NHS
West Essex
Clinical Commissioning Group

Information Risk Policy

Policy Reference: IG06

Brief Summary:
This policy sets out the principles by which the Clinical Commissioning Group will embed within its working practices, to ensure that all foreseeable and encountered information risks are identified and controlled at each stage to prevent or minimise the likelihood of a recurrence.

Compliance with all CCG policies, procedures, protocols, guidelines, guidance and standards is a condition of employment. Breach of policy may result in disciplinary action.

Document Management

Version	Date Issued	Details	Brief Summary of Change	Author
0.1	14/03/2013	Draft	New Document	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
1.0	03/12/2014	Draft	Amendments made following comments from IG Steering Group	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
1.1	18/12/2014	Draft	Key Contacts Added following amendments	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
1.2	05/03/2015	Final	Approved by the West Essex CCG Board	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
3.0	07/10/2016	Final	Review approved by West Essex CCG Executive Committee	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)

For more information on the status of this policy, please contact:	
NHS West Essex CCG	Information Governance Team
Approved by	Executive Committee
Approval Date	7th October 2016
Next Review Date	March 2019
Responsibility for Review	CCG's Information Governance Team
Audience	All NHS West Essex CCG officers and staff (which includes temporary staff, contractors and seconded staff).

Contents

1. Introduction

In order to ensure that the information held by CCGs is at a minimum risk of being compromised, the CCG will need to continue to build upon the strong foundations previously embedded by the CSU with regards to implementing effective, overarching, Information Governance Frameworks. All staff should be mindful that risk management responsibilities are not the sole responsibility of IT or Information Governance staff. All employees have an important role to play in order to ensure that risks are minimised and when encountered appropriately managed. It is important to remember that risk management is not about apportioning blame, but about promoting a fair and responsible culture, which contributes to learning and improvements when mistakes may occur.

This policy contains details about the organisational responsibilities to manage risks and the processes that are used.

2. Purpose

The Information Risk Policy has been created to:

- Protect the CCG, its staff (and Governing Body members) and its patients from information risks where the likelihood of occurrence and the consequences are significant;
- Provide a consistent risk management framework in which information risks will be fully considered and addressed during key approval, review and control processes;
- Encourage a pro-active approach to managing risks, rather than a re-active risk management method;
- Provide structure, transparency and assistance to improve the quality of decision making throughout the Group;
- Meet all legal or statutory requirements; and
- Assist in adequately safeguarding the CCG's information assets.

3. Scope

This policy is applicable to all areas of the CCG and its staff inclusive of contractors and staff that may be provided through external agencies. The necessity of full adherence will be detailed and included within all contracts and for outsourced or shared services. There are no exclusions.

4. Definitions and terms

Key definitions are:

- **Risk:** The chance of something happening, which will have an impact upon objectives. It is measured in terms of *consequence* and *likelihood*.
- **Consequence:** The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

- **Likelihood:** A qualitative description or synonym for probability or frequency.
- **Risk Assessment:** The overall process of risk analysis and risk evaluation.
- **Risk Management:** The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.
- **Risk Treatment:** Selection and implementation of appropriate options for dealing with risk. Conceptually, treatment options will involve one or a combination of the following five strategies:
    - Avoid the risk
    - Reduce the likelihood of occurrence
    - Reduce the consequences of occurrence
    - Transfer the risk
    - Retain/accept the risk
- **Risk Management Process:** The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.

Annual Governance Statement: High quality and proportionate internal control systems will help organisations achieve their aims. The Annual Governance Statement is a public accountability document that describes the effectiveness of internal controls in an organisation and is personally signed by the Accounting Officer.

5. Roles and Responsibilities

Accountable Officers for West Essex CCG

The Chief Officer (CO), as the Accountable Officer, has overall responsibility for information governance within the CCG. The CO is responsible for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery and continuity and will provide assurance, through the Annual Governance Statement, that all risks to the organisation, including those relating to information, are effectively managed and mitigated.

The CO has delegated operational responsibility for information governance to the Director of Finance, Contracting and Performance.

Senior Information Risk Owner (SIRO) for West Essex CCG

The role of Senior Information Risk Owner (SIRO) in the CCG has been assigned to the Director of Finance, Contracting and Performance. The SIRO takes ownership of the organisation's information risks policy and acts as advocate for information risk on the CCG Governing Body and Audit Committee. This includes oversight of information security incident reporting and response arrangements.

The SIRO will act as an advocate for information risk on the CCG Board and during internal discussions, and will provide written advice to the Accountable Officer on the content of the annual Governance Statement in regard to information risk.

The SIRO is responsible for the 'on-going' development and day-to-day management of the CCG's Risk Management Program for information privacy and security.

Summary of SIRO key responsibilities are to:

- oversee the development of an Information Risk Policy and a Strategy for implementing the policy within the existing information governance framework;
- take ownership of the risk assessment process for information risk, including review of an annual information risk assessment to support and inform the Annual Governance Statement;
- review and agree action in respect of identified information risks;
- ensure that the organisation's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff, including the board;
- provide a focal point for the resolution and / or discussion of information risk issues;
- ensure the Board is adequately briefed on information risk issues

Caldicott Guardian for West Essex CCG

The Caldicott Guardian has particular responsibilities for protecting the confidentiality of patients / service users information and enabling appropriate information sharing. For the CCG, this is an executive Chief Medical Officer. Acting as the 'conscience' of the organisation, the Caldicott Guardian will actively support work to enable information sharing where it is appropriate to share and will advise on options for lawful and ethical processing of information.

All Staff

The majority of staff handle information in one form or another. Staff that in the course of their work create, use or otherwise process information have a duty to keep up to date with and adhere to, relevant legislation, case law and national guidance.

The CCG policies and procedures will reflect such guidance and compliance with these polices and will ensure a high standard of Information Governance compliance within the organisation. All staff and officers, whether permanent, temporary, contracted or contractors are responsible for ensuring that they are aware of their responsibilities in respect of Information Governance.

Information Asset Owners (IAOs)

CCG Information Asset Owners (IAOs) shall ensure that information risk assessments are performed at least once annually or as required on all information assets where they

have been assigned ‘ownership’, following guidance from the SIRO on assessment method, format, content, and frequency. IAOs shall submit the risk assessment results and associated mitigation plans to the SIRO for review, along with details of any assumptions or external dependencies. Mitigation plans shall include specific actions with expected completion dates, as well as an account of residual risks.

Information Asset Administrators (IAAs)

Information Asset Owners can appoint Information Asset Administrators (IAAs) to support in the delivery of their information risk management responsibilities. Information Asset Administrators ensure that policies and procedures are followed, recognise actual or potential security incidents and take steps to mitigate those risks, consult with their Information Asset Owner on incident management and ensure that information asset registers are accurate and up to date.

6. Information Risk

The CCG Board has approved the introduction and embedding of information risk management into the key controls and approval processes of all major business processes and functions of the CCG. This decision reflects the high level of importance placed upon minimising information risk and safeguarding the interests of patients, staff and the CCG itself.

Information risk is inherent in all administrative and business activities and everyone working for, or on behalf of the CCG must effectively manage information risks for which they are responsible. The Board recognises that the aim of information risk management is not to eliminate risk, but rather to provide a structured approach to accurately identify, prioritise and manage the risks involved in all CCG related activities. It requires a balance between the cost of managing and treating information risks with the anticipated benefits that will be derived.

The CCG acknowledges that information risk management is an essential element of broader information governance and is an integral part of good management practice. The intent is to embed information risk management in a practical and achievable way into business processes and functions, so that there is a clear, structured process that staff can easily follow. This is achieved through key approval and the frequent review of processes and controls. Risk management should not be considered as a burdensome extra requirement for the organisation to undertake, but effectively integrated as a matter of routine in working towards achieving best practice management standards.

The principal objectives of the risk management function are, therefore:

- To assist with the identification of all reasonably foreseeable risks, particularly which may have potentially adverse effects on the quality of care, confidentiality of patient information, safety of patients, staff and visitors (risk identification)
- To assist and support in the assessment of risks in terms of likelihood and severity (risk assessment)
- To ensure risk ratings are applied to identified risks (risk quantification)
- To identify the appropriate level of management to be responsible for the risk (risk owner)
- To take positive action to eliminate or reduce risks to as low as is reasonably practicable , and continually review these actions (risk treatment)
- To keep the IG Steering Group / Governing Body and Senior Management appraised of the significant risks present across the CCG (principally via the risk register and risk reports)
- To create an escalation and accountability framework to help ensure satisfactory risk mitigation processes and risk owners are encouraged and supported in their task.

7. Information Asset Registers

The CCG will establish a program to ensure that their Information Assets (IAs) are identified and assigned to an IAO. The SIRO will oversee a review of the organisation's asset register to ensure it is kept up to date, complete and robust.

All critical IAs will be identified and included within the Information Asset Register (IAR), together with details of business criticality, the IAO, the Information Asset Administrator (IAA) and risk reviews to be carried out. In order to improve the usability and maintainability, the Information Asset register may be organised by service, rather than by location.

8. Audit and monitoring compliance

The CCG will use a variety of methods to monitor compliance with the processes in this policy, including as a minimum the following method/s:

IG Incidents

Information Governance compliance will be monitored quarterly through the monitoring of reported IG incidents by the IG Steering Group.

The IG Steering Group has responsibility for providing assurances that this policy is adequate for providing clear guidance in the event of significant changes which may affect it. The IG Lead will ensure that adequate arrangements exist for:

- Reporting incidents and Caldicott issues.
- Analysing and upward reporting of incidents and adverse events.

- Reporting IG work programs and progress reports.
- Reporting Information Governance Toolkit (IGT) assessments and improvement plans.
- Communicating IG developments.

In addition to the monitoring arrangements described above the CCG may undertake additional monitoring of this framework as a response to the identification of any gaps, or as a result of the identification of risks arising from the framework prompted by incident review, external reviews or other sources of information and advice.

9. Dissemination and implementation

The policy will be published on the organisation's internet/intranet. Managers are required to ensure that their staff understand its application to their practice. Awareness of any new content or change in process will be through electronic channels for example through e-mail, in bulletins and so on.

Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the SIRO.

10. Training

All staff likely to be in post 3 months or longer (permanent, temporary, contracted or seconded) are required to complete the online mandatory IG training modules (https://www.igtt.hscic.gov.uk/igte/index.cfm) within one month of joining, with further training required for managers / team leaders, staff who process personal information, and staff with specific information roles. A Training Needs Analysis (TNA) has been developed for staff in key roles, as part of effective delivery of training program.

However, should staff have access to personal identifiable information, training should be completed within 1 week, regardless of intended service length.

11. Related documents

The following documentation relates to the management of information and together underpins the CCG's Information Governance Assurance Framework. This policy should be read in conjunction with other policies:

Information Governance Policy
Data Protection & Confidentiality Policy
IM&T Security Policy
Acceptable Use of Electronic Communications Policy

Forensic Readiness Policy
Privacy Impact Assessment Policy
Safehaven Policy
Access to Information Policy

Related Acts

Data Protection Act 1998

12. Equality and Diversity

The CCG recognises the diversity of the local community and those in its employment. The CCG aims to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need. This document has been assessed for equality impact on the protected groups, as set out in the Equality Act 2010.

This Policy is applicable to every member of staff within the CCG irrespective of their age, disability, sex, gender reassignment, pregnancy or maternity status, race (which includes colour, nationality and ethnic or national origins), sexual orientation, religion or belief, marriage or civil partnership.

13. Key Contacts

Within the CCG

Senior Information Risk Owner	Director of Finance, Contracting and Performance
Caldicott Guardian	Chief Medical Officer
CCG IG Champion	Governance and Risk Manager

Information Governance Team

Jane Marley	Head of Information Governance	jane.marley@nhs.net
Tracey van Wyk	IG Lead	tracey.vanwyk@nhs.net
Ian Gear	FOI Lead	iain.gear@nhs.net
Debbie Smith-Shaw	Information Governance Adviser	debbie.smith-shaw@nhs.net

APPENDIX 1

RISK ASSESSMENT GUIDANCE AND FORMS

1. Identify the Risks

The information risks are identified as follows:

- Identify the assets, and the owners of these assets;
- Identify the threats to those assets.
- Identify the vulnerabilities that might be exploited by the threats.
- Identify the value / impacts that losses of confidentiality, integrity and availability may have on the assets.

2. Analyse and Evaluate the Risks

- Assess the business impacts upon the organisation that might result from security failures, taking into account the consequences of a loss of confidentiality, integrity or availability of the assets.
- Assess the realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented.
- Estimate the levels of risks.
- Determine whether the risks are acceptable or require additional treatment.

3. Identify and evaluate options for the treatment of risks

Possible options / actions to consider include:

- applying appropriate controls;
- knowingly and objectively accepting risks, providing they clearly satisfy the organisations policies and the criteria for accepting risk;
- avoiding risks
- transferring the associated business risks to other parties, for example insurers, suppliers.

4. Select Control Objectives and Controls for the treatment of risks

A control objective sets out what is trying to be achieved by implementing a series of related / associated controls measures. For example:

A.5.1	***Information security policy***			
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.				
			Selected	Risk Reduction
A.5.1.1	Information security policy document	*Control* An information security policy document shall be approved by management, and published and communicated to all employees and relevant external third parties		
A.5.1.2	Review of the information security policy	*Control* The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.		

This is the objective – What will be achieved by having an Information Security Policy

These are the related actions to be taken to achieve the objective

Control objectives and controls shall be selected and implemented to meet the requirements identified by the risk assessment and risk treatment process. This selection shall take account of the criteria for accepting risks as well as legal, regulatory and contractual requirements.

The control objectives and controls from Section 12 shall be selected as part of this process as suitable to cover the identified requirements. The list provided is not meant to be exhaustive and additional control objectives and controls may also be selected.

NOTE: The table provided in Section 12 contains a comprehensive list of control objectives and controls that have been found to be commonly relevant in organisations.

5. Criteria for Acceptable Risk

A level of risk does not necessarily have to be at its lowest residual level to be acceptable to the organisation. In determining what an acceptable risk is the following should be considered:

- Have sufficient control objectives and controls been selected in order to minimise the impact of the risk on the organisation (see Section 11 for control objectives and controls);
- Have the control objectives and controls been implemented fully?
- Has risk avoidance or transfer been considered?
- Where an unacceptable risk has been identified, is there a robust plan in place to monitor and report that risk, thereby making the risk acceptable?
- Has the organisation fulfilled its legal, statutory, regulatory or contractual obligations.

6. Catalogue of Threats

The Catalogue of Threats contains a list of different threats that could impact upon the availability, confidentiality and integrity of the Key Information Assets.

Ref.	Threat	Likelihood	Severity	VALUE	Ref.	Threat	Likelihood	Severity	VALUE
1.1	Airborne particles/dust	M	H	M	1.2	Maintenance error	M	H	M
1.2	Air conditioning failure	M	VH	H	1.2	Malicious software (for example, Viruses, worms, Trojan horses)	H	H	H
1.3	Bomb Attack	L	VH	M	1.3	Masquerading of user identity	M	H	M
1.4	Communications infiltration	M	VH	H	1.3	Misrouting or rerouting of messages	M	H	M
1.5	Damage to communication lines/cables	L	H	L	1.3	Misuse of resources	M	VH	H
1.6	Deterioration of storage media	L	VH	M	1.3	Network access by unauthorised persons	M	VH	H
1.7	Earthquake	L	H	L	1.3	Operational support staff error	M	H	M
1.8	Eavesdropping	M	H	M	1.3	Power fluctuation	M	H	M

1.9	Environmental contamination (and other forms of natural or man-made disasters)	L	H	L	1.3	Repudiation (for example, of services, transactions, sending/receiving messages)	M	H	M
1.1	Extremes of temperature and humidity	M	M	L	1.3	Software failure	M	VH	H
1.1	Failure of communications services	M	H	M	1.3	Staff shortage	M	H	M
1.1	Failure of network components	M	H	M	1.3	Theft	M	H	M
1.1	Failure of power supply	L	VH	M	1.4	Traffic overloading	M	H	M
1.1	Failure of water supply	L	M	VL	1.4	Transmission errors	M	M	L
1.2	Fire	M	VH	H	1.4	Unauthorised use of software	M	H	M
1.2	Flooding	L	H	L	1.4	Unauthorised use of storage media	M	M	L
1.2	Hardware failure	M	H	M	1.4	Use of network facilities in an unauthorised way	M	H	M
1.2	Hurricane	L	H	L	1.4	Use of software by unauthorised users	M	H	M
1.2	Illegal import/export of software	H	H	H	1.4	Use of software in an unauthorised way	M	H	M
1.2	Illegal use of software	H	H	H	1.4	User error	M	M	L
1.2	Industrial action	M	H	M	1.4	Willful damage	M	H	M
1.2	Lightning	M	H	M					

7. Catalogue of Vulnerabilities

The catalogue of vulnerabilities identifies how each of the identified threats to the organisations key assets might be exploited.

Ref	Vulnerability	VALUE	Ref	Vulnerability	VALUE
2.1	Absence of personnel	M	2.2	Dial up lines	H
2.2	Unsupervised work by outside or cleaning staff	M	2.2	Unprotected sensitive traffic	M
2.3	Insufficient security training	L	2.3	Single point of failure	M
2.4	Lack of security awareness	L	2.3	Inadequate network management	H

2.5	Poorly documented software	M	2.3	Lack of care at disposal	M
2.6	Lack of monitoring mechanisms	H	2.3	Uncontrolled copying	M
2.7	Lack of policies for the correct use of telecommunications media and messaging	H	2.3	Unprotected public network connections	H
2.8	Inadequate recruitment procedures	M	2.3	Complicated user interface	H
2.9	Inadequate or careless use of physical access control to buildings, rooms and offices	M	2.3	Disposal or reuse of storage media without proper erasure	H
2.1	Lack of physical protection for the building, doors and windows	M	2.3	Lack of audit trail	M
2.1	Location in an area susceptible to flood	H	2.3	Lack of documentation	H
2.1	Unprotected storage	M	2.3	Lack of effective change control	M
2.1	Insufficient maintenance/faulty installation of storage media	M	2.4	Lack of identification and authentication mechanisms	VH
2.1	Lack of periodic equipment replacement schemes	M	2.4	No 'logout' when leaving the work station	M
2.2	Susceptibility of equipment to humidity, dust, soiling	L	2.4	No or insufficient software testing	L
2.2	Susceptibility of equipment to temperature variations	M	2.4	Poor password management (easily guessable passwords, storing of passwords, insufficient frequency of change)	H
2.2	Susceptibility of equipment to voltage variations	L	2.4	Unclear or incomplete specification for developers	M
2.2	Unstable power grid	M	2.4	Uncontrolled downloading and using software	VH
2.2	Unprotected communication lines	M	2.4	Unprotected password tables	M
2.2	Poor joint cabling	L	2.4	Well known flaws in the software	L
2.2	Lack of identification and authentication mechanisms	H	2.4	Wrong allocation of access rights	H
2.2	Lack of proof of sending or receiving messages	M	2.4	Insufficient or irregular water supply	M

8. Controlling and Reducing the Risks

The following table indicates a number of control objectives and controls that may be selected by the CCG in order to mitigate a risk. Controls can reduce the assessed risks in the following ways:

- Avoid the risk **(A)**
- Transfer the risk **(T)**
- Reduce the threat **(R)**
- Reduce the vulnerabilities **(V)**
- Reduce the possible impacts **(I)**
- Detect unwanted events, react and recover from them **(D)**

As well as identifying the controls and their objective, the table also shows whether the CCG has adopted that control and in what way it mitigates the risks. The controls shown are taken from BS ISO/IEC 27001:2005 and are aligned with and derived from those listed in ISO/IEC 17799:2005 Clauses 5 to 15.

A.5 Security Policy				
A.5.1 Information security policy *Objective:* To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.				
			Selected	Risk Reduction
A.5.1.1	Information security policy document	*Control* An information security policy document shall be approved by management, and published and communicated to all employees and relevant external third parties		
A.5.1.2	Review of the information security policy	*Control* The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.		
A.6 Organisation of information security				
A.6. 1 Internal organisation *Objective:* To manage information security within the organisation				

A.6.1 .1	Management commitment to information security	*Control* Management shall actively support security within the organisation through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.		
A.6.1.2	Information security co-ordination	*Control* Information security activities shall be coordinated by representatives from different parts of the organisation with relevant roles and job functions.		
A.6.1 .3	Allocation of information security responsibilities	*Control* All information security responsibilities shall be clearly defined.		
A.6.1.4	Authorisation process for information processing facilities	*Control* A management authorization process for new information processing facilities shall be defined and implemented.		
A.6.1.5	Confidentiality agreements	*Control* Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified and regularly reviewed.		
A.6.1.6	Contact with authorities	*Control* Appropriate contacts with relevant authorities shall be maintained.		
A.6. 1.7	Contact with special interest groups	*Control* Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.		
A.6.1.8	Independent	*Control* The organisation's approach to managing		

	review of information security	information security and its implementation (for instance, control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur.		
A. 6.2 External parties *Objective:* To maintain the security of the organisation's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.				
A.6.2.1	Identification of risks related to external parties	*Control* The risks to the organisation's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.		
A.6.2.2	Addressing security when dealing with customers	*Control* All identified security requirements shall be addressed before giving customers access to the organisation's information or assets.		
A.6.2.3	Addressing security in third party agreements	*Control* Agreements with third parties involving accessing, processing, communicating or managing the organisation's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.		
A.7 Asset management				
A.7. 1 Responsibility for assets *Objective:* To achieve and maintain appropriate protection of organisational assets.				
A.7.1.1	Inventory of assets	*Control* All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.		
A.7.1.2	Ownership of assets	*Control*		

		All information and assets associated with information processing facilities shall be 'owned' [1] by a designated part of the organisation.		
A.7. 1.3	Acceptable use of assets	*Control* Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.		
A.7.2 Information classification *Objective:* To ensure that information receives an appropriate level of protection.				
A.7.2.1	Classification guidelines	*Control* Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organisation.		
A.7.2.2	Information labeling and handling	*Control* An appropriate set of procedures for information labeling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organisation.		
A.8 Human resources security				
A.8. 1 Prior to employment [2] *Objective:* To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.				
A.8.1 .1	Roles and responsibilities	*Control* Security roles and responsibilities of employees, contractors and third party users shall be defined		

[1] The term 'owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term 'owner' does not mean that the person actually has property rights to the asset.

[2] The word 'employment' is meant here to cover all of the following different situations: employment of people (temporary or longer lasting), appointment of job roles, changing of job roles, assignment of contracts, and the termination of any of these arrangements

		and documented in accordance with the organisation's information security policy.		
A.8.1.2	Screening	*Control* Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.		
A.8.1 .3	Terms and conditions of employment	*Control* As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organisation's responsibilities for information security.		
A.8.2 During employment *Objective:* To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organisational security policy in the course of their normal work, and to reduce the risk of human error.				
A.8.2.1	Management responsibilities	*Control* Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organisation.		
A.8.2.2	Information security awareness, education and training	*Control* All employees of the organisation and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function.		
A.8.2.3	Disciplinary process	*Control* There shall be a formal disciplinary process for employees who have committed a security breach.		

A.8.3 Termination or change of employment *Objective:* To ensure that employees, contractors and third party users exit an organisation or change employment in an orderly manner.				
A.8.3.1	Termination responsibilities	*Control* Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.		
A.8.3.2	Return of assets	*Control* All employees, contractors and third party users shall return all of the organisation's assets in their possession upon termination of their employment, contract or agreement.		
A.8.3.3	Removal of access rights	*Control* The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.		
A.9 Physical and environmental security				
A. 9.1 Secure areas *Objective:* To prevent unauthorised physical access, damage and interference to the organisation's premises and information.				
A.9.1.1	Physical security perimeter	*Control* Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.		
A.9.1.2	Physical entry controls	*Control* Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.		

A.9. 1.3	Securing offices, rooms and facilities	*Control* Physical security for offices, rooms, and facilities shall be designed and applied.		
A.9.1.4	Protecting against external and environmental threats	*Control* Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied.		
A.9.1.5	Working in secure areas	*Control* Physical protection and guidelines for working in secure areas shall be designed and applied.		
A.9.1 .6	Public access, delivery and loading areas	*Control* Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.		
A.9.2 Equipment security *Objective:* To prevent loss, damage, theft or compromise of assets and interruption to the organisation's activities.				
A.9.2.1	Equipment siting and protection	*Control* Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.		
A.9.2.2	Supporting utilities	*Control* Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.		
A.9.2.3	Cabling security	*Control* Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.		

A.9.2.4	Equipment maintenance	*Control* Equipment shall be correctly maintained to ensure its continued availability and integrity.		
A.9.2.5	Security of equipment off-premises	*Control* Security shall be applied to off-site equipment taking into account the different risks of working outside the organisation's premises.		
A.9.2.6	Secure disposal or re-use of equipment	*Control* All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.		
A.9.2.7	Removal of property	*Control* Equipment, information or software shall not be taken off-site without prior authorization.		
A.10 Communications and operations management				
A. 10.1 Operational procedures and responsibilities *Objective:* To ensure the correct and secure operation of information processing facilities.				
A.10.1.1	Documented operating procedures	*Control* Operating procedures shall be documented, maintained, and made available to all users who need them.		
A.10.1.2	Change management	*Control* Changes to information processing facilities and systems shall be controlled.		
A.10.1.3	Segregation of duties	*Control* Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organisation's assets.		

A.10.1.4	Separation of development, test and operational facilities	*Control* Development, test and operational facilities shall be separated to reduce the risks of unauthorised access or changes to the operational system.		
A. 10.2 Third party service delivery management *Objective:* To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.				
A.10.2.1	Service delivery	*Control* It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.		
A.10.2.2	Monitoring and review of third party services	*Control* The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.		
A.10.2.3	Managing changes to third party services	*Control* Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.		
A. 10.3 System planning and acceptance *Objective:* To minimize the risk of systems failures.				
A.10.3.1	Capacity management	*Control* The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.		
A.10.3.2	System acceptance	*Control* Acceptance criteria for new information systems,		

		upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.		
A.10.4 Protection against malicious and mobile code *Objective:* To protect the integrity of software and information.				
A.10.4.1	Controls against malicious code	*Control* Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.		
A.10.4.2	Controls against mobile code	*Control* Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing.		
A10.5 Back up *Objective:* To maintain the integrity and availability of information and information processing facilities.				
A.10.5.1	Information back-up	*Control* Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.		
A. 10.6 Network security management *Objective:* To ensure the protection of information in networks and the protection of the supporting infrastructure				
A.10.6.1	Network controls	*Control* Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.		

A.10.6.2	Security of network services	*Control* Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.		
A.10.7 Media handling *Objective:* To prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities.				
A.10.7.1	Management of removable media	*Control* There shall be procedures in place for the management of removable media.		
A.10.7.2	Disposal of media	*Control* Media shall be disposed of securely and safely when no longer required, using formal procedures.		
A.10.7.3	Information handling procedures	*Control* Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.		
A.10.7.4	Security of system documentation	*Control* System documentation shall be protected against unauthorised access.		
A. 10.8 Exchange of information *Objective:* To maintain the security of information and software exchanged within an organisation and with any external entity.				
A.10.8.1	Information exchange	*Control* Formal exchange policies, procedures, and controls		

	policies and procedures	shall be in place to protect the exchange of information through the use of all types of communication facilities.		
A.10.8.2	Exchange agreements	*Control* Agreements shall be established for the exchange of information and software between the organisation and external parties.		
A.10.8.3	Physical media in transit	*Control* Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organisation's physical boundaries.		
A.10.8.4	Electronic messaging	*Control* Information involved in electronic messaging shall be appropriately protected.		
A.10.8.5	Business information systems	*Control* Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.		
A.10.9 Electronic commerce services *Objective:* To ensure the security of electronic commerce services, and their secure use.				
A.10.9.1	Electronic commerce	*Control* Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.		
A.10.9.2	On-line transactions	*Control* Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message		

		duplication or replay.		
A.10.9.3	Publicly available information	*Control* The integrity of information being made available on a publicly available system shall be protected to prevent unauthorised modification.		
A. 10.10 Monitoring *Objective:* To detect unauthorised information processing activities.				
A.10.10.1	Audit logging	*Control* Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.		
A.10.10.2	Monitoring system use	*Control* Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.		
A.10.10.3	Protection of log information	*Control* Logging facilities and log information shall be protected against tampering and unauthorized access.		
A.10.10.4	Administrator and operator logs	*Control* System administrator and system operator activities shall be logged.		
A.10.10.5	Fault logging	*Control* Faults shall be logged, analyzed and appropriate action taken.		
A.10.10.6	Clock synchronization	*Control* The clocks of all relevant information processing systems within an organisation or security domain shall be synchronized with an agreed		

		accurate time source.		
A.1 1 Access control				
A.11.1 Business requirement for access control *Objective:* To control access to information				
A.11.1.1	Access control policy	*Control* An access control policy shall be established, documented, and reviewed based on business and security requirements for access.		
A. 11.2 User access management *Objective:* To ensure authorized user access and to prevent unauthorized access to information systems.				
A.1 1.2.1	User registration	*Control* There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.		
A.11.2.2	Privilege management	*Control* The allocation and use of privileges shall be restricted and controlled.		
A.11.2.3	User password management	*Control* The allocation of passwords shall be controlled through a formal management process.		
A.11.2.4	Review of user access rights	*Control* Management shall review users' access rights at regular intervals using a formal process.		
A.11.3 User responsibilities *Objective:* To prevent unauthorized user access, and compromise or theft of information and information processing facilities.				
A.11.3.1	Password use	*Control* Users shall be required to follow good security practices in the selection and use of		

		passwords.		
A.1 1.3.2	Unattended user equipment	*Control* Users shall ensure that unattended equipment has appropriate protection.		
A.1 1.3.3	Clear desk and clear screen policy	*Control* A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.		
A. 11.4 Network access control *Objective:* To prevent unauthorized access to networked services.				
A.1 1.4.1	Policy on use of network services	*Control* Users shall only be provided with access to the services that they have been specifically authorized to use.		
A.1 1.4.2	User authentication for external connections	*Control* Appropriate authentication methods shall be used to control access by remote users.		
A.1 1.4.3	Equipment identification in networks	*Control* Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.		
A.1 1.4.4	Remote diagnostic and configuration port protection	*Control* Physical and logical access to diagnostic and configuration ports shall be controlled.		
A.11.4.5	Segregation in networks	*Control* Groups of information services, users, and information systems shall be segregated on networks.		

A.1 1.4.6	Network connection control	*Control* For shared networks, especially those extending across the organisation's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications (see 11.1).		
A.1 1.4.7	Network routing control	*Control* Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.		
A. 11.5 Operating system access control *Objective:* To prevent unauthorised access to operating systems				
A.11.5.1	Secure log-on procedures	*Control* Access to operating systems shall be controlled by a secure log on procedure.		
A.1 1.5.2	User identification and authentication	*Control* All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.		
A.1 1.5.3	Password management system	*Control* Systems for managing passwords shall be interactive and shall ensure quality passwords.		
A.1 1.5.4	Use of system utilities	Control The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.		
A.11.5.5	Session time out	*Control* Inactive sessions shall shut down after a defined period of inactivity.		

A.11.5.6	Limitation of connection time	*Control* Restrictions on connection times shall be used to provide additional security for high risk applications.		
A. 11.6 Application and information access control *Objective:* To prevent unauthorized access to information held in application systems.				
A.1 1.6.1	Information access restriction	*Control* Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.		
A.11.6.2	Sensitive system isolation	*Control* Sensitive systems shall have a dedicated (isolated) computing environment.		
A.11.7 Mobile computing and teleworking *Objective:* To ensure information security when using mobile computing and teleworking facilities.				
A.1 1.7.1	Mobile computing and communications	*Control* A formal policy shall be in place and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.		
A.11.7.2	Teleworking	*Control* A policy, operational plans and procedures shall be developed and implemented for teleworking activities.		
A.12 Information systems acquisition, development and maintenance				
A. 12.1 Security requirements of information systems *Objective:* To ensure that security is an integral part of information systems.				

A.12.1.1	Security requirements analysis and specification	*Control* Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.		
A. 12.2 Correct processing in applications *Objective:* To prevent errors, loss, unauthorized modification or misuse of information in applications				
A.12.2.1	Input data validation	*Control* Data input to applications shall be validated to ensure that this data is correct and appropriate.		
A.12.2.2	Control of internal processing	*Control* Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.		
A.12.2.3	Message integrity	*Control* Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.		
A.12.2.4	Output data validation	*Control* Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.		
A. 12.3 Cryptographic controls *Objective:* To protect the confidentiality, authenticity or integrity of information by cryptographic means.				
A.12.3.1	Policy on the use of cryptographic controls	*Control* A policy on the use of cryptographic controls for protection of information shall be developed and implemented.		

A.12.3.2	Key management	*Control* Key management shall be in place to support the organisation's use of cryptographic techniques.		
A. 12.4 Security of system files *Objective:* To ensure the security of system files.				
A.12.4.1	Control of operational software	*Control* There shall be procedures in place to control the installation of software on operational systems.		
A.12.4.2	Protection of system test data	*Control* Test data shall be selected carefully, and protected and controlled.		
A.12.4.3	Access control to program source code	*Control* Access to program source code shall be restricted.		
A. 12.5 Security in development and support processes *Objective:* To maintain the security of application system software and information.				
A.12.5.1	Change control procedures	*Control* The implementation of changes shall be controlled by the use of formal change control procedures.		
A.12.5.2	Technical review of applications after operating system changes	*Control* When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organisational operations or security.		
A.12.5.3	Restrictions on changes to	*Control* Modifications to software packages shall be discouraged, limited to necessary changes, and all		

	software packages	changes shall be strictly controlled.		
A.12.5.4	Information leakage	*Control* Opportunities for information leakage shall be prevented.		
A.12.5.5	Outsourced software development	*Control* Outsourced software development shall be supervised and monitored by the organisation.		
A. 12.6 Technical Vulnerability Management *Objective:* To reduce risks resulting from exploitation of published technical vulnerabilities.				
A.12.6.1	Control of technical vulnerabilities	*Control* Timely information about technical vulnerabilities of information systems being used shall be obtained, the organisation's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.		
A.13 Information security incident management				
A. 13.1 Reporting information security events and weaknesses *Objective:* To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.				
A.13.1.1	Reporting information security events	*Control* Information security events shall be reported through appropriate management channels as quickly as possible.		
A.13.1 .2	Reporting security weaknesses	*Control* All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.		
A.13.2 Management of information security incidents and improvements				

Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.				
A.13.2.1	Responsibilities and procedures	*Control* Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.		
A.13.2.2	Learning from information security incidents	*Control* There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.		
A.13.2.3	Collection of evidence	*Control* Where a follow-up action against a person or organisation after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).		
A.14 Business continuity management				
A. 14.1 Information security aspects of business continuity management *Objective:* To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.				
A.14.1.1	Including information security in the business continuity management process	*Control* A managed process shall be developed and maintained for business continuity throughout the organisation that addresses the information security requirements needed for the organisation's business continuity.		
A.14.1.2	Business continuity and risk assessment	*Control* Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and		

		their consequences for information security.		
A.14.1.3	Developing and implementing continuity plans including information security	*Control* Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.		
A.14.1.4	Business continuity planning framework	*Control* A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.		
A.14.1.5	Testing, maintaining and reassessing business continuity plans	*Control* Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.		
A.15 Compliance				
A. 15.1 Compliance with legal requirements *Objective:* To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.				
A.15.1 .1	Identification of applicable legislation	*Control* All relevant statutory, regulatory and contractual requirements and the organisation's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organisation.		
A.15.1.2	Intellectual property rights (IPR)	*Control* Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.		

A.15.1 .3	Protection of organisational records	*Control* Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.		
A.15.1.4	Data protection and privacy of personal information	*Control* Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.		
A.15.1.5	Prevention of misuse of information processing facilities	*Control* Users shall be deterred from using information processing facilities for unauthorized purposes.		
A.15.1 .6	Regulation of cryptographic controls	*Control* Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.		
A. 15.2 Compliance with security policies and standards, and technical compliance *Objective:* To ensure compliance of systems with organisational security policies and standards.				
A.15.2.1	Compliance with security policies and standards	*Control* Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.		
A.15.2.2	Technical compliance checking	*Control* Information systems shall be regularly checked for compliance with security implementation standards.		
A. 15.3 Information systems audit considerations *Objective:* To maximize the effectiveness of and to minimize interference to/from the information systems audit process.				
A.15.3.1	Information	*Control*		

	systems audit controls	Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.		
A.15.3.2	Protection of information systems audit tools	*Control* Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.		

9. Inventory of Major Assets

The following is a broad inventory of the major CCG assets. The table identifies the type of asset, its value to the organisation, which threat and vulnerabilities are applicable and what the resultant level of risk is to the organisation. This list is generic and assessors should review the catalogues' of threats and vulnerabilities

Asset	Value (VH,H,M,L)	Threats	Vulnerabilities	Measure of Risk
Paper Documents				
Training Materials	M	1.3, 1.7, 1.9, 1.10, 1.15, 1.16, 1.18, 1.22, 1.34, 1.43	2.2, 2.8,2.9, 2.10, 2.11, 2.12,2.28,	3
Personnel Files	VH	1.3, 1.7, 1.9, 1.10, 1.15, 1.16, 1.18, 1.22, 1.34, 1.43	2.2, 2.8,2.9, 2.10, 2.11, 2.12,2.28,	5
Contracts	H	1.3, 1.7, 1.9, 1.10, 1.15, 1.16, 1.18, 1.22, 1.34, 1.43	2.2, 2.8,2.9, 2.10, 2.11, 2.12,2.28,	4
Tax Returns	M	1.3, 1.7, 1.9 1.10, 1.15, 1.16, 1.18, 1.22, 1.34, 1.43	2.2, 2.8,2.9, 2.10, 2.11, 2.12,2.28,	3

Invoices and Utility bills	M	1.3, 1.7, 1.9, 1.10, 1.15, 1.16, 1.18, 1.22, 1.34, 1.43	2.2, 2.8,2.9, 2.10, 2.11, 2.12,2.28,	3
Correspondence	M	1.3, 1.7, 1.9, 1.10, 1.15, 1.16, 1.18, 1.22, 1.34, 1.43	2.2, 2.8,2.9, 2.10, 2.11, 2.12,2.28,	3
Bank Statements	L	1.3, 1.7, 1.9, 1.10, 1.15, 1.16, 1.18, 1.22, 1.34, 1.43	2.2, 2.8,2.9, 2.10, 2.11, 2.12,2.28,	2
Financial Statements	L	1.3, 1.7, 1.9, 1.10, 1.15, 1.16, 1.18, 1.22, 1.34, 1.43	2.2, 2.8,2.9, 2.10, 2.11, 2.12,2.28,	2
Emails	H	1.3, 1.7, 1.9, 1.10, 1.15, 1.16, 1.18, 1.22, 1.34, 1.43	2.2, 2.8,2.9, 2.10, 2.11, 2.12,2.28,	4
Asset	**Value (VH,H,M,L)**	**Threats**	**Vulnerabilities**	**Measure of Risk**
Physical Assets				
Desktop PCs	L	1.3, 1.7, 1.9, 1.13, 1.15, 1.16, 1.17, 1.20, 1.22, 1.24, 1.25, 1.27, 1.30, 1.34, 1.37, 1.41, 1.42, 1.43	2.2, 2.3, 2.4, 2.6, 2.10, 2.11, 2.15, 2.17, 2.18, 2.27,	2
Laptop PCs	L	1.3, 1.7,1.9, 1.13, 1.15, 1.16, 1.17, 1.20, 1.22, 1.24, 1.25, 1.27, 1.30, 1.34, 1.37, 1.41,	2.2, 2.3, 2.4, 2.6, 2.10, 2.11, 2.15, 2.17, 2.18, 2.27,	2

		1.42, 1.43		
Servers	M	1.1, 1.2, 1.3, 1.4, 1.6, 1.7, 1.9, 1.10, 1.11,1.12, 1.13, 1.15, 1.16, 1.17, 1.20, 1.21, 1.22, 1.23, 1.24, 1.25, 1.27, 1.29, 1.30, 1.32, 1.34, 1.37, 1.38, 1.40, 1.41, 1.42, 1.43	2.3, 2.4, 2.6, 2.8, 2.9, 2.10, 2.11, 2.14, 2.15, 2.16, 2.17, 2.18, 2.21, 2.29, 2.34, 2.35, 2.36, 2.38, 2.43	3
Printers	L	1.3, 1.7, 1.13, 1.15, 1.16, 1.17, 1.22, 1.23, 1.27, 1.30, 1.34, 1.43	2.2, 2.8, 2.9, 2.10, 2.11, 2.14, 2.15, 2.17, 2.18, 2.32,	2
Photocopiers	L	1.3, 1.7, 1.13, 1.15, 1.16, 1.17, 1.22, 1.23, 1.27, 1.30, 1.34, 1.43	2.2, 2.8, 2.9, 2.10, 2.11, 2.14, 2.15, 2.17, 2.18, 2.32,	2
Telephones	L	1.3, 1.7, 1.13, 1.15, 1.16, 1.17, 1.22, 1.23, 1.27, 1.30, 1.34, 1.43	2.2, 2.7, 2.8, 2.9, 2.10, 2.11, 2.18,	2

Asset	Value (VH,H,M,L)	Threats	Vulnerabilities	Measure of Risk
Fax Machines	L	1.3, 1.7, 1.13, 1.15, 1.16, 1.17, 1.22, 1.23, 1.27, 1.30, 1.34, 1.43	2.2, 2.7, 2.8, 2.9, 2.10, 2.11, 2.18,	2
Network Hubs and Routers	VH	1.1, 1.3, 1.4, 1.7, 1.9, 1.11, 1.12, 1.13, 1.15, 1.16, 1.17, 1.22, 1.23, 1.27, 1.28, 1.29,	2.3, 2.4, 2.6, 2.9, 2.10, 2.11, 2.12, 2.14, 2.15, 2.16, 2.17, 2.18, 2.25, 2.26, 2.34,	5
Backup Media	VH	1.3, 1.7, 1.13, 1.15, 1.16, 1.17, 1.22, 1.23, 1.27, 1.30, 1.34, 1.43	2.2, 2.3, 2.4, 2.6, 2.8, 2.9, 2.10, 2.11, 2.12, 2.13, 2.27, 2.28, 2.31,	5
Storage Cabinets	L	1.3, 1.7, 1.15, 1.16, 1.18, 1.22,	2.8, 2.9, 2.10, 2.11, 2.12,	2
General Office Equipment	L	1.3, 1.7, 1.15, 1.16, 1.18, 1.22,	2.8, 2.9, 2.10, 2.11, 2.12,	2
Logical Assets				

Applications software	L	1.3, 1.6, 1.13, 1.15, 1.16, 1.17, 1.19, 1.20, 1.24, 1.25, 1.27, 1.28	2.3, 2.4, 2.5, 2.6, 2.12, 2.32, 2.33, 2.34, 2.37, 2.39, 2.40, 2.42	2
Technical Software (for example Windows)	L	1.3, 1.6, 1.13, 1.15, 1.16, 1.17, 1.19, 1.20, 1.24, 1.25, 1.27, 1.28, 1.29, 1.32, 1.37, 1.38, 1.40, 1.41, 1.42, 1.43	2.3, 2.4, 2.5, 2.6, 2.12, 2.32, 2.33, 2.34, 2.37, 2.39, 2.40, 2.42	2

Asset	Value (VH,H,M,L)	Threats	Vulnerabilities	Measure of Risk
Electronic Data	VH	1.2, 1.3, 1.4, 1.9, 1.10, 1.6, 1.13, 1.15, 1.16, 1.17, 1.19, 1.20, 1.22, 1.23, 1.24, 1.25, 1.27, 1.28, 1.29, 1.30, 1.31, 1.32,	2.3, 2.4, 2.6, 2.8, 2.9, 2.10, 2.11, 2.12, 2.13, 2.14, 2.15, 2.16, 2.17, 2.18, 2.28, 2.35, 2.38,2.43	5
Networks	VH	1.2, 1.3, 1.4, 1.9, 1.10, 1.11, 1.12, 1.13, 1.15, 1.16, 1.17, 1.19, 1.20, 1.22, 1.23, 1.24, 1.25, 1.27, 1.28,	2.3, 2.4, 2.6, 2.8, 2.9, 2.10, 2.11, 2.12, 2.13, 2.14, 2.15, 2.16, 2.17, 2.18, 2.28, 2.35, 2.38,2.43	5
People				
	VH	1.1, 1.3, 1.7, 1.10, 1.14, 1.15, 1.16, 1.18, 1.21, 1.22, 1.27, 1.30, 1.33, 1.34, 1.43	2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.11	5

Services				
Telephone System	H	1.3, 1.5, 1.7, 1.8, 1.9, 1.11, 1.12, 1.13, 1.15, 1.16, 1.17, 1.22, 1.23, 1.27, 1.28, 1.30,	2.3, 2.4, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.12, 2.14, 2.15, 2.16, 2.17, 2.18	4

Asset	Value (VH,H,M,L)	Threats	Vulnerabilities	Measure of Risk
Heating/Air Conditioning	H	1.1, 1.2, 1.3, 1.7, 1.9, 1.10, 1.13, 1.14, 1.15, 1.16, 1.17, 1.18, 1.21,	2.3, 2.4, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.12, 2.14, 2.15, 2.16, 2.17,	4
Electrical Supply	VH	1.3, 1.7, 1.9, 1.13, 1.15, 1.16, 1.18, 1.22, 1.23, 1.30, 1.31, 1.42.	2.11, 2.17, 2.18, 2.25, 2.34	5
Smoke/Gas detectors	VH	1.1, 1.3, 1.5, 1.7, 1.9, 1.10, 1.13, 1.15, 1.18,1.22,	2.17, 2.18, 2.25, 2.34	5
UPSs	H	1.1, 1.3, 1.5, 1.7, 1.9, 1.10, 1.13, 1.15, 1.18,1.22,	2.3, 2.4, 2.6, 2.9 2.10, 2.11, 2.13, 2.14, 2.15, 2.16,	4
Water Supply	M	1.1, 1.3, 1.5, 1.7, 1.9, 1.10, 1.13, 1.14, 1.15, 1.16,	2.44	3
CCG Image and Reputation				

Reputation with Suppliers	M	1.3, 1.4, 1.7, 1.8, 1.9, 1.11, 1.12, 1.15, 1.18,1.22, 1.23, 1.25, 1.27,	2.1, 2.2, 2.3, 2.4, 2.6, 2.7, 2.8,2.11, 2.12, 2.18, 2.19, 2.24, 2.28, 2.30,	3
Reputation with Customers	VH	1.3, 1.4, 1.7, 1.8, 1.9, 1.11, 1.12, 1.15, 1.18,1.22, 1.23, 1.25, 1.27,	2.1, 2.2, 2.3, 2.4, 2.6, 2.7, 2.8,2.11, 2.12, 2.18, 2.19, 2.24, 2.28, 2.30,	5
Asset	**Value (VH,H,M,L)**	**Threats**	**Vulnerabilities**	**Measure of Risk**
Public confidence	VH	1.3, 1.4, 1.7, 1.8, 1.9, 1.11, 1.12, 1.15, 1.18,1.22, 1.23, 1.25, 1.27,	2.1, 2.2, 2.3, 2.4, 2.6, 2.7, 2.8,2.11, 2.12, 2.18, 2.19, 2.24, 2.28, 2.30,	5

10. Threat, Vulnerability & Asset Value Matrix

The matrix shown below has been used to determine the 'Measure of Risk' as detailed in section 9 of this assessment (Inventory of Major CCG Information Assets). The matrix is 3 dimensional taking into account Threats, Vulnerabilities and Asset Value resulting in an overall 'Measure of Risk' in the range 0 (no risk) to 9 (very high risk).

	Levels of Threat	**Very Low/Low**				**Medium**				**High**				**Very High**			
	Levels of Vulnerability	**L**	**M**	**H**	**VH**	**L**	**M**	**H**	**VH**	**L**	**M**	**H**	**VH**	**L**	**M**	**H**	**VH**
Asset Value	**VL/L**	0	1	2	3	1	2	3	4	2	3	4	5	3	4	5	6
	M	1	2	3	4	2	3	4	5	3	4	5	6	4	5	6	7
	H	2	3	4	5	3	4	5	6	4	5	6	7	5	6	7	8
	VH	3	4	5	6	4	5	6	7	5	6	7	8	6	7	8	9

11. Information Security Risk Summary Tables

Impact / Likelihood Analysis

This summary table is for recording the outcomes of the organisations Information Risk Assessment and may be used both corporately and departmentally. Each of the headings used relates to the Control Objectives and Controls detailed in Section 8, these being the nationally agreed areas of information risk set out in the British Standard. The record form is on pages 39 & 40.

Departmental Record

Once asset owners have completed their information risk assessments the record table is to be completed. For each of the main headings, any risks / gaps in assurance should be recorded along with proposed actions to resolve that issue, what the outcome control will be and what the objective of that control is. Pre and post action likelihoods should also be recorded

Corporate Record

Similarly, once all department summary records have been compiled the table can be used to summarise the position within the organisation, using the departmental outcomes to feed into the overall level of information risk within the CCG.

Unacceptable Residual Risk

The table below is to be used to record any unacceptable residual risks. The unacceptable risks will be subject to frequent review in order to determine whether the additional controls being implemented are having an effect upon the level of risk. Any improvement in likelihood (that is medium to low) may result in the risk becoming an acceptable risk (impact is deemed to remain unchanged).

Residual Risks	Likelihood	Impact	Further controls
Example: Assets that have not been classified correctly will receive an incorrect level of protection	*Medium*	*High*	*Introduce regular reviews and attempted unauthorised access trials*

Information Security Risk Summary Table – Impact / Likelihood Analysis

Risk	Impact	Pre-strategy likelihood	Strategy/Action to resolve	Control	Objective	Post Strategy Likelihood
Security Policy						
Example: The CCG does not have an Information Security Policy	*High*	*High*	*Develop policy, get approved, published and communicated*	*Information Security Policy*	*To demonstrate management commitment and set out the organisations approach to managing information security*	*Low*
Organisation of Information Security						
Asset Management						

Human Resources Security						
Physical & Environmental Security						
Communications & Operations Management						
Access Control						

Information systems acquisition, development & maintenance						
Management of Information Security Incidents & Improvements						
Business Continuity Management						
Compliance						

16. Completing an Assessment

This document provides the reader with the necessary information for completing an Information Asset Risk Assessment. However, it is acknowledged that this is not a normal or familiar approach to risk assessment.

The following flow diagram will provide you with the necessary steps, and how to use the information in this document. There is also a copy of the risk assessment form with guidance added in to complement the flow diagram.

First part of the form has been removed for ease of understanding, but must be completed as part of the assessment
Step 1;Description of the information asset: Please use description as per information asset register
Step 2: Please identify category of people affected: Staff / Patients / Visitors / Contractors / CCG (Indicate all that apply) Whose information does the asset hold, also consider if staff/patient details contained in asset would this also have impact on the CCG if lost / unavailable / stolen and so on. Number of people affected:
Step 3: Threats identified: See section 6 on page 15 of Information Risk Policy and identify all threats that could affect the asset, see also section 9 starting on page 33 for some of potentials threats for key assets (please note the list in section 12 is not exhaustive)
Step 4: Vulnerabilities Identified: See section 7 on page 16 of Information Risk Policy and identify all threats that could affect the asset, see also section 9 starting on page 33 for some potentials threats for key assets (please note the list in section 9 is not exhaustive)
Step 5: Asset Value: See sections 9 & 10 starting on page 33 for suggested value of key assets, however this is just a guide and asset values will differ depending on the value of the information to the organisation and the organisations ability to function without it, as well as the consequences of that information being lost/stolen and confidentiality breaches

Step 6: What precautions exist to control the risk: Are there any controls in place currently to avoid, transfer or reduce the risk. The controls listed in section 8 starting on page 17 are a guide of the types of control that could be in place Calculate the **Risk Rating** with existing controls in place: Are these arrangements satisfactory: Yes / No
Step 7: If No, What further control measures are required: Do any further controls need to be put in place to avoid, transfer or reduce the risk, again the controls listed in section 8 are a guide of the types of control that could be put in place Calculate the **Risk Rating** with recommended control measures: Approximate costing of introducing further controls: **£**_____ Expected completion date: _____
Signatures of Information Asset Administrator: Signature of Information Asset Owner: Risk Assessment Reviewed by Information Governance Steering Group on: Escalation of Risk to CCG Board: Yes/No

Information Asset Risk Assessment Flow Diagram

Step 1 – Description of Information Asset. Only use the description contained within the Asset Register.

If the asset is not on the register ask for it to be added.

Step 2: Please identify category of people affected this will be dependent upon the type of asset – whether it is a piece of hardware or a database / spreadsheet. Consider whose information the asset holds. You should also consider if staff / patient details are contained on/within the asset, would this also have impact on CCG if lost / unavailable / stolen and so on. You should select all that apply from the list provided.

Step 3: Threats identified: Refer to Section 6 on page 14 of this document and identify all threats that could affect the asset. You should also refer to Section 9 starting on page 38 for some generic listings of potentials threats for key assets (please note that neither list is exhaustive)

Step 4: Vulnerabilities Identified:

Refer to Section 7 on page 15 of this document and identify all vulnerabilities that could affect the asset. You should also refer to Section 9 starting on page 38 for some generic listings of potential vulnerabilities for key assets (please note that neither list is exhaustive)

Step 5: Asset Value: Refer to Sections 9 & 10 starting on pages 38 & 45 for suggested value of key assets, however this is just a guide and asset values will differ depending on the value of the information to the organisation and the organisations ability to function without it, as well as the consequences of that information being lost / stolen and confidentiality breaches

Step 6: What precautions exist to control the risk:

Are there any controls in place currently to avoid, transfer or reduce the risk. The controls listed in section 8 starting on page 16 are a guide of the types of control that could be in place

Calculate the **Risk Rating** with existing controls in place: You should refer to information in Section 9 starting on page 38 and the Matrix in Section 10 on page 45.

Step 7: If No, What further control measures are required:

Do any further controls need to be put in place to avoid, transfer or reduce the risk, again the controls listed in section 8 are a guide of the types of control that could be put in place

Calculate the **Risk Rating** with recommended control measures: Complete the second part of Step 6. Remember that Step 6 asks you to assess the risk for the existing control measures. You are now calculating the level of residual risk after your recommendations have been implemented.

Risk Assessment Form

Risk Register Number: ……..

(Allocated by Risk Manager, if applicable)

Directorate / Service: Dept / Other: Site: Address:	Assessment Date: Review Assessment Date: Name of Assessor: Signature of Assessor: ……..
Description of the information asset:	
Please identify category of people affected: Staff / Patients / Visitors / Contractors / CCG (Indicate all that apply) Number of people affected:	
Threats identified:	
Vulnerabilities Identified:	

Asset Value:
What controls exist to manage the risk: Calculate the **Risk Rating** with existing controls in place: Are these arrangements satisfactory: Yes / No
If No, What further control measures are required: Calculate the **Risk Rating** with recommended control measures: Approximate costing of introducing further controls: **£**_____ Expected completion date: _____
Signatures of Information Asset Administrator: Signature of Information Asset Owner: Risk Assessment Reviewed by Information Governance Steering Group on: Calculation of risk to CCG Board: Yes / No