For publication

DRAFT INFORMATION GOVERNANCE STRATEGY

Author: Robert Beane (Veritau Ltd)

Date: March 2010

Approval: Executive

Audience: Council officers

Contents

Introduction

1. The objective of this strategy is to fulfil the objectives of the Information Governance Policy, including ensuring business efficiency, effective service delivery, and compliance with the individual and social obligations the council has in respect of all the information it holds. Information Assurance and Information Risk Management (IRM) are the means by which this will be done.

2. The council recognises the importance of reliable information to support the provision of good quality services. Information governance (IG) and assurance play a key part in ensuring the reliability of this information as service delivery relies on the right information being available to the right people at the right time, whilst maintaining individual privacy.

3. IG offers assurance to the council, its customers and other stakeholders that all information, including confidential and personal information, is dealt with in accordance with legislation and regulations, and its confidentiality, integrity and availability is appropriately protected.

4. This Information Governance Strategy provides a mechanism for ensuring that the council meets its responsibilities in the following areas:

   a) the growing need for it to share information means that it must apply the common standards mandated by the Code of Connection and Connecting for Health.

   b) The LGA's "Data Handling Guidelines" apply the government's Security Policy Framework to local authorities and set out standards to be applied by the council to ensure security of data, and be seen to do so.

   c) The mandatory Records Management Code of Practice.

   d) However, in addition to these standards there is a body of best practice measures, which if applied will assist the council in discharging its obligations to enact effective IRM.

5. The Data Protection Act and Human Rights Act provide the legal framework to safeguard privacy. The council is responsible for managing the personal information it controls, and also for responding to requests for information in accordance with the legislation.

6. Technical and managerial security measures must be taken to minimise the scope for error or malicious action. Technology and external threats both continue to change quickly whilst the use of information in the council is likely to increase as services are improved through MoreforYork. The council must embed risk management in the use of

information, both when planning business and operating it. Clear accountability is vital, particularly at senior levels, to ensure that risks to information are considered from the outset. Because no information handling system provides total protection, performance needs to be monitored and lessons learned on an ongoing basis.

7. The move to the new council Headquarters is not a strategic information governance objective – but it is certainly a test of the council's ability to manage its records under time pressure. It is actually a once-in-a-lifetime opportunity to put records management in good order and the principal tool to do so, the Documentum EDRMS, is already in place. With sound policy guidance the full benefits of that investment can be realised within the new building.

Strategy Objective

8. To assist the Senior Information Risk Owner (SIRO; see reference 1 for explanation) to put in place an effective change programme to improve IG and IRM, it is proposed that the Cabinet's Information Assurance Maturity Model (IAMM) will be adopted and adapted by the Information Governance Officer, Veritau (IGO). This Model will incorporate the requirements of the government's Security Policy Framework and its 2008 Data Handling Review and is aligned with the ISO27001 Standard and the broader outcomes sought by the National Information Assurance Strategy.

9. The Model is designed to help the SIRO establish a comprehensive programme of work to achieve progress through clearly identifiable milestones towards the achievement of three main information assurance goals:

(A) Embedding IRM Culture within the Organisation:

10. The need to assure information as a key business asset is embedded within the culture of the council, its delivery partners and its arm's length bodies

11. Procedures are in place so that CMT is able to understand and manage the information risk to which the council is exposed

12. The agreement of external stakeholders is reached on the treatment of information risks, particularly when they will impact on the delivery of Shared Services and Transformational Government objectives

(B) Implementing Best Practice Information Assurance Measures:

13. Through-life measures are implemented to assure all information within the council, its delivery partners and its arm's length bodies, so that changes can be made to processes and systems to match the tempo of the business without introducing undue vulnerabilities.

14. Systematic monitoring of networks, systems and boundary points is undertaken so that the council can effectively detect and respond to vulnerabilities, threats and incidents in a timely manner, thus reducing potential adverse impacts to its business to an acceptable level.

(C) Effective Compliance:

15. An effective compliance regime is implemented across the council, its delivery partners and its arm's length bodies, to ensure its compliance with legislation and the proper management of information risks in accordance with national policy & standards.

16. Internal and external review provides independent assurance to the SIRO that the compliance processes are working effectively.

17. Achieving maturity towards these goals assisted by the Model will enable the council to generate greater trust in its information systems and processes, both internally and between trusted partners. This will be particularly important in the context of shared services, and the issues surrounding shared versus individual risks to information; whether it belongs to the council or to the member of public.

18. Each level of the Model will aim to build on the achievement of the preceding levels; as such the measures are cumulative. The levels below summarise how the council will know when it has achieved compliance:

Level 1 – Initial. At this level CMT will be aware of the criticality of IG to the business and of its legal requirements. Consequently it will have initiated activity to address areas of immediate weakness and have policy in place to guide the improvement process. It also has applied this policy to all new information systems. The Government's Data Handling Report measures are built into Level 1 of the Model and hence putting in place measures to deliver this level of maturity will result in delivering Data Handling Report compliance.

Level 2 – Established. At this level IG processes will be institutionalised within the council, its delivery partners and its arm's length bodies. A programme of targeted IG education and training will have been initiated and work to inculcate an appropriate IRM culture started. Discovery work will have been undertaken and the IG status of the entire council's

information systems and related processes determined. A definitive list of business critical information systems will have been endorsed by the SIRO. Based on this list and the discovery work, a fundamental requirement at this level, is for the SIRO to have personally made the business case to CMT for a targeted programme of work to improve understanding and control of information risk, and gained approval for the programme. Within most organisations, progress to Level 2 will require extensive work to be undertaken.

Level 3 – Business Enabling. At level 3 IG awareness across the council has increased leading to a measured improvement in IRM behaviours at all levels within the organisation, its delivery partners and its arm's length bodies. Building on the framework of IG processes rolled out at Level 2, Level 3 will be achieved when all critical areas of the business are subject to a robust IG regime.

Level 4 – Quantitatively Managed. At level 4 there will be evidence to show that staff attitudes and behaviours towards assuring information are aligned to the needs of the business. The regime established at level 3 for critical areas of the business is extended to embrace the whole business. As a consequence the SIRO will have the IG metrics available to take an informed approach to managing the risk to the information used by the business.

Level 5 – Optimised. Level 5 is achieved when IG is fully integrated as an aspect of normal business and the culture of the business is such that at all levels of management, IG is judged to be a business enabler.

19. The council's Model will be a living document which will be updated in line with changes in the threat, changes in national standards, and as a result of lessons learned from applying them to the council.

20. The top level statements contained in each box of the Model are by necessity very brief. To gain a full understanding of what is required to satisfy a particular Level refer to the IA Assessment Framework.

Information Assurance Assessment Framework

21. The Framework provides specific details of the measures which are expected to be in place within the council and is seeking to meet the top level statements of maturity contained within the Maturity Model. This enables the Maturity Model and the Framework to be used as an integral part of an IG Review Process.

22. The contents of both the Model and Framework have been drawn from a variety of sources and are compliant with the requirements of the Information Security Management System (ISMS) embodied in ISO 27001.

Using the Information Assurance Maturity Model and Information Assurance Assessment Framework

23. Included within the main body of the Model is a range of internal reporting and compliance mechanisms, which are aimed at establishing and maintaining clear management responsibility and accountability for IRM within the council. These arrangements should facilitate the collection of the information required annually for potential inclusion in the Annual Governance Statement.

24. The council along with other local authorities is encouraged to adapt and use the Model and Framework to establish the programmes of work needed to achieve IG maturity and also to conduct self assessment reviews.

25. By adopting the Model, the council will have to address a number of action plans and to allocate the appropriate roles and responsibilities. **Appendix 1** provides a summary overview of the proposed different IG roles and responsibilities for the council. **Appendix 2** is a diagrammatic presentation of the "tree" of policies, strategies and tools which might feed into the council's overall IG framework; this picture will evolve to reflect new standards and legislation, and the outcomes of MoreforYork and the EDRMS Project.

26. Adopting and applying the Model to the council will be an extensive and long term exercise requiring resources to be identified for delivery and a considerable cultural change. An action plan for Level 1 compliance is in progress and will eventually form part of this Strategy. To assist the SIRO in establishing immediate priorities, an initial high level action plan is included at **Appendix 3**. Attainment of these key actions will ultimately assist in meeting the requirements of the more detailed Level 1 action plan to be developed.

IG roles and responsibilities

References are to the table at Appendix 1

27. The Chief Executive takes overall responsibility for the council's information governance performance and in particular is required to ensure that:
    a) decision-making is in line with council policy and procedures for information governance and any statutory provisions set out in legislation;
    b) that information risks are assessed and mitigated to an acceptable level;
    c) information governance performance is continually reviewed;
    d) suitable action plans for improving information governance are developed and implemented;

e) the council's management competency framework is used to measure the performance of senior managers against information governance targets and objectives.

28. To satisfy the above responsibilities, the Chief Executive will nominate a Senior Information Risk Owner (SIRO) who will be accountable for the council's overall information governance arrangements.

Ref 1 Senior Information Risk Owner

29. The Chief Executive must appoint a manager of an appropriate seniority as its SIRO. The Director of Resources is a member of CMT, and is already accountable to Audit & Governance Committee on information governance matters, and is therefore an appropriate SIRO.

30. Responsibilities of the SIRO include:

a) owning the information risk policy and risk assessment;
b) acting as an advocate for information governance and assurance at CMT and in internal discussions;
c) chairing the Corporate Information Governance Group (CIGG);
d) providing written advice to the Audit and Governance Committee relating to information risk;
e) managing delivery of information governance and assurance services.

Ref 2 Directors

31. Each Director is responsible for the information within their directorate and must therefore take overall responsibility for information governance matters. In particular Directors are required to:

a. ensure that adequate resources are available to successfully manage information governance within their directorate;
b. use competency frameworks to measure the performance of senior managers against information governance targets and objectives;
c. assign a senior manager as the Directorate's Information Governance Champion at Assistant Director Level;
d. ensure implementation of corporate information governance associated policies and procedures;
e. identify their information assets (in all formats);
f. categorise these information assets in a way that is meaningful to the directorate and identify for each information a responsible Service Manager;

32. Each Directorate is also responsible for:

a. managing its own information risks;
b. ensuring proper management of information risks;

c. meeting the mandatory corporate information governance requirements; and
d. meeting the requirements of the Information Policy.

33. Directorates must have and execute plans to lead and foster a culture that values, protects, uses information for service delivery, and monitors progress when conducting a service user (including employees) survey or equivalent. Directorates must also reflect performance in managing information risk into HR processes in particular making clear that failure to apply directorate and corporate procedure is a serious matter, and in some situations non compliance may amount to gross misconduct.

Ref 3 Directorate Information Governance Champions

34. Each Directorate's Information Governance Champion adopts a strategic role for Information Governance and will co-ordinate Information Governance across the directorate and will lead in Information Governance planning, reporting and review. The Champions are required to meet on a regular basis with their Corporate Directors and Service Managers to ensure that Information Governance plans and performance are continually reviewed.

Ref 4 Service Managers

35. These are senior officers involved in running the relevant business area within a Directorate. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has accessed it and why. All information should be categorised in accordance with the Document Security Marking Policy and stored in line with the council's eDRMS arrangements.

36. This will facilitate an understanding of the risks to the information and how those risks need to be managed to ensure compliance with legislation. Service Managers will be expected to support the audit process and produce an annual written judgement of their information asset to include the use and security of their asset.

37. Service Managers have the most work to do since they will be applying all the policies in table 2 to their services and all the information they use. They must identify and maintain a record of those members of staff, contractors and others with access to or involved in handling individual records containing personal data. Service Managers should:

a. ensure that information is used correctly and protected;
b. review each records series in the light of each of the above policies to ensure that (for instance) security marking, legal admissibility and access controls are all properly applied;
c. consider whether and how better use could be made of their information assets and to information held by other services.

eDRMS being a part of MoreforYork provides a mechanism for this, as does the new Intranet, COLIN.

Ref 5 Audit & Information Assurance Manager

38. The role of the Audit & Information Assurance Manager (Veritau) is to provide assurance that the council's Information Governance and Assurance Framework is operating according to its structure of policies, strategies and action plans. Based on an audit risk assessment, Veritau's Internal Audit Service will undertake a programme of compliance testing to ensure that the council is meeting its obligations. The Audit & Information Assurance Manager will be a member of the council's new Corporate Information Governance Group.

Ref 6 Information Governance Officer

39. The Information Governance Officer is responsible for the development and communication of information governance policy, strategy and action plans and for ensuring that the council adopts information governance best practice and standards. The Information Governance Officer is the first point of contact on information governance matters for all officers and elected members, members of the public and the Information Commissioner. The officer reports to the Audit and Information Assurance Manager and will also be a member of the Corporate Information Governance Group.

Ref 7 Information Governance Team

40. The Information Governance Team supports the Information Governance Officer by contributing to the development of information governance policy and strategy. The Team will also be the central co-ordination point for all responses to requests for information made under the Data Protection, Freedom of Information and Environmental Information legislation. The Team maintains a record of all such information requests received and responded to and ensures that statutory deadlines are met.

Ref 8 Corporate Information Governance Group (CIGG)

41. The terms of reference and membership of the council's current Information Governance Working Group will be revised to reflect the Framework. The new Group will be referred to as CIGG and will have the following roles and responsibilities:

    a) Approval of corporate policies and procedures which ensure:
        - compliance with legislation
        - data quality
        - information security (compliance with ISO 27000)
        - records management (compliance with ISO 15489).

b) Co-ordination and approval of corporate standards for the mitigation of risk.
c) Monitoring compliance with the Information Governance Assurance Framework
d) Establishing a policy for reporting, managing and recovering from information risk incidents, including losses of protected personal data and ICT incidents, defining responsibilities and making staff aware of the policy and reporting to councillors if appropriate.
e) Providing and maintaining mechanisms that command the confidence of individuals through which they may raise concerns about information risk to senior management or the Audit and Governance Committee, anonymously if necessary, and recording concerns expressed and action taken in response.

42. In addition, consideration will need to be given to how directorates manage and monitor their own information governance issues on an ongoing basis. For example, it may be appropriate for information governance to become a standing or regular agenda item at directorate management team meetings. This will give Directorate Information Governance Champions the opportunity to highlight issues or to report on progress made in managing the directorate's information assets. Any significant issues identified can then be reported to the Corporate Information Governance Group.

Ref 9 Internal Audit (Veritau)

43. Based on an audit risk assessment, Veritau's auditors will undertake a programme of compliance testing to ensure that the council is meeting its obligations.

Ref 10 Audit & Governance Committee

44. The SIRO will report to Audit & Governance Committee twice a year on information governance matters. The SIRO will highlight changes in framework and policy and detail the progress made in embedding the framework across the council. The results of compliance testing will also be reported where applicable.

Ref 11 eDRMS

45. The Electronic Document Records Management System (eDRMS) Project will have a significant positive impact on many areas of the council's operations as it will enable improved management of, and access to, the documents and records held within the organisation, as well as providing a secure, single data repository. The Information Governance Officer will work with the eDRMS Project Manager in delivering the benefits of the system in line with the Information Governance Policy .

Ref 12 Information Security

46. Information Security considers the provision of ICT services to the council in a secure environment in accordance with the ISO 27000 series of standards including:

    a. development and management of the council's information security policy;
    b. investigation of technical security incidents and breaches;
    c. periodic verification of compliance with policies via information security reviews;
    d. provision of awareness and compliance programmes for the council.

Ref 13 Data Quality

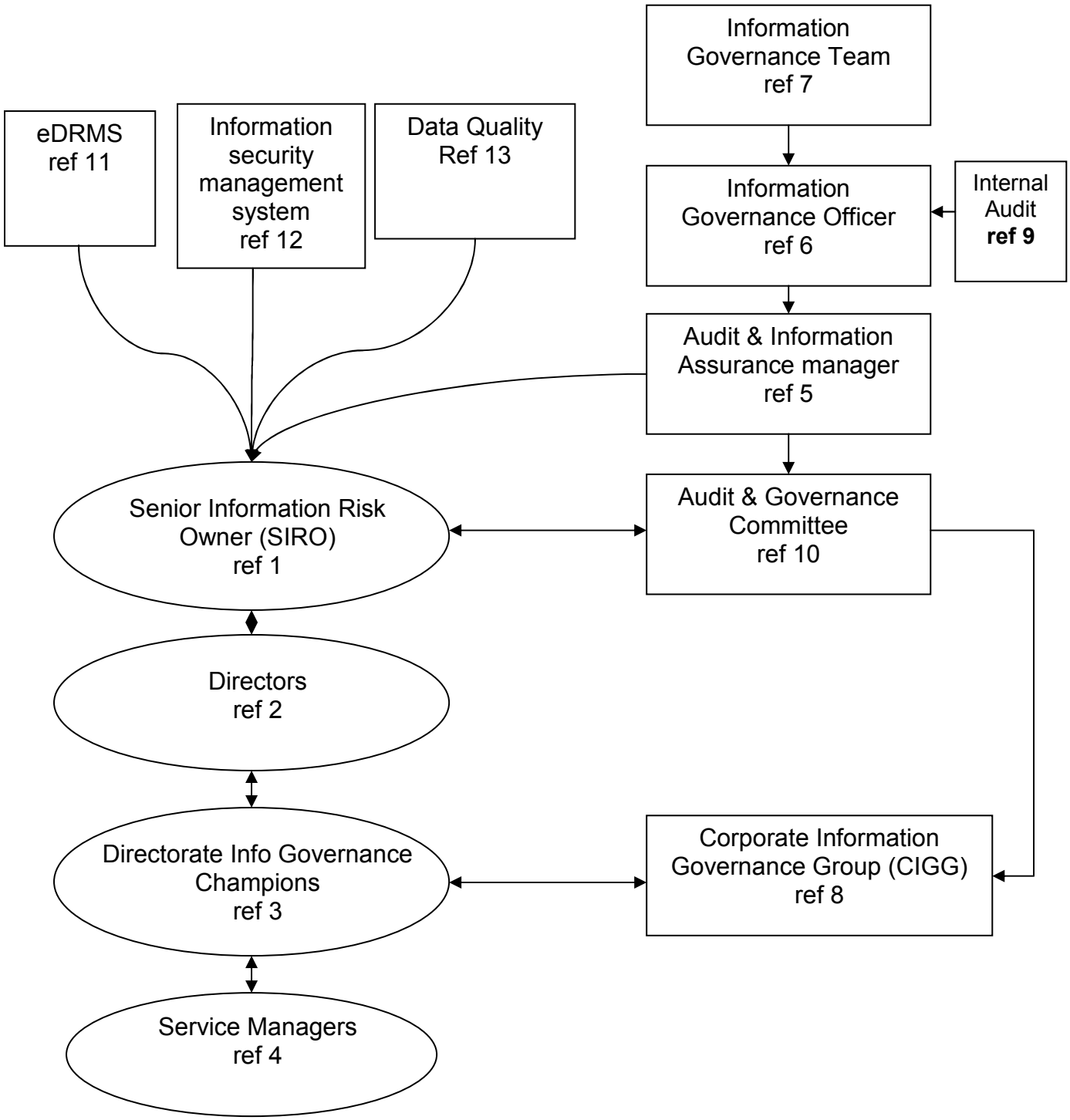
47. The council will put in place appropriate policies and procedures to secure the quality of data it records and uses. The approach will ensure:

    a. a formal data quality policy and associated operational procedures and guidance for staff are in place, covering data collection, recording, analysis and reporting;
    b. all data quality policies and procedures meet the requirements of any relevant national standards, rules, definitions and guidance, and define local practices and monitoring arrangements;
    c. periodic review of all data quality policies and procedures;
    d. data quality policies and procedures are appropriately accessible to staff;
    e. consistent application of data quality policies, procedures and guidance.

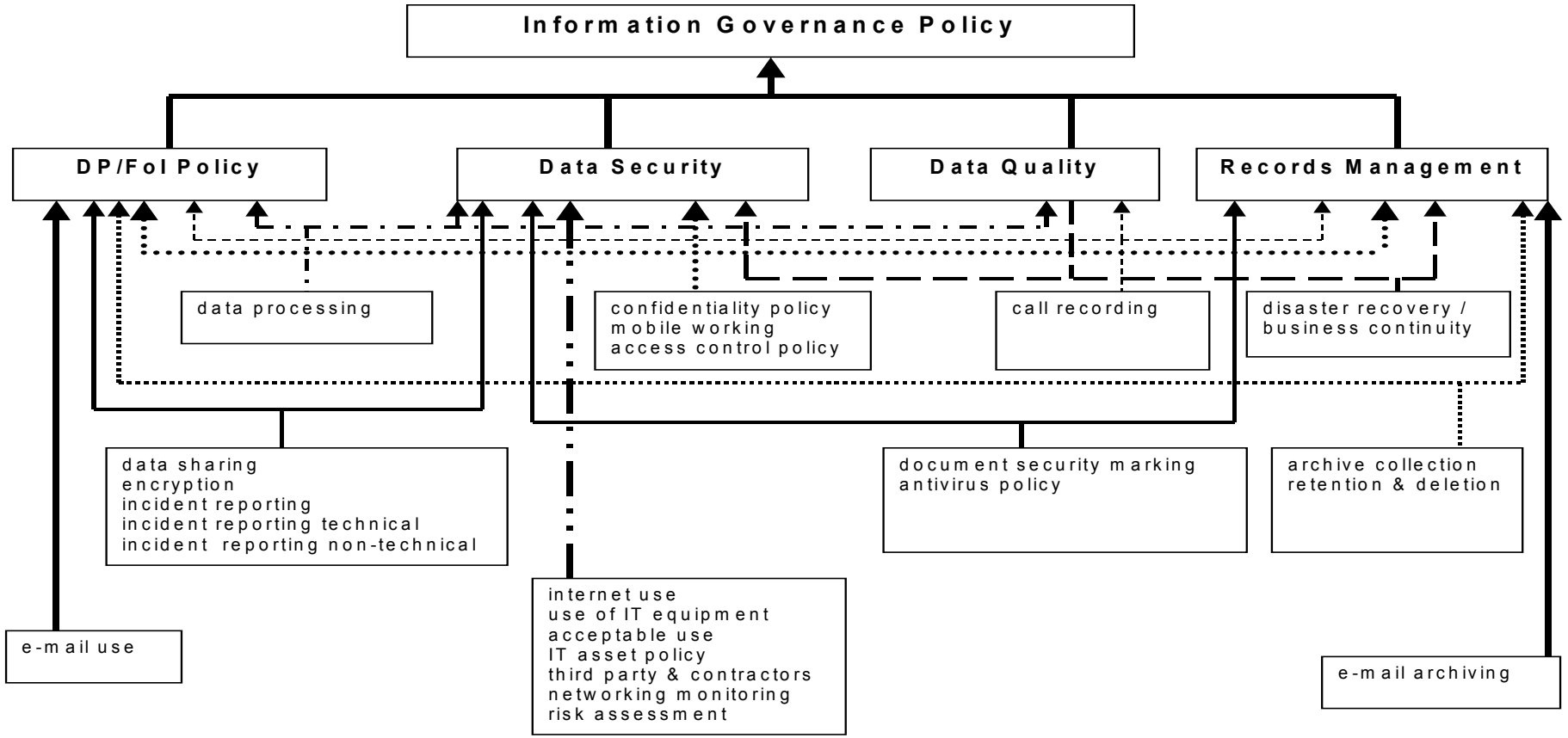
First Steps

48. In meeting the requirements of the Information Governance Policy the council will seek to undertake a number of key initial actions as part of delivering its Strategy. The council will have to set the foundations for creating the right culture and for ensuring that the correct policies and procedures are in place to provide accountability and scrutiny. Therefore, Appendix 3 represents the first steps that the council will have to take.

Appendix 1: Roles and responsibilities



Appendix 2: Policy Tree



Appendix 3 - Immediate Action Plan

Ref	***Requirement***	**Current position**	**Actions required**	**Target Date**	**Action Taken**
P1 People					
P1a	*Appoint a Senior Information Risk Owner (SIRO) to ensure there is accountability*	• SIRO not yet formally appointed • Currently Information Governance Working Group	• Recommend that SIRO should be Director of Resources. • Corporate Directors to nominate at least one Information Governance Champion (DIGC) within each of their directorates. • Create a new Corporate Information Governance Group comprising key representatives and clear ToR with SIRO as Chair.	April 2010 April – May 2010-01-11 April 2010	
P1b	*Each Information Asset should have a named Service Manager as Owner*	2004 records survey and eDRMS project plan have identified services and records series.	• Commence compilation of Register of Information Assets. • service managers and their information assets to be formally identified by Directorates with assistance from Information Governance Officer together with explanation of roles and responsibilities.	Summer 2010 Summer 2010	
P1c	*Identify Users and their access rights*	No clear evidence / consistent process for access controls for different types of data	• Consider how best to undertake an audit of access rights.	2010/11 Audit Plan	Nb - impact of eDRMS project

Ref	***Requirement***	**Current position**	**Actions required**	**Target Date**	**Action Taken**
			• Review any current procedures. Concentrate on confidential / sensitive information access control. • Develop Impact Labelling mechanism.	Summer 2010 June 2010	
P1d	*Foster a culture that properly values, protects and uses information*	Awareness of privacy and confidentiality is good Principal policies and guidelines exist although will have to be amended to be incorporated into the overall IG Framework.	• Assess training and promotion requirements across the council and significant partners • Establish appropriate and targeted training / awareness courses/briefings • Deliver training and collect evidence of completion as appropriate • Assess effectiveness of training • Establish review process / programme using appropriate methods of communication • Links to induction and appraisal procedures	May – June 2010 Summer 2010 Ongoing Ongoing Ongoing 2010/11	
P1e	*Maintain mechanisms for reporting and managing information risk incidents*	Information security incident reporting and management procedures need devising	• Devise procedures and raise awareness (can be part of the revised employees guide roll-out) • Assess benefits of joining a regional WARP (Warning,	May 2010 May 2010	

Ref	***Requirement***	**Current position**	**Actions required**	**Target Date**	**Action Taken**
			Advice and Reporting Point for information security threats and incidents) Review what is currently in place.		
P1f	*Maximising public benefit*	Information management review/audit is currently being considered.	Determine if an audit is appropriate if so agree the scope, objectives and timing of information audit to be undertaken by Veritau.	2010/11 Audit Plan	
P1g	*Publish an information charter*	An Information Charter has been drafted but will require CMT approval.	Approve draft corporate information charter.	April 2010	
P2 Places					
P2a	*Undertake regular risk assessments*	An Information Security Management programme is yet to be established.	Agree a corporate information security risk assessment approach / programme and compile a Corporate Information Risk Register.	May – June 2010	
P2b	*Ensure buildings and premises are secure*	Establish an Information Security Management programme	Conduct an audit of compliance with the following controls: • ID badges for staff. • Visitor management. • Clear desk / screen policy. • Security of personal paper -based information.	Audit Plan 2010/11	
P2c	*Wherever possible avoid the use of removable media*	IT has a programme for encryption and control of removable media	• Review current arrangements and implement additional controls of removable media where necessary. • Incorporate into encryption policy.	See IT devt plan	
P3 Processes					

Ref	***Requirement***	**Current position**	**Actions required**	**Target Date**	**Action Taken**
P3a	*Work towards a policy of least privilege*	No specific policy at present.	• Consider whether specific policy is required as may be covered under P1c and via Impact labelling arrangements. • If required - incorporate appropriate least privilege 'tests' into information security audit programme.	Summer 2010 Audit Plan 2010/11	
P3b	*Personal information should be kept within secure premises and systems*	Compliant for the most part with appropriate policies, procedures and guidelines in place.	• Raise awareness in conjunction with the release of the revised Employees Guide to Information Security. • Sign up to the Information Commissioner's Office 'Personal Information Promise'.	Summer 2010 April 2010	
P3c	*Wherever possible the bulk transfer of information should be carried out via a secure network*	Government Connect achieved Secure Email including encryption available now for external emails	Develop a strategy to limit the movement of confidential / sensitive information in favour of providing appropriately controlled access.	Summer 2010	
P3d	*Engage independent experts to carry out penetration testing*	Consult IT for current position	Establish a regular schedule of penetration testing.	Refer IT	
P3e	*Conduct Privacy Impact Assessments*		Develop PIA toolkit from ICO guidance.	April/May 2010	
P3f	*New ICT systems should be accredited to Government standards*	Consult IT for current position	Agree whether accreditation to Government standards will be pursued.	Refer IT	
P3g	*Ensure that suppliers and contractors adopt appropriate equivalent*		Liaise with Corporate Procurement to develop model contract clauses where necessary.	2010/11	

Ref	***Requirement***	**Current position**	**Actions required**	**Target Date**	**Action Taken**
	standards				
P4 Procedures					
P4a	*Produce a Corporate Information Risk Policy*	No formal document entitled 'Corporate Information Risk Policy' but IG policy specifies IRM as policy therefore separate document not required.	Ensure IRM incorporated into training & guidance.	April 2010	
P4b	*Complete Corporate Information Risk Plans (review and forward looking)*	No formal plans/risk register specific to IG in place.	Review Corporate Risk register on an annual basis.	Ongoing	
P4c	*Produce a Risk Recovery Policy*	No specific policy in place.	A separate policy is not required as the overall IG Policy will cover. Response to data security incidents will be detailed in the Data Security Incident Procedure to be drafted and approved by Summer 2010 – this will deal with recovery from incidents.	Summer 2010	
P4d	*Risk reporting mechanisms*	Corporate risk reporting currently in place.	Information Security Incident Procedure to be drafted and approved by CMT. This will detail how information security incidents both technical and non technical will be investigated and reported.	Summer 2010	
P4e	*Regularly test your policies and procedures*	Not possible until policies and procedures are formally implemented	Include in Audit Plan for 2010/11 onwards.	2010/11 onwards	