT	Feb 17	1
IG Group	IG Group	Dec 17	2
IG Group	IG Group	Mar 20	2.1
Governance Committee	Governance Committee	Mar 20	2.1
Senior Management Team	Senior Management Team	Mar 20	2.1

Approval

Name	Role	Date	Version
K Rigden	SMT	Feb 17	1
IG Group	IG Group	Dec 17	2
IG Group	IG Group	Mar 20	2.1
Governance Committee	Governance Committee	Mar 20	2.1
Senior Management Team	Senior Management Team	Mar 20	2.1

Distribution

Name	Role	Date	Version
Saved in policy folder		Dec 17	2
Updated policy tracker		Dec 17	2
GMSS Publication scheme		Dec 17	2
The Bulletin		Jan 18	2
People Matters		Jan 18	2
Saved in policy folder		Feb 20	2.1
Updated policy tracker		Mar 20	2.1
GMSS Publication scheme		Mar 20	2.1
The Bulletin		Mar 20	2.1
People Matters		Mar 20	2.1

DOCUMENT STATUS:
This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of the document are not controlled

Contents

Appendices

1. Assurance Statement

This policy lays the framework for a formal information risk management programme in Greater Manchester Shared Services (GMSS) by explicitly establishing responsibility for information risk identification and analysis, planning for information risk mitigation, information risk management and its oversight.

GMSS and their management team are required to assure the formal introduction and embedding of information risk management into key controls and approval processes of all major business processes and functions of the organisation.

Information risk is inherent in all administrative and business activities and everyone working for or on behalf of GMSS continuously manage information risk.

It should be noted that this policy complements and works on the same principle outlined in GMSS's Risk Management Policy, which forms an integral part of the overall organisation Risk Management Framework. This policy specifically relates to risk associated with management information, records and data.

2. Introduction

Information risk is a factor that exists in all areas where information of a personal or confidential nature are used and managed.

This policy sets out the requirements placed on all staff in the use and management of information and the risks associated with using such information.

The policy takes key areas from the NHS National Patient Safety Agency "Risk Matrix for Risk Managers" and works in conjunction with the Risk Management Policy as well as the Data Security, Protection & Confidentiality Policy and Record Management Policy.

Information Risk management is a part of Information Governance (IG) and it is acknowledged that information governance, including the management of information risks become part of the culture of the organisation, ensuring that staff are aware of, and work to, good IG (and therefore information risk) practices.

3. Purpose & Scope

The purpose of this policy is to provide a consistent way of managing information risk in the organisation allowing the information to be managed in a way that highlights when information may be at a significantly high risk, thereby providing a layer of protection for patient, staff and the organisation. The highlighting of risk will then allow risks to be properly addressed and the risk managed in a way that is most suitable.

There are legal and statutory requirements for the protection of information, both personal and confidential, and this policy sets out how the risks to that information will be managed in compliance with those requirements.

This policy covers all organisational areas including information risk associated with third party provision of services.

4. Communication/Dissemination

This policy will be made available to all staff. The policy will be published, as a minimum, in the following ways:

- GMSS People Matters page,
- Publication in the Publication Scheme (Freedom of Information)

5. Definitions

Definitions used in this Policy and risk management include:

- **Risk:** The chance (probability) of something happening which will impact in an adverse way something of value. This may be damage to information or reputation or may involve injury or liability. In this context risk is measured as a product of "consequence" x "likelihood" which are given numerical values.
- **Consequence:** The result of a risk becoming a reality. For example injury, financial loss, damage. There may be more than one consequence for each risk occurring.
- **Likelihood:** What is the possibility of the risk actually occurring (becoming an issue).
- **Assessment**: The process of identifying and evaluating risks.
- **Management**: In this context, the management of the risk processes within an organisation.
- **Treatmen**t: Ways of mitigating risk. General risks mitigation involves avoidance, reduction of the risk (consequence, likelihood or both), transfer the risk to someone else, accept the risk.

Please refer to the Risk Management Policy for more definitions.

6. Roles and Responsibilities

Managing Director

The Managing Director has overall responsibility for Data Security & Protection within GMSS. As Accountable Officer, they are responsible for the management of Data Security & Protection and for ensuring appropriate mechanisms are in place across the entire organisation (GMSS) to support service delivery and continuity. Information Governance provides a framework to ensure that information is used appropriately and is held securely.

Caldicott Guardian

The Caldicott Guardian is the conscience of the organisation and is responsible for ensuring that national and local guidelines on the handling of confidential personal information are applied consistently across the organisation. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

Senior Information Risk Owner (SIRO)

The SIRO takes ownership of GMSS's information risk framework, as a member of the

Senior Management Team the SIRO acts as an advocate for information risk and provides written advice to the Managing Director on the content of their annual governance statement in regard to information risk. To fulfil their responsibility the SIRO will:

- Provide independent senior board-level accountability and assurance to SMT that information risks are addressed.
- Ensure that information risks are treated as a priority for business outcomes.
- Provide accountability and assurance to SMT that GMSS has embedded and is maintaining operational compliance with the Information Governance Framework policies and associated data protection, information security, information management and information technology processes and procedures.
- Play a vital role in getting the organisation to recognise the value of its information and enabling its optimal effective use.

Data Protection Officer (DPO)

The DPO informs and advises staff about their obligations to comply with GDPR, the Data Protection Act 2018 and other relevant legislation. The DPO monitors GMSS's compliance with data protection policies and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities.

Heads of Service

Heads of Service take responsibility for ensuring that the Data Security, Protection & Confidentiality framework is communicated and implemented within their service, and ensures that all staff remain compliant, including any temporary or contract staff.

Information Asset Owner / Administrator (IAO / IAA)

The IAO / IAA are responsible for ensuring that specific information assets are handled and managed appropriately. This means making sure that information assets are properly protected and that their value to the organisation is fully exploited.

Information Governance Team

Data Security & Protection responsibilities will be supported by the GMSS Information Governance Team and will be accountable for ensuring effective management, accountability, compliance and assurance for all aspects of the Data Security & Protection Framework.

They are responsible for:

- Supporting the SIRO in overseeing the management of significant information risks across GMSS.
- Developing and maintaining Information Risk Policy, Information Asset Registers and associated documentation.
- Overseeing information risks from across GMSS.
- Reviewing the Information Asset Registers and any information risks on a quarterly basis and undertake a risk moderation exercise if required.
- Arranging for awareness and identification training with all relevant employees as required.
- Recommending changes to the Information Risk Framework if necessary to

the SIRO (where applicable) and Governance Committee.

Head of Corporate IT & IT Security Manager

The Head of Corporate IT and IT Security Manager are responsible for ensuring that all GMSS electronic equipment and assets have adequate security measures to comply with data protection and data security legislation and regulations.

All staff

All staff, whether permanent, temporary or contracted, working in a clinical or non-clinical environment are responsible for ensuring that they are aware of the Data Security & Protection requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

All staff have a responsibility to ensure they complete the mandatory training requirements of the organisation, Data Security & Protection are part of these mandatory training requirements.

7. Information Risk Management Processes

The information risk management process will take place using the NHS “5x5 Risk Matrix” as detailed in the NPSA’s Risk Matrix. This document contains guidance on how to interpret the scores that will be attributed to risks and provide the basis for information risk reporting to SMT. Information on the matrix relating to this policy may be found in Appendix A.

Data Protection Impact Assessments (DPIA)

Risks to personal and confidential information that arise as a consequence of changes to systems / process (projects) will be identified via the completion of a DPIA. This will be a questionnaire completed by the project manager or other suitable project member who will be considered by IG and where necessary a report on information risks and actions to be taken will be produced. This will be managed as part of the overall project with IG oversight at all times.

The DPIA process and proforma are available from the Information Governance Team or on People Matters.

Local Information Risks

It is the IAO’s responsibility to be aware of, and formally record, information risks to the assets which they manage. Many risks will be managed and resolved locally, but higher risks will need to be managed via IG in order to ensure the organisation is aware of those risks and can be assured that active management of them is in place.

It is necessary to ensure a consistent approach to risk assessment and risk priority ratings so that all risks can be initially prioritised and ultimately agreed by the appropriate governance group. The Senior Management Team will be informed of significant risks.

To ensure this consistency and assurance to each of GMSS’s Committees that GMSS are managing their risks adequately, the following tools are used:

- Risk Management process and action plans.
- Risk Analysis and recording.
- Risk Consequence Table.
- Risk Rating Matrix.
- Specific Risk Assessment Form.
- Risk Register Template.

Management of Information Risks

An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Please refer to Appendix B for more information on Information Assets

Information assets have recognisable and manageable value, risk, content and lifecycles. All breaches and incidents regarding Information Assets should be reported using GMSS online incident reporting system – DATIX.

Information risks will be managed locally, unless the risk score attributed to an individual risk is 15 or greater. The Risk Matrix and scoring is available for reference in the Risk Management Policy.

The treatment options for information risk are:

- **Avoid:** not proceeding with activity likely to generate the risk.
- **Reduce**: reducing or controlling the likelihood of consequences of the occurrence.
- **Transfer**: arranging for another party to bear or share some part of the risk, through contracts, partnerships, joint ventures, etc.
- **Accept**: some risks may be minimal and retention acceptable.

Risks will be managed via a standard risk log format that will enable risks to be managed consistently across the organisation ensuring a high quality level of support, where it is necessary.

Information risks relating to personal and special category data and confidential information in hard and soft format will be systematically evaluated throughout the Information Governance team and the Risk Manager and action taken on a risk assessed basis. All significant breaches will be included in the IG report which will link in with Datix Process.

All special category data will be handled as ‘confidential information’, kept securely in locked cabinets and via appropriate permissions on the network. It will be made available on a need-to-know basis and advice provided to staff as appropriate.

Policies are in place to support information risk management including information security, data protection, confidentiality and record management on GMSS’s People Matters page.

All internal staff as well as third parties, contractors, agency staff will be required to sign and follow GMSS Confidentiality clauses.

Escalation of Risks

Please refer to GMSS’s Risk Management Policy for more information on escalation of

Risk. The IAO will be responsible for managing the risks; reporting and ensuring that suitable mitigations are put in place either locally or with support from information governance/risk management.

Any Information Risks that are considered high risks will be reported through the Corporate Risk process.

Proactive planning will be undertaken for investigating and identifying risks through different scenarios, regular policy reviews, ICO recommendations and assessment of sources of legal weight and admissibility of evidence for reducing risks.

Information Risk Management Training

NHS Digital E-Learning is used for Additional IG Training as part of your job role. Please see the IG TNA for further details.

Access to the NHS Digital E-Learning Portal can be obtained from the IG Team.

All staff must complete all Mandatory and IG TNA role specific IG Training.

Information Asset Register

GMSS will establish a programme to ensure that their Information Assets (IA's) are identified and assigned to an IAO. The SIRO will oversee a review of the organisation's Information Asset Register to ensure it is kept up to date, complete and robust.

All critical IA's will be identified and included within the Information Asset Register (IAR), together with details of business criticality. Risk Assessments are to be carried out by the IAO and/or IAA using the Information Asset Risk Assessment Form. See Appendix C.

In order to improve the usability and maintainability, the Information Asset Register may be organised by service, rather than by location.

Support

Support will be provided to staff in assessing risk and managing their local processes by the IG and Risk teams, locally. Where necessary these teams will seek further advice on behalf of the department making the query.

8. Training and Awareness

This policy will be made available to all staff via The Bulletin and published on GMSS Website and on People Matters for GMSS staff.

All staff are responsible for adhering to the General Data Protection Regulations 2016, Caldicott Principles, the National Data Guardian Data Security Standards, the Data Protection Act 2018 and the common law duty of confidentiality.

All staff are mandated to undertake Data Security Awareness training on an annual basis.

Staff will receive guidance regarding this policy from a number of sources:

- Policies and procedure located on People Matters;
- Line manager;
- Other communication methods (e.g. staff briefings, team meetings, IG updates).
- The IG Team.
- Other training methods will be used as necessary to meet individual needs due to disability.

9. Classification of Information

GMSS implement appropriate information classifications controls, based upon the data security legislation.

Further details of the classifications controls can be found in the Information Classification Policy and the Records Management Policy.

10. Legislation & Guidelines

A set of procedural documents will be made available via People Matters.

- General Data Protection Regulations 2016
- Data Protection Act 2018
- The National Data Guardian Data Security Standards
- Confidentiality: NHS Code of Practice
- Common Law Duty of Confidence
- Human Rights Act 1998
- Computer Misuse 1998
- Electronic Communications Act 2000
- Guide to the Notification of Data Security and Protection Incidents.
- ISO31000:2009 - Risk Management – Principles and Guidelines.

11. Equality Statement

GMSS aims to design and implement services, policies and measures that are fair and equitable. As part of its development, this policy and its impact on staff, patients and the public have been reviewed in line with the GMSS legal equality duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on employees, patients and the public on the grounds of race, socially excluded groups, gender, transgender, non-binary, disability, age, sexual orientation, pregnancy/maternity or religion/belief.

The Equality Analysis has been completed and any associated policies and procedures will be analysed accordingly.

12. Monitoring and Review

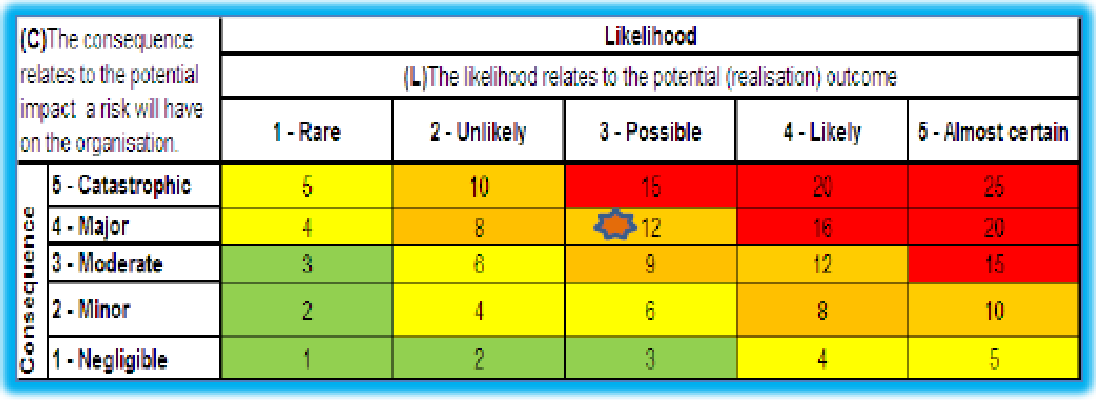
This policy will be monitored through staff awareness and supporting evidence to the Data Security & Protection Toolkit.

This policy will be reviewed on a two yearly basis and in accordance with the following as and when required:

- Legislative changes;
- Good practice guidance;
- Case law;
- Significant incidents reported;
- New vulnerabilities; and
- Changes to organisational infrastructure.

The next review is scheduled for February 2022.

Appendix A - Information Risk Scoring Matrix (taken from GMSS Information Asset Risk Assessment form)



(C)The consequence relates to the potential impact a risk will have on the organisation.		Likelihood				
		(L)The likelihood relates to the potential (realisation) outcome				
		1 - Rare	2 - Unlikely	3 - Possible	4 - Likely	5 - Almost certain
Consequence	5 - Catastrophic	5	10	15	20	25
	4 - Major	4	8	12	16	20
	3 - Moderate	3	6	9	12	15
	2 - Minor	2	4	6	8	10
	1 - Negligible	1	2	3	4	5

Appendix B - Information Assets

Assessing whether something is an information asset.

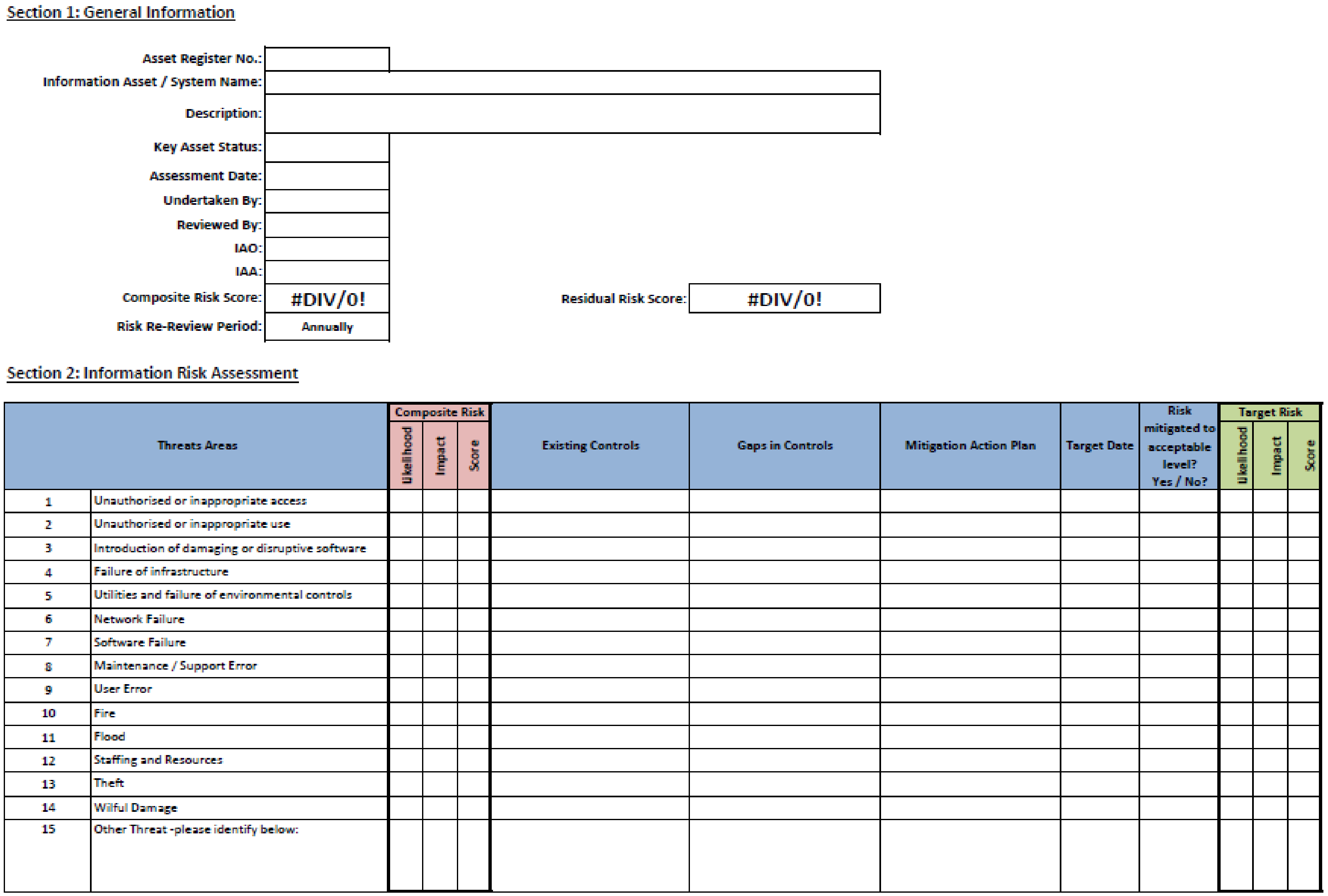
To assess whether something is an information asset, task the following questions:

- Does the information have a value to GMSS? How useful is it? Will it cost money to reacquire? Would there be legal, reputational or financial repercussions if you couldn't produce it on request? Would it have an effect on operational efficiency if this information could not be accessed easily? Would there be consequences of not having it?
- Is there a risk associated with the information? Is there a risk of losing it? A risk that it is not accurate? A risk that someone may try to tamper with it? A risk arising from inappropriate disclosure?
- Does the group of information have a specific content? Is there an understanding of what the information is and what it is for? Does it match the purpose associated with the information?
- Does the information have a manageable lifecycle? Were all the components created for a common purpose? Will they be disposed of in the same way and according to the same rules?

Examples of typical assets include:

Personal Information Content	**Software**
• Databases and data files • Back-up and archive data • Audit data • Paper records (patient case notes and staff records) • Paper reports	• Applications and System Software • Data encryption utilities • Development and Maintenance tools
Other Information Content	**Hardware**
• Databases and data files • Back-up and archive data • Audit data • Paper records and reports	• Computing hardware including PCs, • Laptops, PDA, communications devices e.g. mobile phones and removable media.
System/Process Documentation	**Miscellaneous**
• System information and • Documentation • Operations and support procedures • Manuals and training materials • Contracts and agreements • Business continuity plans	• Environmental services e.g. power and air-conditioning • People skills and experience Shared service including Networks and • Printers • Computer rooms and equipment • Records libraries

Appendix C – Information Asset Risk Assessment form (for reference only, contact IG for copy)



Section 1: General Information

Asset Register No.:			
Information Asset / System Name:			
Description:			
Key Asset Status:			
Assessment Date:			
Undertaken By:			
Reviewed By:			
IAO:			
IAA:			
Composite Risk Score:	#DIV/0!	Residual Risk Score:	#DIV/0!
Risk Re-Review Period:	Annually		

Section 2: Information Risk Assessment

	Threats Areas	Composite Risk			Existing Controls	Gaps in Controls	Mitigation Action Plan	Target Date	Risk mitigated to acceptable level? Yes / No?	Target Risk		
		Likelihood	Impact	Score						Likelihood	Impact	Score
1	Unauthorised or inappropriate access											
2	Unauthorised or inappropriate use											
3	Introduction of damaging or disruptive software											
4	Failure of infrastructure											
5	Utilities and failure of environmental controls											
6	Network Failure											
7	Software Failure											
8	Maintenance / Support Error											
9	User Error											
10	Fire											
11	Flood											
12	Staffing and Resources											
13	Theft											
14	Wilful Damage											
15	Other Threat -please identify below:											