
By: Roger Gough, Cabinet Member for Business Strategy, Performance and Health Reform

David Cockburn, Corporate Director Business Strategy & Support

To: Corporate Policy Overview and Scrutiny Committee

Date: 11 January 2012

Subject: Information Security.

Classification: Unrestricted.

Summary: Members are asked **to note** the context and principles of the effective management of Information Security.

---

1. Introduction

(1) All organisations that handle personal information about individuals have to protect that information under the Data Protection Act 1998. In addition, public authorities must provide information through an approved Publication Scheme and respond to requests under the Freedom of Information Act and Environmental Information Regulations. The Information Commissioner's Office (ICO) is the UKs independent authority set up to uphold information rights.

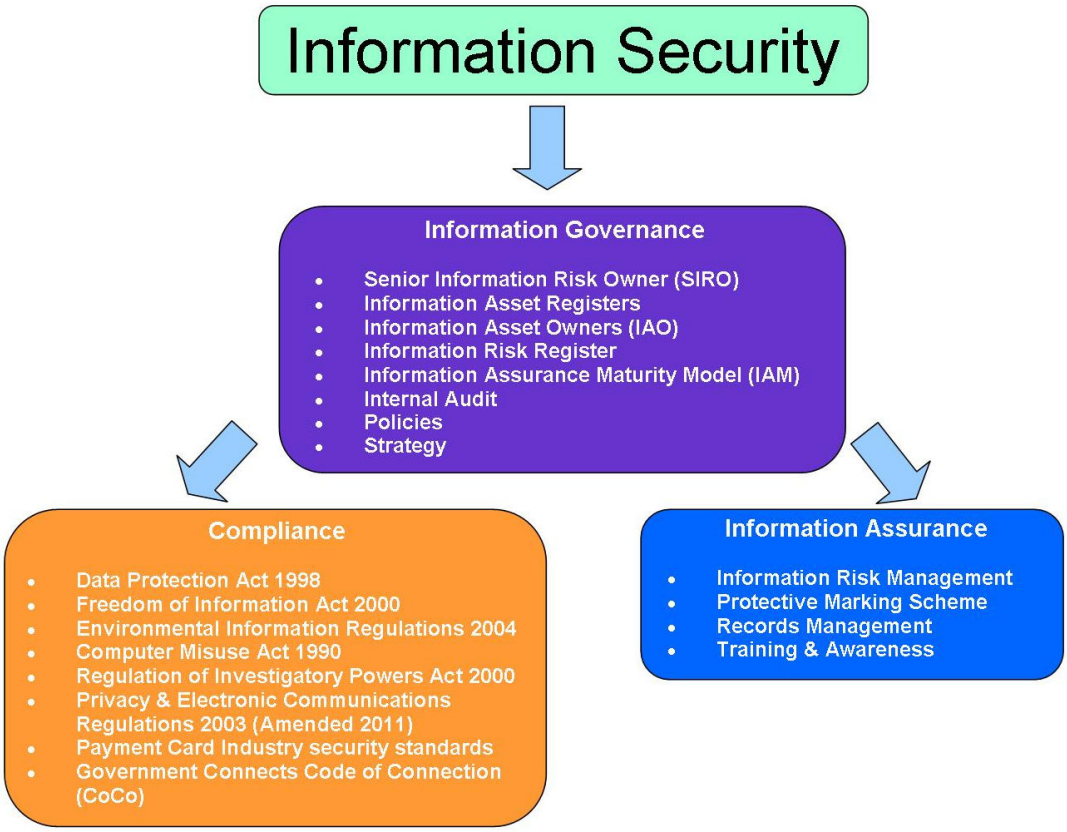
(2) The 2007 HMRC data loss incident and subsequent high profile breaches highlight the need for effective information security. The ICO has the power to impose large fines and has increasingly demonstrated its willingness to exercise these powers. Where a breach or incident occurs the ICO investigates governance arrangements and has the power to compel an organisation to sign undertakings to improve information security. As important is the growing public awareness of their rights as Data Subjects.

(3) KCC responds with technical and operational measures aimed at improving information security in the way we communicate and transact business, including compliance with GCSx Code of Connection (CoCo) and Payment Card Industry (PCI) standards. Connecting to partners in health also requires KCC to gain accreditation to their information governance standards.

(4) KCC handles significant amounts of personal data and has a legal and moral duty to protect and safeguard this information. This is demonstrated through effective information security, sound governance and risk management. The growth in inter-agency information sharing and Shared Services suggests adoption of common approaches and standards. KCCs centralisation of business strategy and support offers opportunities for a strategic approach to

further developing our information assurance maturity to ensure an accurate awareness of significant, systemic enterprise-wide information risks.

2. Information Security in Context



Information Security

(1) Information Security is the generic term for protecting information, data and information systems from threats and vulnerabilities. Whilst most information is stored and processed electronically, the term includes manual records, documents and data stores.

Information Governance

(2) Information Governance (IG) is about having effective structures and policies in place to ensure legal and regulatory compliance and the effective management of Information Risk.

(3) KCCs Senior Information Risk Owner (SIRO) is ultimately responsible for organisational information risk management and for legal and regulatory compliance. This role is undertaken by the Director of Governance and Law. In order to be effective, organisational structures must support systemic identification and reporting of information risk. KCC is making steady progress with an established Information Governance working group and the recent consolidation of information assurance roles within a single team. This approach enables the SIRO to know what information is held (Information Assets), for what purpose, and who is accountable (Information Asset Owners).

(4) KCC has issued Policies and Guidance Notes that set out the acceptable behaviour of users of its ICT based business systems together with the measures it takes to monitor activity and the consequences of unacceptable behaviours. These are available to all users who have access to KNet. These include:

- The Information Security Policy;
- The ICT Security Policy;
- The Electronic Communications Policy;
- The Electronic Communications User Guidance;
- The Acceptable Use Policy for non-KCC Owned Electronic Devices;
- The Malicious Software Protection Policy.

Information Assurance

(5) Information Assurance (IA) is the practice of how the business maintains an environment where information is appropriately protected (confidentiality), kept up to date and processed correctly (integrity), and made available where and when required (availability).

Information Risk management

(6) Information Assets implicitly have value. This value may be in terms of the impact on the business if it becomes unavailable through error, nature (e.g. flood or fire) or malicious activity, or the reputational impact of uncontrolled disclosure. Storing and protecting data that is out of date or of little (if any) value adds overheads to the business in terms of storage capacity and potential risk. There is also a realisation that resources might be protected to exploit copyright in order to be traded to recover the costs of creation and production.

(7) An Information Security Management System (ISMS) is a formal approach to managing Information Risk and is exemplified by the ISO27000 suite of standards. These standards describe a systemic approach to identifying, valuing and appropriately protecting information assets, data, records and information. The business impact of the information's vulnerability to various threats is assessed using worse-case scenarios, and where appropriate, treatments and controls implemented.

(8) Implementation of a comprehensive ISMS across KCC would require considerable commitment in time and resource and is only likely to be achieved in the context of a maturity model (see below).

Protective Marking

(9) Protective Marking is the routine marking of documents and files according to the sensitivity of their content. This is usually in the form of a classification that is added as a 'header' and/or 'footer' to a document or included in a filename for electronic documents. The Government Protective Marking Scheme has six categories of confidentiality of which four are applicable to LAs. These are, in increasing order of sensitivity: NOT PROTECTIVELY MARKED; PROTECT; RESTRICTED and CONFIDENTIAL.

The remaining two: TOP SECRET and SECRET relate to national security and are unlikely to be encountered. Most are used with an additional descriptor that indicates the reason for protection, e.g. PROTECT - PERSONAL where the document contains personal information about an individual, or PROTECT - COMMERCIAL where the interest of the Council or a Third Party may be prejudiced by disclosure. With a coherent and consistent Protective Marking scheme, LAs can set policies and procedures for the way documents are produced, handled, stored and destroyed. The process of determining an appropriate Protective Marking is based on a risk assessment of the impact on Council business or on Council Members, Contractors, employees or members of the public if disclosed.

(10) Protective Marking is an important means for enabling computer and IT systems developers to determine appropriate technical controls when commissioning new services.

(11) There is considerable variance in the way Protective Marking is implemented across LAs, and the Information Governance working group are currently exploring how a coherent protective marking scheme might be implemented.

Records Management and Retention

(12) Storage and retention of records, documents and data has a cost, whether in paper or electronic form. These include storage costs in terms of the physical and electronic space they consume and the cost of their protection. The speed and ease with which electronic records and documents can be copies and distributed leads to multiple versions, duplication and an increase in risk. This can potentially impact on the integrity of business processes and increase the risk of a breach of confidentiality.

(13) A number of LAs enforce strict document management and archiving systems to assure the integrity of documents and data. Records management systems typically differentiate between ‘principal records’, ‘reference copies’ and ‘reference material’. An effective document management system reduces risk by controlling who has access to protected information and at what level, e.g. view only, editor, contributor etc.

(14) KCC has well developed policies and guidance for effective records management, however the increasing use of electronic document formats and inconsistent national approaches to archiving presents risks that will need to be effectively managed.

Data Protection Act Compliance and Privacy Impact Assessment

(15) It is important to recognise the importance of compliance with the principles of the Data Protection Act 1998 when designing, commissioning or operating business systems that process personal or sensitive personal information. Individuals are increasingly aware of their right to fair and lawful processing of their information and systems must be in place to ensure their rights are upheld and their privacy protected.

(16) The Information Commissioners Office sets out useful guidance and model processes for ensuring compliance and for assessing impact on privacy. Effective technical and organisational measures must ensure that appropriate safeguards are in place and that the impact on privacy is considered when designing systems. KCC is committed to ensuring staff at all levels are aware of the basics of data protection law and privacy.

ICT Security

(17) KCC's ICT Division operates a layered security model that controls physical access to buildings and logical access to network and computing resources. This substantially reduces the risk of unauthorised access to business systems and the personal and/or sensitive information these may contain. The risk that legitimate access to personal/sensitive information is misused for personal gain or inappropriate and unauthorised disclosure remains. Whilst pro-active monitoring of user activities, use of 'Data Loss Prevention' software and adoption and enforcement of 'access to information' policies may provide greater protection, it would add considerable additional cost and remain far from fool proof.

(18) Critical ICT infrastructure is housed in secure facilities with servers and network components housed in dedicated data-centres where access is restricted to authorised personnel. Where third-party engineers require access they are escorted at all times by an ICT Division engineer. Malicious acts by ICT staff with administrator or physical access cannot be ruled out however the risks of complete data loss are very low as systems are regularly backed-up. Any such act would be recorded and traceable to the instigator which all professional ICT staff are aware of. This staff group will also be aware of the zero tolerance approach to any breach of security protocols.

(19) Access to KCC computers, authorised network resources and business systems requires a valid current User Account. The creation and deletion of these User Accounts can only be carried out by authorised ICT Division personnel in response to requests received from appropriately authorised line managers and/or HR Division.

(20) HR Division provides assurance that all newly employed personnel have been vetted in line with HMGs Baseline Personnel Security Standard. ICT Division relies on the processes adopted by Kent Top Temps for the vetting of contractors and temporary staff. The process for controlling User Accounts meets industry recognised standards and has been audited and approved by KCC's Internal Audit's ICT Auditors as well as external agencies.

(21) Password policies meet industry standards and are set to provide sufficient complexity and force periodic change to prevent use of dormant accounts. The computer accessing the network must also be known to the system, creating a second logon check. If the computer or user is unknown, access will be denied and the attempt logged as a security warning.

(22) ICT Division encourages the use of Microsoft products as these allow centralised management of security policies. Most line-of-business applications (e.g. ICS, Impulse, SWIFT, WAMS, OBS and Spydus) have separate user identification and authentication processes and hence different user

accounts/passwords. The level of access granted to these users is defined and governed by these application systems.

(23) System Administrators that have rights to grant access or have direct access to data now sit within ICT Division. Audit features are built into applications and ICT Division's administrator activities are logged.

(24) Since Oct 2009 all new remote-working personal computers (e.g. lap-tops, notebooks and tablets) ordered from ICT Division's IT-Shop are provided with full-disk encryption as standard. This includes an option to install encryption software on existing PCs. Encryption software is now installed in 2,730 lap-tops etc. ICT Division are able to provide software on request for encrypting documents sent using storage devices (e.g. CDs, DVDs etc.) or as email attachments to external organisations. Since July 2009, ICT Division's IT-Shop has provided over 550 encrypted USB memory sticks.

(25) Since late 2004, the Criminal Justice Secure Mail (CJSM) email system has been available for the secure exchange of e-mails between KCC and other organisations involved in criminal justice. The system was initially installed for staff involved with the Youth Justice Board, but has since been extended to other areas of KCC dealing with justice and vulnerable citizens. Since June 2009, KCC has been able to use the local government e-mail system (GCSx) of central government's secure network (GSi) for sending/receiving e-mails to central government departments, other local authorities, police forces and the NHS. Currently, KCC has 420 GCSx e-mail accounts.

3. Achieving Information Assurance Maturity

"… underpinning all of the technical requirements, is cultural change management"

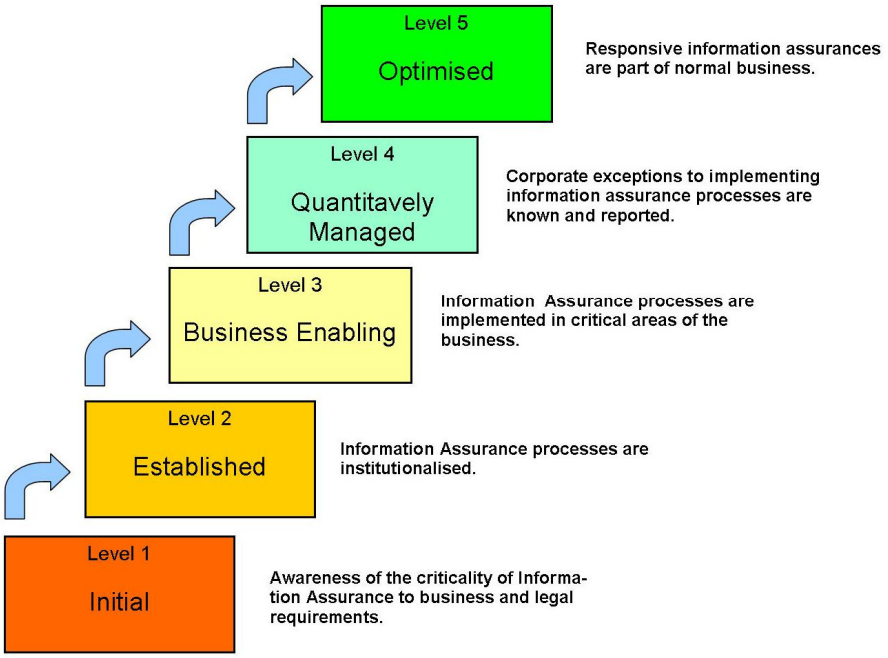
(1) Effective Information Assurance is a challenge facing all LAs as public and media awareness of the legal and regulatory framework for information security, data protection and privacy increases. KCC is committed to continuous improvement and is already developing a 'Statement of Required Practice' for information management that recognises a need for investment in staff awareness and training. Recent organisational changes have centralised responsibility for information assurance within the Business Strategy and Support (BSS) Directorate. This directly supports the role of Senior Information Risk Owner (SIRO).

(2) The move from reactive incident management to proactive risk management is an important change that will support managers in understanding information risk and prioritise actions for improvement. Organisational maturity models provide a useful framework for improvement, and the Information Assurance Maturity Model (IAMM), widely adopted across government is recommended as a strategic approach for improvement.

(3) Whilst the Information Assurance Maturity Model provides a framework for measuring improvement, this will be supported through an effective strategy that sets out a formal programme of work to target those areas of the business managing the highest risk and the time scales over which this can be achieved.

(4) It is worth considering the unique role of ICT in achieving effective information assurance. ICT is primarily concerned with the technical measures required to protect the confidentiality, integrity and availability of information and data held on business information systems. An information risk management approach ensures that technical measures are appropriate and not unduly excessive. Information Assurance must however be business led and integrated with other aspects of business risk management.

Information Assurance Maturity Model



4. Conclusion

(1) "Compliance is often the business driver behind WHY we have information governance, risk gives us the intelligence and data to understand WHAT threats, vulnerabilities and exploits our information is exposed to. Information Assurance gives us a practical framework to know HOW to deal with the risks, through operational processes, procedures and scrutiny. Governance gives us the formal structure WHERE and HOW we implement, monitor, audit and improve WHAT we are doing. This in the long run, will save money, improve efficiency and effectiveness by reducing risk.

(2) "You cannot reduce risk until you can quantify the risks you are dealing with. A car cannot know how fast it is going, unless you have a speedometer, brakes to slow it down and an accelerator to speed it up. You wouldn't want to rely on speed cameras and speeding fines to monitor your speed for you!" *(Quote from Information Governance a Structured Approach (Gov Connects G3C Toolkit 2010))*

5. Recommendations

Members are asked to note the contents of this report.

6. Background Documents

Government Connects G3C Toolkit
http://g3ctoolkit.net/

HMG IA Maturity Model – CESG The National technical Authority for Information Assurance (2010)
http://www.cesg.gov.uk/products_services/iacs/iamm/index.shtml

Managing Information Risk: A guide for accounting officers, board members and senior information risk owners - National Archives (2008)
http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf

What is an information asset? (Factsheet) – National Archives (2008)
http://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf

7. Author Contact Details

Peter Bole, Director of ICT

✉ peter.bole@kent.gov.uk ☎ 01622 696174

Geoff Wild, Director of Governance at Law

✉ Geoff.wild@kent.gov.uk ☎ 01622 694302