**Central Bedfordshire Council**
**Priory House**
**Monks Walk**
**Chicksands,**
**Shefford SG17 5TQ**

**please ask for** Martha Clampitt
**direct line** 0300 300 4032
**date** 16 September 2010

# NOTICE OF MEETING

## AUDIT COMMITTEE

Date & Time
**Monday, 27 September 2010 9.30 a.m.**

Venue at
**Room 15, Priory House, Monks Walk, Shefford**

Richard Carr
**Chief Executive**

To: The Chairman and Members of the AUDIT COMMITTEE:

Cllrs D Bowater (Chairman), R A Baker (Vice-Chairman), Mrs A Barker, T Green, A Shadbolt, P Snelling and B J Spurr

[Named Substitutes:

Cllrs: R D Berry, P A Blaine, P Freeman and A M Turner]

All other Members of the Council - on request

***MEMBERS OF THE PRESS AND PUBLIC ARE WELCOME TO ATTEND THIS MEETING***

# AGENDA

1. **APOLOGIES FOR ABSENCE**

Apologies for absence and notification of substitute members.

2. **CHAIRMAN'S ANNOUNCEMENTS AND COMMUNICATIONS**

To receive any announcements from the Chairman and any matters of communication.

3. **MINUTES AND ANY MATTERS ARISING**

To approve as a correct record the Minutes of the meetings of the Audit Committee held on 28 June 2010 and 30 June 2010.

4. **MEMBERS' INTERESTS**

To receive from Members declarations and the **nature** thereof in relation to:-

(a) Personal Interests in any Agenda item

(b) Personal and Prejudicial Interests in any Agenda item

5. **PUBLIC PARTICIPATION**

To receive any questions, statements or deputations from members of the public in accordance with the Procedure as set out in Part A4 of the Constitution.

6. **PETITIONS**

To receive petitions in accordance with the scheme of public participation set out in Annex 2 in Part A4 of the Constitution.

## REPORTS

| Item | Subject | Page Nos. |
|---|---|---|
| 7 | **Annual Governance Report** | To Follow |

To receive the findings of the accounts audit.

8 **Internal Audit Charter** * 5 - 24

This report presents the Internal Audit Charter 2010/11.

9 **Information Governance Framework** * 25 - 52

The report presents the Council's Information Governance Framework for approval.

10. **EXCLUSION OF PRESS AND PUBLIC**

To consider whether to pass a resolution under section 100A of the Local Government Act 1972 to exclude the Press and Public from the meeting for the following item of business on the grounds that the consideration of the item is likely to involve the disclosure of exempt information as defined in Paragraphs 3 of Part 1 of Schedule 12A of the Act.

**Items likely to be considered following the exclusion of the Public**

| *Item* | *Subject* | *Exempt Para.* | *Page Nos.* |
|---|---|---|---|
| EX1 | **Internal Audit Progress Report**<br><br>This report provides a progress update on the status of Internal Audit work for 2010/11. | * 3 | 53 - 58 |
| EX2 | **Tracking of Internal Audit Recommendations**<br><br>This report summarises the high risk recommendations arising from Internal Audit reports and outlines how these will be monitored, tracked and reported to the Audit Committee. | * 3 | 59 - 72 |

This page is intentionally left blank

**Meeting:** **Audit Committee**

**Date:** **27 September 2010**

**Subject:** **2010/11 Internal Audit Charter**

**Report of:** **Director of Customer and Shared Services**

**Summary:** This report presents the Internal Audit Charter 2010/11.

Contact Officer: Kathy Riches, Head of Audit

Public/Exempt: Public

Wards Affected: All

Function of: Audit Committee

**CORPORATE IMPLICATIONS**

**Council Priorities:**

An effective internal audit function will indirectly contribute to all of the Council's priorities.

**Financial:**

Although there are no financial risks from the issues identified in the report, the outcome of implementing the Audit Charter and Audit Plan is for the Council to better manage its risks, thereby increasing protection from adverse events.

**Legal:**

None arising directly from the report.

**Risk Management:**

None arising directly from the report.

**Staffing (including Trades Unions):**

None directly from this report.

**Equalities/Human Rights:**

None directly from this report.

**Community Safety:**

None directly from this report.

**Sustainability:**

None directly from this report.

**RECOMMENDATION:**

**that the Audit Committee note and endorse the 2010/11 Internal Audit Charter.**

## Background

1. Under the Accounts and Audit Regulations 1996 (revised in 200), the Council is required to maintain an adequate and effective system of internal audit of its accounting records and of its system of internal control in accordance with proper practices in relation to internal control.

2. Clearly the responsibility for internal control rests with the management of CBC and that role includes ensuring that key risks are identified and mitigating controls are in place to remove the impact or probability of these risks occurring.

3. The role of the internal audit function is to determine how effective the controls systems are and to measure the degree of reliance that can be placed upon these controls.

## Internal Audit Charter

4. To help management, employees, Members and contractors understand how Internal audit will interact with the organisation when carrying our its work an Internal audit Charter has been produced and is attached at Appendix A.

5. This document contains no significant changes from the 2009/10 Charter presented to the committee in April 2009. It has been updated to reflect revised roles and responsibilities arising from the Senior Management review.

6. The charter describes:
   (i) how the brief of each of these audits will be completed,
   (ii) how the audits will be carried out,
   (iii) the mechanism for communicating feedback from the audits
   (iv) an assurance rating and any recommendations arising from the audit.
   (v) follow-up arrangements of the audits and
   (vi) the escalation procedures where recommendations or reporting processes are not completed.

7. Also contained within the document are details of the responsibilities around fraud and investigations, the use of internal audit for consultancy purposes and the performance management framework that internal audit will work under setting out the key performance indicators for the function.

8. The final sections of the charter include the relationships that Internal Audit has with the Audit Committee, contractors and External Audit.

**Conclusion and Next Steps**

9. Adherence to the Internal Audit Charter by Managers, Officers and Auditors will help ensure that Internal Audit can successfully deliver the audit plan.

**Appendices:**
Appendix A Internal Audit Charter 2010/11.

**Background Papers:**
None

**Location of papers:** Priory House, Chicksands, Bedfordshire

This page is intentionally left blank

Appendix A

# CENTRAL BEDFORDSHIRE

# INTERNAL AUDIT CHARTER

Internal Audit
Central Bedfordshire Council

September 2010

# INTERNAL AUDIT - CHARTER

Contents

## 1. Introduction

1.1 This charter establishes the arrangements for the working relationship between Internal Audit and officers and members of Central Bedfordshire Council (CBC). It clarifies the arrangements for Internal Audit in CBC by setting out the responsibilities of the parties involved, namely Internal Audit, Officers of the Council, Members, and Partners and External Agencies.

1.2 Section 151 of the 1972 Local Government Act requires every Local Authority to make arrangements for the "proper administration of the financial affairs of the Authority." Under the Accounts and Audit Regulations 1996 (revised in 2006), the Council is required to maintain an adequate and effective internal audit of its accounting records and control systems. This responsibility is currently with the Assistant Director – Financial Services, who has sought to achieve this through the establishment of an efficient and effective Internal Audit Service. Internal Audit will seek to fulfil its role following both the Auditing Practices Board (APB) guidelines issued to all professional accountancy bodies and the CIPFA Code of Practice for Internal Audit in Local Government (2006).

## 2. Management responsibility for internal control

2.1 Management is responsible for the internal control systems that enable the Council to meet its objectives and deliver services efficiently and effectively. Its role is to identify risks to the service and to maintain an adequate and effective system of internal control to mitigate these risks. Management is also responsible for ensuring that staff are aware of the processes and procedures required to operate the control systems. It should be ensured that these controls are operating properly by periodic checking and supervision.

2.2 The role of the Internal Audit service is to determine the effectiveness of the controls and the degree of reliance that may be placed on the accounting and other records. The role is set out in the Council's constitution and is summarised in Section 5.4 of the Code of Financial Governance.

## 3. Audit Strategy & Annual Plan

3.1 Internal Audit has adopted a risk based approach to audit planning. The Head of Internal Audit and the Assistant Director – Financial Services will agree a one-year risk based audit plan of general systems reviews (including follow-ups of high risk reviews). The plan will also have a provision for fraud investigation works, information computer technology audits, contract audits, follow-ups, and ad-hoc consultancy work.

3.2 The annual plan will present the total number of audit days and how they are allocated to various reviews and Directorates. The Head of Internal Audit will be responsible for discussing and updating the annual plan with Assistant Directors, Directors and Senior Managers. The plan will be presented to the

Corporate Management Team (CMT) and Audit Committee for consideration and approval.

## 4. Audit Brief

4.1 The Auditor will discuss the scope of the audit and issue a consultation audit brief to the Principal Auditee (Service Manager/Assistant Director with the most responsibility in area under review) and/or the relevant Head of Service. A brief would include the following:

- Introduction
- Scope
- Objectives
- Risk Assessment
- Methodology
- Reporting
- Key contacts
- Budgeting (audit days allocated to review)
- Approval of brief

4.2 The Principal Auditee should promptly respond to a consultation draft brief. Following discussions and agreement on the brief, the Auditor will issue a final draft.

**4.3 The Principal Auditee has the following responsibilities to facilitate the review:**

**a. Approve the brief to confirm their understanding and agreement of the scope and nature of the review.**
**b. Identify controls which should be in place to address risks identified within the brief.**
**c. Inform appropriate staff and officers associated with the process under review about the nature of the review and what is required of them.**
**d. Provide suitable work space for the Auditor if on-site review is required.**
**e. Complete the action plan in the draft report and return to the Auditor within ten (10) working days.**
**f. Complete the Management Satisfaction Survey (Appendix A) at the end of the review and return to the Head of Internal Audit within five (5) working days.**

4.4 One week's notice will be provided to the Principal Auditee before the start of audit work. There is an exception in situations where fraud is involved or Internal Audit is requested to undertake urgent work.

## 5. Fieldwork

5.1 Internal Audit will undertake the fieldwork in accordance with agreed audit procedures and the final audit brief. Any changes in the scope of the audit must be agreed with the Principal Auditee.

5.2 During the course of the fieldwork, service departments will be required to make themselves and the appropriate records available to the Auditor within reasonable timeframes agreed between both parties. These timeframes should be appropriate for the information being requested and take into account the need for the Auditor to complete the review within the agreed budget. Officers need to ensure that a deputy (identified at the time of the brief) is informed of the audit should they need to progress the audit work.

## 6. Feedback of issues

6.1 At the end of the fieldwork:

- The Auditor will present their findings and recommendations for an internal quality review process.
- The Auditor will arrange the first exit meeting with the Principal Auditee (the Auditor will also invite key staff in the process to attend), to discuss the key findings and recommendations of the review and to obtain initial management actions to be taken to address the recommendations made.
- During the meeting, the Auditor and the Principal Auditee should discuss the findings and agree on the recommendations.

## 7. First draft report

7.1 Within 10 working days of the first exit meeting, a draft report will be electronically distributed to the:

- Principal Auditee

7.2 The Auditor will discuss the draft report in detail with the Principal Auditee and associated officers at a second exit meeting, where necessary.

7.3 To support the agreement of recommendations, a management action plan template will accompany the draft report. The Principal Auditee should complete this plan after the second exit meeting (in consultation with appropriate colleagues), setting out the names of staff responsible for implementing recommendations together with implementation dates. The Principal Auditee should return the completed action plan to the Auditor by the tenth (10) working day, after the second exit interview.

7.4 The Principal Auditee should ensure that officers with responsibilities in the action plan receive copies of the draft report and subsequent reports, are aware of the recommendations, and agree with the management actions.

7.5 To maintain confidentiality, Auditors will only issue reports to designated recipients, as agreed in the brief. Report recipients can distribute and discuss audit reviews with others at their discretion.

## 8. Final draft report

8.1 Following the second exit interview and agreement of the management action plan, the Auditor will produce an amended draft. When the final draft report is issued it should contain nothing unexpected. The Principal Auditee, and Assistant Director will receive the Final draft report. A completed management action plan to address the recommendations will be included in the report. The cover note to the final draft report should:

- Clearly explain that a formal response is expected within 10 days (end date provided)
- State that report will become final once accepted or at the end of the 10 days
- Explain that the key issues may be reported to CMT and the Audit Committee.

8.2 The Principal Auditee should use this opportunity to consult managers, officers and applicable cross-departmental colleagues to ensure their awareness and agreement of report details. A final draft report may not be necessary if the Principal Auditee accepts the draft report with minor exceptions. The draft report can then be issued as a final report.

## 9. Final Report

9.1 The final audit report containing all agreed recommendations and actions will be distributed within 10 days of receiving agreement to the final draft report to:

- the Principal Auditee (should ensure officers with responsibility for implementing any actions are appropriately notified)
- the relevant Assistant Director, Directorate Representative and Director
- and copied to the Assistant Director – Financial Services.

9.2 A summary of all significant final reports may be included in the progress report presented to CMT and the Audit Committee. Where appropriate, sensitive information will be protected and/or reported in the confidential section to the Committee.

9.3 Internal Audit will issue a quality control questionnaire with the final report for the Principal Auditee to complete. The Principal Auditee should return the questionnaire to the Head of Internal Audit within 5 working days from receipt of the final report. Internal Audit will analyse the survey returns and discuss expressed concerns with appropriate officers and the Assistant Director – Financial Services.

9.4 The survey will be tracked and comments may be reported to the Audit Committee, as part of Internal Audit's performance management system.

9.5 The Head of Internal Audit will escalate unresolved issues raised in surveys and non-returned surveys with applicable officers, Assistant Directors and Directors and these will be reported to the Audit Committee.

9.6 The audit process is documented as a flowchart at Appendix A.

## 10. Audit 'Opinions'

10.1 Reports will include an 'opinion' on the adequacy of controls in the audited area. There are four opinions in use:

| Opinion | Level of Assurance | Implications on systems of internal control |
|---|---|---|
| **Full Assurance** | High | • Good controls<br>• Low risk of not meeting objectives<br>• Low risk of fraud, negligence, loss, damage to reputation |
| **Adequate Assurance** | Medium | • Adequate controls<br>• Medium/Low risk of not meeting objectives<br>• Medium/Low risk of fraud, negligence, loss, damage to reputation |
| **Limited Assurance** | Medium/Low | • Limited controls<br>• Medium risk of not meeting objectives<br>• Medium risk of fraud, negligence, loss, damage to reputation |
| **No Assurance** | Low | • Inadequate controls<br>• High risk of not meeting objectives<br>• High risk of fraud, negligence, loss, damage to reputation |

The 'opinion' will impact upon the circulation of the report and what, if any follow-up work is necessary. 'Limited & No Assurance' reviews that exhibit significant control risks will be distributed to the appropriate level of management to ensure immediate action to address recommendations. The Audit Committee may request responsible officers to update them on implementation of actions within committed timescales.

## 11. Implementation of recommendations

11.1 All managers have the responsibility to implement internal and external audit agreed recommendations within timescales, hence the importance of agreeing practical and realistic recommendations. **It is the responsibility of the manager to inform Internal Audit of completed actions. Internal Audit will then undertake a follow-up as and when necessary.**

11.2 Audit reports will contain a management action plan with recommendations prioritised as:

High risk (1 – 3 months implementation period)
Medium risk (1 – 6 months implementation period)
Low risk (1 – 12 months implementation period)

The Principal Auditee should return the completed action plan within ten days of receiving the draft report.

11.3 Internal Audit will track the implementation of recommendations and will use the information as part of their follow-up work and audit planning. CMT and the Audit Committee will receive reports on outstanding recommendations, as part of a progress report.

## 12. Follow-up arrangements

12.1 Follow-up review involves Internal Audit ensuring management have given proper consideration to audit reports, and recommendations have been implemented within appropriate timescales. Internal Audit will undertake follow-ups for high-risk, 'unsatisfactory' reviews, and reviews that warrant follow-ups. These follow-ups may be undertaken as part of a full audit. The report will be brief, focusing on the progress on audit recommendations, and providing one of the following opinions:

- 'Good' Progress has been made (all recommendations are fully implemented) – Level of assurance is high as risk to controls is minimal.
- 'Satisfactory' Progress has been made (most recommendations implemented) – Level of assurance is medium as risk to controls is low.
- 'Unsatisfactory' Progress has been made (most recommendations have not been implemented or limited progress) – Level of Assurance is low as risk to controls is high

12.2 Draft follow-up reports will be issued and exit interviews offered to the Principal Auditee, who will have 10 working days to respond before the report is finalised and issued.

12.3 Internal Audit will report key issues arising from follow-up reviews to CMT and the Audit Committee, as part of its progress report.

12.4 A brief is not required for a follow-up review. However; the Auditor should make appropriate arrangements with the Principal Auditee before the start of the review.

## 13. Fraud and Investigations

13.1 Management is responsible for managing the risks associated with fraud and corruption, including the introduction and implementation of effective control arrangements to help prevent and detect fraud and corruption.

13.2 Senior Officers, managers, staff, members and the public are encouraged to report attempts to defraud the Council. The Council's Confidential Reporting (Whistle Blowing) Policy details the rights afforded to individuals who suspect and report fraudsters. The Council's fraud response plan (to be determined) clarifies the role of Internal Audit, managers and staff in responding to fraud matters.

13.3 Fraud investigations (excluding those arising from Housing Benefit fraud) may start with the submission of a brief from Internal Audit to the appropriate manager. The brief will state the objectives, scope of the investigation, and audit resource requirement. The impact of the Regulation of Investigatory Powers Act (RIPA) and the Human Rights Act will be taken into account. Field work will be undertaken in accordance with the brief and the reporting framework identified in the brief.

13.4 Proactive fraud work will be undertaken on assessed risks. It is likely that officers may not be aware that a proactive investigation is in progress.

13.5 Reports will be confidentially delivered to the following officers, depending on the level of investigation and degree of involvement:

- Officer(s) commissioning the work – First draft, Final draft and Final reports
- Appropriate officer(s) who may need the information in areas like Legal, and Human Resources – Final draft & Final report (as appropriate).
- Assistant Director – First draft, Final draft and Final report (as appropriate)
- Responsible Director and Assistant Director – Financial Services – First draft, Final draft and Final report (as appropriate)

13.6 Internal Audit maintains a special investigations log for quality assurance and monitoring purposes. The Head of Internal Audit will review the log and report activities to the Assistant Director – Financial Services The Audit Committee will receive appropriate progress reports on the fraud activities.

## 14. Consultancy work

14.1 Managers and staff can make brief enquiries about audit matters through Internal Audit as ad-hoc advice. Enquiries that require more audit time will be classified as ad-hoc consultancy.

14.2 The Head of Internal Audit approves ad-hoc consultancy work. It is possible for an advice or consultancy to turn into an audit review, if the Auditor and the Head of Internal Audit feel that internal controls are compromised.

14.3 Although Auditors will provide consultancy advice, they must remain independent of operational activities. Objectivity is presumed impaired, if Auditors review activities which they have operational responsibilities.

## 15. Escalation procedure

15.1 Where disagreements, deadlines and timescales on processes and reporting arrangements are not met, and agreement on alternative processes cannot be reached, the following escalation procedures will be adopted:

a. **Stage 1:**

Reminder telephone call (or email) to be made to Auditee highlighting the fact that escalation procedures will be used if an appropriate response is not received 10 working days from this notification (follow up with e-mail to be sent for audit trail).

b. **Stage 2:**

If the matter is not resolved in Stage 1, the Auditor will send an e-mail/ telephone call to the Auditee highlighting the information/appointment requested and copied to the relevant Manager/Directorate Representative. The Auditee has 10 days to respond to Audit's request.

c. **Stage 3:**

If there is no response to Stage 2, Internal Audit will inform the Assistant Director (Auditee copied) via e-mail and/or telephone call after 10 working days following Stage 2 notification.

d. **Stage 4:**

If requested information/appointment is not received 10 working days following notification at Stage 3, Internal Audit will inform the applicable Director via e-mail (applicable Assistant Director and Assistant Director – Financial Services copied).

e. **Stage 5:**

The Assistant Director – Financial Services /Head of Internal Audit will progress disagreements that have gone through Stages 1 – 4 without a resolution to the Chief Executive.

15.2 At any stage, reasonable extension of deadline dates and resolutions to issues can be agreed where possible and where valid reasons exist. However, any

significant delays may be noted in the final report (with summaries reported to CMT and the Audit Committee).

15.3 If Auditees are concerned that Internal Audit has not followed the procedures or met the deadlines outlined in this protocol, they should initially raise their concerns with their Directorate Representative and the Head of Internal Audit, to try and reach an agreement on the way forward.

## 16. Performance Management

16.1 Internal Audit, in addition to its quality assurance process, will use a set of agreed Key Performance Indicators to assess the effectiveness and efficiency of audit services. The Director of Customer and Shared Services, CMT and the Audit Committee will receive progress reports on the indicators. This ensures that Internal Audit meets its first priority : Audit plan completed in accordance with CIPFA codes of practice

Table 1: Key Performance Indicators

| KPI | Definition | Target |
|---|---|---|
| KPI 01 | Percentage of total audit days completed. **Compute, Total number of audit days completed to final stage plus days spent on fraud work/Total number of planned audit days** | **80%** |
| KPI 02 | Percentage of the total number of planned reviews completed. **Compute, Total number of audit reviews completed to final stage/Total number of planned reviews** | **80%** |
| KPI 03 | Time taken to complete an audit within the planned time budget **Compute, Total number of audit reviews completed/ Total number of planned reviews completed within budget** | **80%** |
| KPI 04 | Time taken to return draft reports: Percentage of reviews where the first draft report was returned within 10 available working days of receipt of the report from the Auditor. **Compute, number of days between the conclusion of the second exit interview and receipt of report from Principal Auditee, with completed management action plan.** | **80%** |
| KPI 05 | Time taken to issue a final report: Percentage of reviews where the final report was issued within 10 available working days of receipt of the response agreeing to the formal report. **Compute, number of days between response to the final draft report and distribution of a final report.** | **80%** |
| KPI 06 | Overall customer satisfaction - Survey Forms Assessed. **Compute, the total number of survey forms collected to total number of survey forms distributed, and results analysed.** | **80%** |

## 17. Risk Management

17.1 There is a strong link between Internal Audit and Risk Management. The responsibility for risk management lies with the Chief Executive, and is

delegated to the Assistant Director – Strategy and Performance. Effective links between Internal Audit and Risk Management will enhance service delivery.

17.2 Internal Audit and Risk Management, as mechanisms for controlling risks that threaten the assets and objectives of the Council, form a complementary and valuable partnership. Audit Managers will hold frequent meetings with risk management staff and directorates on audit and risk management issues.

## 18. Audit Committee

18.1 Internal Audit must report to those charged with governance. The Audit Committee is the member body with responsibility of monitoring the work of internal and external audit. Its purpose as stated in its terms of reference is:

*"The purpose of the Audit Committee is to provide independent assurance on the adequacy of the risk management framework and the associated control environment, independent scrutiny of the Authority's financial and non-financial performance to the extent that it affects the Authority's exposure to risk and weakens the control environment, and to oversee the financial reporting process. Where the Authority risk is extended into partnerships with other Authorities and contracts with suppliers, then the Committee will be empowered to request the attendance of the third parties to provide an entire picture of both audit and risk."*

18.2 Progress reports on the work of Internal Audit will be frequently provided to the Audit Committee. Directorates should send representatives to Audit Committee meetings to respond to Members concerns pertaining to their service area.

18.3 The Head of Internal Audit will maintain a positive and professional working relationship with the Audit Committee to ensure the right balance in:

- meeting its terms of reference
- the Committee's role in reviewing the performance of Internal Audit and Risk Management
- the Committee's role in handling the results of Internal Audit work
- the provision of appropriate support and adequate training for members
- using the Assistant Directors' skill and knowledge to shape the Committee's work programme.

## 19. Relationship with Partners/Contractors

19.1 A portion of the processes which deliver key services or generate fundamental information for the Council are operated through or by contractors or partners, as independent, external parties. To form an opinion upon the adequacy of both control arrangements and quality/integrity of data for those areas delivered under the contract or Partnership, the Councils Auditors (Internal and External) must seek and obtain adequate assurance.

19.2 The Head of Internal Audit must review the processes that are in place to ensure that the governance arrangements of contracts or partnerships are sound and provide for a clear definition of responsibilities. They must also be satisfied that clear arrangements have been established to determine, irrespective of which organisation provides the Internal Audit service, rights of access to the staff, systems and information of the governing body of partnerships. Partnerships should adhere to the Constitution and Financial Procedures of the Accountable Body.

19.3 Internal Audit can derive assurance in a number of ways:

- by audit of the contract management, monitoring and performance measurement processes
- by audit of inputs to outputs i.e. treating the contracted area like a "black box" and auditing both ends of the process
- through audit of the systems and processes operated by the Contractor. This may involve interviews, obtaining of documents and examination of systems or records and is more akin to an in-house audit.
- from reliance placed upon Contractor's own review and assurance mechanisms and processes where they exist (for example where there are audit or other internal risk assessment processes in place)

19.4 Internal Audit will seek to use all the four options identified in 19.3 to discharge their responsibilities. In addition, it will use the audit process outlined for CBC services to undertake reviews with Contractors however; it will agree briefs and distribute reports only with CBC Contract Managers. Internal Audit advocates CBC Contract Managers share audit findings and recommendations with Contractors, to foster service improvement and strengthen controls.

19.5 Guiding principles for partnerships:

- The partners are committed to an open and constructive working relationship
- Information will be treated as confidential within the partnership and will not be withheld unreasonably
- The partners have a common goal of ensuring that unnecessary and unproductive elements of process are eliminated whilst maintaining adequate and visible control mechanisms
- Developments should be jointly owned and adequately discussed with all relevant parties and understood prior to implementation

19.6 The detailed audit arrangements around the Service Level Agreements with Bedford Borough Council have been agreed and are reflected in the Internal Audit Protocol between Central Bedfordshire and Bedford Borough Councils.

## 20. Relationship with External Agencies

20.1 The Audit Commission (The Commission) as the Council's External Auditors need to place reliance on the work of internal audit. The Commission reviews

the adequacy and work of internal audit on an annual basis. The Commission and Internal Audit have agreed a 'managed audit' protocol that establishes audit arrangement between CBC's Internal Audit Service and the Audit Commission.

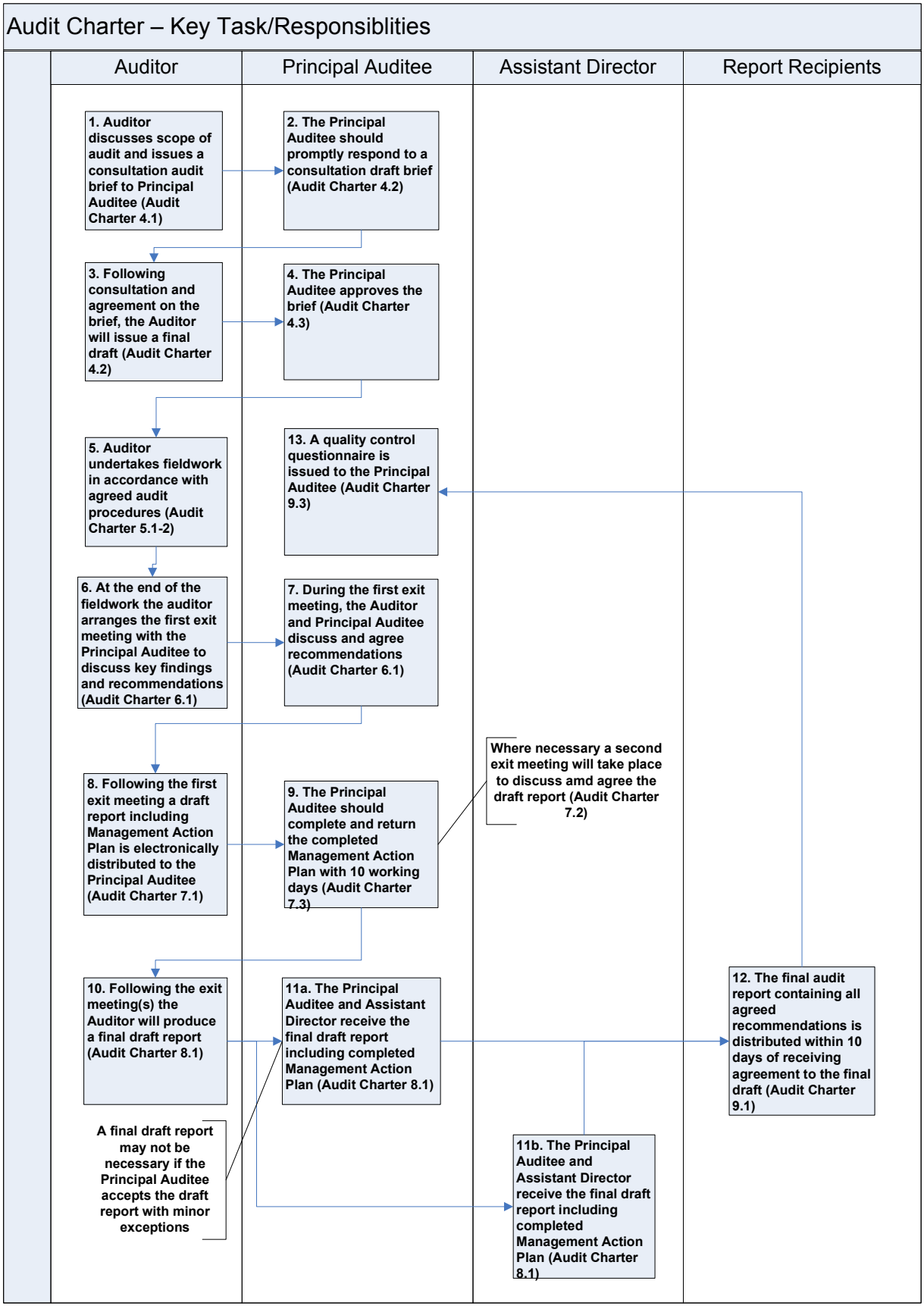
20.2 Although Internal and External Audit have different roles and priorities there can be common objectives. Good co-operation is essential in order to minimise duplication of effort and maximise the benefits of working together. Effective co-operation should enable both parties to devote more time to the key issues facing the authority and ensure that the Council gets maximum value for its total audit resource.

20.3 The protocol includes regular liaison meetings between senior officers in CBC and the Commission. CBC managers should forward any concerns to their Directorate Representative or the Head of Internal Audit for discussion at liaison meetings.

20.4 Internal Audit will liaise with other internal review functions and obtain their reports for information, for review and for comment where proposals may affect internal control arrangements and the risks facing CBC.

20.5 Internal Audit will liaise with other external review agencies (such as the Police, DWP and Inland Revenue) where activities may affect internal control arrangements and the risks facing CBC. Internal Audit will start considering the work of external inspection bodies. The Head of Internal Audit will seek to foster constructive working relationships with such inspection bodies, particularly where Internal Audit reviews are undertaken on, or may be relevant to, the area under inspection, and vice versa. Internal Audit should receive copies of all reports issued to the authority and take these reports into account when considering the risk assessment and audit work as part of the audit planning process, with a view to avoiding duplication of work while ensuring relevant risks are considered.

APPENDIX A


Audit Charter – Key Task/Responsiblities
Auditor
Principal Auditee
Assistant Director
Report Recipients
1. Auditor discusses scope of audit and issues a consultation audit brief to Principal Auditee (Audit Charter 4.1)
2. The Principal Auditee should promptly respond to a consultation draft brief (Audit Charter 4.2)
3. Following consultation and agreement on the brief, the Auditor will issue a final draft (Audit Charter 4.2)
4. The Principal Auditee approves the brief (Audit Charter 4.3)
5. Auditor undertakes fieldwork in accordance with agreed audit procedures (Audit Charter 5.1-2)
13. A quality control questionnaire is issued to the Principal Auditee (Audit Charter 9.3)
6. At the end of the fieldwork the auditor arranges the first exit meeting with the Principal Auditee to discuss key findings and recommendations (Audit Charter 6.1)
7. During the first exit meeting, the Auditor and Principal Auditee discuss and agree recommendations (Audit Charter 6.1)
Where necessary a second exit meeting will take place to discuss amd agree the draft report (Audit Charter 7.2)
8. Following the first exit meeting a draft report including Management Action Plan is electronically distributed to the Principal Auditee (Audit Charter 7.1)
9. The Principal Auditee should complete and return the completed Management Action Plan with 10 working days (Audit Charter 7.3)
10. Following the exit meeting(s) the Auditor will produce a final draft report (Audit Charter 8.1)
11a. The Principal Auditee and Assistant Director receive the final draft report including completed Management Action Plan (Audit Charter 8.1)
12. The final audit report containing all agreed recommendations is distributed within 10 days of receiving agreement to the final draft (Audit Charter 9.1)
A final draft report may not be necessary if the Principal Auditee accepts the draft report with minor exceptions
11b. The Principal Auditee and Assistant Director receive the final draft report including completed Management Action Plan (Audit Charter 8.1)

This page is intentionally left blank

**Meeting:** **Audit Committee**

**Date:** **27 September 2010**

## Subject: Information Governance Framework

**Report of:** Director of Customer and Shared Services

**Summary:** The report presents the Council's Information Governance Framework for approval.

Contact Officer: Clive Jones, Assistant Director Customer & Systems

Public/Exempt: Public

Wards Affected: All

Function of: Council

**CORPORATE IMPLICATIONS**

**Council Priorities:**

The implementation and continuous improvement of the Council's Information Governance systems are crucial to the safeguarding of the Council's information assets in the interests of all of its stakeholders, and as such support and indeed underpin all the priorities and objectives of the Council.

**Financial:**

None directly from this report.

**Legal:**

None directly from this report.

**Risk Management:**

The implementation of this framework is intended to reduce the risks related to, and occurrences of information governance incidents that the Council is exposed to. This will be achieved through the specification, implementation, monitoring and improvement of the policies identified within the framework.

**Staffing (including Trades Unions):**

None directly from this report.

**Equalities/Human Rights:**

None directly from this report.

**Community Safety:**

None directly from this report.

**Sustainability:**

None directly from this report.

**RECOMMENDATIONS:**

**that the Audit Committee approves the Information Governance Framework.**

## Background

1. Central Bedfordshire Council acknowledges that information is a valuable asset. It is therefore wholly in the Council's interest to ensure the information it holds, in whatever form, is appropriately governed, in terms of protecting the interests of all its stakeholders.

2. The Council is bound by UK legislation, including but not limited to:
   - the Data Protection Act;
   - the Public Sector Information Regulation; and
   - the Regulation of Investigatory Powers Act,

   The Council is also bound by regulations governing:
   - the code of connection to Government networks (GCSx CoCo); and
   - the storage or transmission of payment cardholder information (PCI-DSS).

3. The Council is responsible for ensuring a system of internal controls are in place to manage the Council's information assets, which help protect the interests of all its stakeholders and meets UK legislation and regulations. To help ensure that the system is functioning correctly the Council must set in place policies, standards and guidelines. The System is overseen by the Council's Information Governance Steering Group which is responsible for appraising and reporting on the efficiency, effectiveness and performance of the information management controls. This Group is chaired by the Council's Senior Information Risk Officer (SIRO) - the Director of Customer and Shared Services .

4. The Information Governance Steering Group have documented, within the Council's Information Governance Framework, the system of internal controls and the management system to: plan, monitor, verify and improve the system.

## Information Governance Framework

5. The Information Governance Framework is a set of high level statements of how the Information Governance system will be delivered to meet the needs of the Council.

6. The framework sets out the approach adopted by the Council and will be reviewed and updated, as appropriate, on a yearly basis.

7. The framework provides details of:
    - the applicable legislation and regulations which the Council is bound by;
    - the management system defined to help ensure continuous improvement of the Information Governance Framework and its underlying components;
    - the role of the Senior Information Risk Officer (SIRO), and key responsibilities of the role;
    - the role of an Information Asset Owner, and key responsibilities of the role; and
    - the structure of the Information Governance Framework, including which policies, standards and procedures each Service area have responsibility for providing, monitoring and maintaining.

8. The framework has been developed with contributions and the support of the following Service areas:
    - Information and Records Management;
    - Performance Management and Data Quality;
    - Information Security Incident Management;
    - ICT;
    - Properties and Facilities Service;
    - Human Resources;
    - Risk Management including Audit and Assurance; and
    - Legal.

**Conclusion and Next Steps**

9. Approval by the Audit Committee of the Council's Information Governance Framework will ensure that the Information Governance Steering Group can progress its work inline with the agreed approach.

10. The Audit Committee will then be able to use the agreed Information Governance Framework to monitor the work related to the continuous improvement of the Council's Information Governance practices to ensure that appropriate assurance is provided on the Council's internal governance system.

**Appendices:**
Appendix A – Information Governance Framework

This page is intentionally left blank

NOT PROTECTED

# Central Bedfordshire Council

# Information Governance Framework

Version [1]

**Document sign-off**

| Owner | Role | Signature | Date | Version |
|---|---|---|---|---|
| Richard Ellis | Director of Business Transformation - Senior Information Risk Owner | | | |
| | | | | |

**Approval History**

| Version No | Approved By | Approval Date | Comments |
|---|---|---|---|
| | | | e.g. approved at IGSG meeting on dd/mm/yyyy |
| v | | | |

**Revision History**

| Version No. | Revision Date | Summary of Changes | Author |
|---|---|---|---|
| v0d8 | 14/01/2010 | 1st draft issued to IGSG for comment | Dave Jones |
| v0d9 | 08/03/2010 | 2nd draft issued to IGSG for comment<br>▪ added target completion dates for incomplete policies,<br>▪ completed section on Legal Service,<br>▪ added guidance on IGF roll out approach including readership and training needs. | Dave Jones |
| v0d10 | 05/07/2010 | 3rd draft issued to EM and CJ final comments prior to sign-off.<br>▪ ,added reference to the Human Rights Act 1998,<br>▪ added reference to RIPA 2000,<br>▪ updated wording of data quality and performance governance controls,<br>▪ removed IGSG membership structure chart,<br>▪ re-sequenced Appendices<br>▪ corrected typos. | Dave Jones |
| v1 | 06/08/2010 | Accept changes recommended by Elaine Malarky | Dave Jones |

**Document Author**

| Version | Authors | Role |
|---|---|---|
| v0d8 | Dave Jones | ICT Service Assurance & Improvement Manager |
| v0d8 | Rob Hutton | Principal Information Risk Officer |
| v0d8 | Peter Badger | ICT Security Manager |
| v0d9 | Dave Jones | ICT Service Assurance & Improvement Manager |
| v0d10 | Dave Jones | ICT Service Assurance & Improvement Manager |
| v0d11 | Elaine Malaky | Head of Planning and Programme Management |
| v1 | Dave Jones | ICT Service Assurance & Improvement Manager |

**Document Governance**

| | |
|---|---|
| **Next Review Date** | This document will be reviewed annually or inline with changing business requirements.<br>This process will be audited as per the Information Security Management Systems audit schedule. |
| **Include in Publication Scheme (Y/N)** | |
| **Publish to Web (Y/N)** | No, Intranet only |
| **Circulation** | This framework is to be made available to all CBC staff and observed by all members of staff, both social care and otherwise.<br>There will be an ongoing professional development and educational strategy to accompany the implementation of this framework. |
| **Information Classification** | **NOT PROTECTED** |

The current version of the Central Bedfordshire Council's Information Governance Framework is available from the CBC intranet at *<insert hyperlink here>*

Alternatively, a copy can be obtained by writing to the Principal Information and Records Officer at:

Central Bedfordshire Council
Priory House
Chicksands
Shefford
SG17 5TQ

# Table of Contents

# 1 Introduction

This document (the Central Bedfordshire Council Information Governance Framework) forms the basis of how Information Governance is structured at Central Bedfordshire Council (CBC), how Information Governance related policies, procedures and guidelines are structured and how the various Directorates and Services are aligned to support Information Governance at CBC. Appendix A contains a diagram of the Information Governance Framework.

Information Governance within CBC is overseen by the Information Governance Steering Group. The Terms of Reference for the Information Governance Steering Group (IGSG) can be found on the CBC intranet. A list of current members of the IGSG can be found on the Information Management pages on the CBC intranet.

Information Governance is many things to many people. Central Bedfordshire Council (CBC) views this as:

- the cornerstone of information management and information security management.
- key to ensuring the Central Bedfordshire Council comply with current legislation, regulation and best practice appropriate to local government, in relation to the creation, handling, storage, security and processing of information.
- allows organisations and individuals to ensure 'Protected' and 'Restricted' information is appropriately identified and dealt with legally, securely, efficiently and effectively.
- provides a platform to initiate User Awareness and training programmes to ensure staff, contractors and 3rd parties are aware of their Information Governance responsibilities.
- The Information Governance Framework (IGF) sets out the structures that are in place to govern the Information Management and the Information Security Management processes including; the policies and procedures that must be put in place to safeguard the council.
- The IGF clearly states the 'Standards' that Central Bedfordshire Council will adopt or work towards adopting to continually improve Information Governance.
- Clearly defines the measures that the council has adopted (KPIs and PI) to report the effectiveness of the Information Governance process.

Information Governance has eight fundamental aims:

- To ensure accountability, the Council will ensure that there is a senior executive who will oversee the information management approach and delegate programme responsibility to appropriate individuals, adopt appropriate policies and procedures to guide personnel, and ensure programme audit ability.
- To ensure integrity of information, an information management programme will be constructed so that information and records generated or managed by, or for, the Council have reasonable and suitable guarantee of authenticity and reliability.
- To ensure that information is protected, the information management programme will ensure that the appropriate level of consideration is given to provide a reasonable level of protection to all information and records especially those that are identified as Protected, Restricted, or are essential to business continuity.
- To ensure that information held meets relevant compliance requirements - the information management programme will be constructed to comply with applicable laws and other binding authorities, as well as the Councils policies.
- To ensure that information is available, the organisation will maintain information and records in a manner that ensures timely, efficient, and accurate retrieval of needed information.
- To ensure that information is transparent, the processes and activities of the Council's information management programme will be documented in an understandable manner and be available to all personnel and appropriate interested parties.
- To ensure that information is retained consistently the Council will maintain its records and information for an appropriate time, taking into account; legal, regulatory, fiscal, operational, and historical requirements.
- To ensure that any disposal of information is carried out correctly, the Council will provide secure and appropriate arrangements for information that is no longer required by any applicable laws and or the council's policies.

The Information Governance framework encompasses:

- Data Protection Act 1998
- Access to Information legislation
    - Freedom of Information Act 2000, including the Council's 'Publication Scheme'
    - Public Sector Information Regulation 2005
    - Environmental Information Regulation 2004

- Regulation of Investigatory Powers Act 2000,
- Human Rights Act 1998, article 8,
- Information and Records Management
- Information Security Management System
- Information Governance Management

## 2 Plan/Do/Check/Act (PDCA) Model

The following review model has been adopted by Central Bedfordshire Council to ensure continuous improvement of the Information Governance Framework:

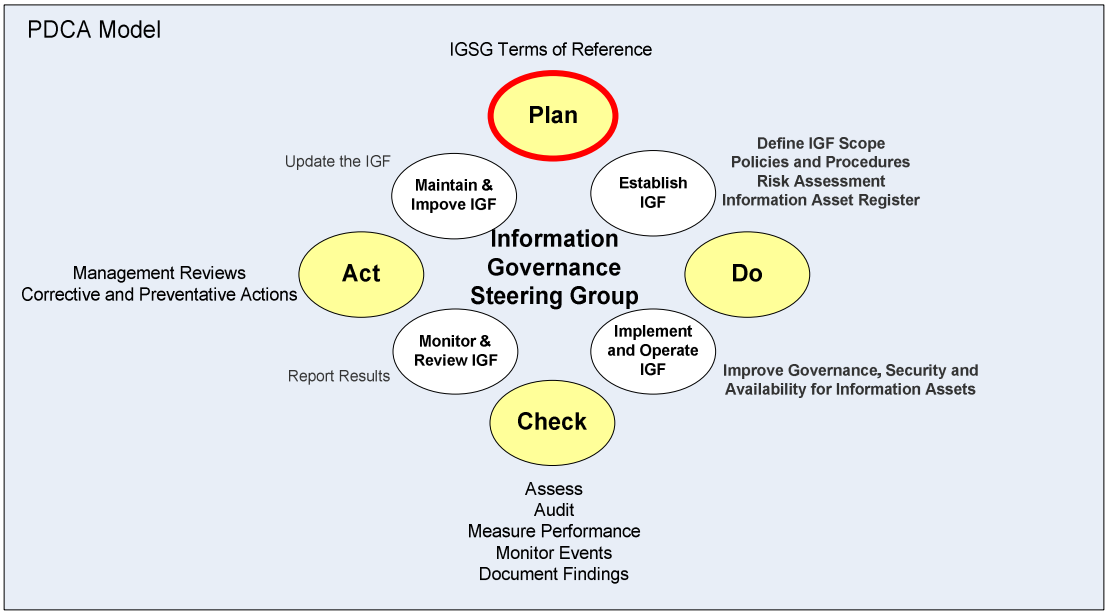



Figure 1 – PDCA Model

**Plan** (establish the IGF)
Establish policies, objectives, targets, processes and procedures relevant to managing risk and improving information governance to deliver results in accordance with CBC's overall policies and objectives.

**Do** (implement and operate the IGF)
Implement and operate policies, controls, processes and procedures.

**Check** (monitor and review the IGF)
Assess and, where applicable, measure process performance against policies, government performance indicators, objectives and practical experience. Report the results on a monthly basis to management for review.

**Act** (maintain and improve the IGF)
Take corrective and preventive actions, based on the results of the management review, to achieve continual improvement of the information governance framework.

# 3 Role of the Senior Information Risk Officer (SIRO)

The SIRO has been appointed by the Chief Executive.

The SIRO is fully aware of how the strategic business goals of the Council may be impacted by information risks.

The SIRO acts as an advocate for information risk on the Council's Management Team (CMT) and in internal discussions, and provides written advice to the Chief Executive Officer on the content of their Annual Governance Statement in regard to information risk.

Working within a simple governance structure, with clear lines of ownership and well defined roles and responsibilities, the SIRO provides an essential role in ensuring the identified information security threats are followed up and incidents managed.

The SIRO also ensures that the Board and the Chief Executive Officer are kept up-to-date on all information risk issues.

The SIRO is responsible to the Board for ensuring that all Information risks are recorded and mitigated where applicable. The SIRO is responsible for ensuring that all record management issues (including electronic media) are managed in accordance with this policy.

The SIRO will chair the Information Governance Steering Group (IGSG) which is responsible for initiating, developing and monitoring the delivery of information governance in Central Bedfordshire Council as part of the Council's corporate information management ???.

The role is supported by Information Asset Owners (IAOs)[1], the Risk Manager; the Principal Information Records Officer, the ICT Security Manager and the Caldicott Guardian, although ownership of the Information Risk Policy and risk assessment process remains with the SIRO.

Please refer to Appendix B for a description of the Information Asset Owner (IAO's) role.

The SIRO is responsible for the appointment and management (in terms of information assets) of the IAO's. Information Asset Owners are senior individuals involved in running the Council. Their role is to understand and address risks to the information assets they or their team(s) 'own' and to provide assurance to the SIRO on the security and use of those assets.

The IAOs (in consultation with the SIRO) are responsible for appointing Information Asset Administrators (IAAs). Information Asset Administrators ensure that policies and procedures are followed, recognise actual or potential

[1] The Council has determined that the IAOs role will be at Head of Service (HoS) level within the organisation.

security incidents, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date.

# 4 Structure of the Information Governance Framework

The main functional areas within CBC that fall within the framework are:

- Information & Records Management
- Performance Management and Data Quality
- Information Security Incident Management
- ICT Services
- Properties & Facilities Services
- Human Resources Services
- Risk Management, including Audit and Assurance
- Legal Services

The Information Governance Framework is guided by the Council's Corporate Strategy and Directorate Plans.

Measurements of effectiveness of every relevant function and control within the overall Information Governance Framework, will be through KPIs and PIs which will be reported upon on a regular basis. A programme of continuous improvement will also be implemented.

An audit and assurance programme will be devised and implemented to ensure the ongoing effectiveness and compliance of the Terms of Reference, this framework document and best practice standards, such as ISO27001:2005, BS15489 and BS25999.

## 4.1 Information & Records Management

Having accurate, relevant and accessible information, both current records and archives, is vital to the efficient management of the Council, which values recorded information as an important corporate asset. The Council must meet its statutory obligations in this area, making 'proper arrangements' for its records, both for its own good governance but also so as to provide the public with access to information. In doing this it will seek to be open and responsive with access to information whilst meeting its duties of confidentiality in relation to personal and commercially sensitive records and information.

This requires the Council to create and manage all its recorded information, irrespective of its medium and position in its managed lifecycle, efficiently, make them accessible when needed, protect and store them securely and dispose of them safely at the appropriate time.

In relation to its semi-current hard copy recorded information and archives, these functions are provided by Bedford Borough Council through a Service Level Agreement (SLA) following Local Government Reorganisation and the creation of Central Bedfordshire Council in 2009.

The Bedfordshire and Luton Archives and Records Service, the subject of the SLA, is a scheduled Place of Deposit for Public Records and also provides a joint arrangement service to Luton Borough Council for both Archives and Records Management.

Please refer to Appendix C for a list of relevant Information & Records Management policies, procedures and guidelines.

The Council (seeks to at all times comply) complies with all relevant legislation (refer to Appendix D) and aims to achieve high standards of best practice. This includes the adoption of principles from recognised bodies such as the British Standards Institute (BSI) and the International Organisation for Standardisation (ISO). In respect of the Service Level Agreement for the provision of Archives and Records Management Services discharged by Bedford Borough Council are concerned, this involves an agreed set of arrangements for governance, monitoring, performance, issue management, and compliance and a series of scheduled Service Level KPIs – see below.

| Service Level PI ref. | Service Key Performance Indicator (KPI) |
|---|---|
| SER1 | Overall performance in national assessment by The National Archives – this includes the following areas: governance, documentation of collections, access and outreach services, preservation and conservation, buildings, security and environment |
| SER2 | Charter Mark accreditation |
| SER3 | Customer satisfaction in national surveys of users |
| ARR1 | Performance in national assessment by The National Archives |
| ARR2 | National accreditation as Place of Deposit for Public Records |
| ARR3 | Volumetric intake of corporate records from each partner |
| ACC1 | Visitor provision – performance against Service Charter targets |
| ACC2 | Remote enquiry provision (written) |
| ACC3 | Remote enquiry provision (telephone) |
| ACC4 | Website pages |
| ACC5 | Website hits |
| ACC6 | Retro-digitisation of lists and related indexing |

| | |
|---|---|
| ACC7<br>ACC8 | Website content development |
| ACC9 | Outreach work |
| ACC10 | Information management<br>• Electronic Records Management linked with…<br>• Digital Preservation |

### 4.2 Performance Management & Data Quality

Central Bedfordshire Council takes the quality of its performance data very seriously. We aim to ensure that our decision makers are provided with information that is fit for purpose and is used to support the decision making process.

Having reliable, accurate and timely information to support decision making and manage services is essential. Data must be fit for purpose and represent an organisation's activity in an accurate and timely manner. This will give us confidence in the decisions we make as a result.

We spend a great deal of time and money on the activities and systems involved in collecting and analysing the data that underpins information at the Council. It is therefore absolutely essential that we should have confidence in the data we produce as increasing reliance is placed on the information that comes from it and it enables us to demonstrate our improvement. It is essential that the responsibility for data lies with all staff that input, store, retrieve or otherwise manage data to ensure that it is of the highest quality.

Our vision for data quality is that we get it right first time, every time. This is vital to the delivery of our Strategic Plan and the monitoring of the actions and target milestones contained in it. We must continue to be robust about demonstrating improvement in our performance as it will give us a level of confidence when providing this information to Government auditors and inspectors and other external assessors.

Data quality in relation to Central Bedfordshire Council's performance indicators is monitored and reported regularly during the year and any concerns regarding the quality of any performance data will be addressed and resolved.

Data used for performance information is subject to proportionate verification to check accuracy, validity, reliability, timeliness, relevance, completeness and security. This underpins the Data Quality Strategy.

Please refer to Appendix E for a list of relevant Performance Management & Data Quality policies, procedures and guidelines.

### 4.3 Information Security Incident Management

The purpose of information security incident management is to ensure information security events, and weaknesses associated with information systems, are communicated in a manner allowing timely corrective action to be taken, and to ensure a consistent and effective approach is applied to the management of all reported information security incidents.

Formal information security event reporting and escalation procedures are in place. All employees, contractors and contracted third parties are aware of the procedures for reporting information security incidents and potential weaknesses that could have an impact on the security of Council's information assets.

All employees, contractors and contracted third parties are required to report any information security incidents and weaknesses as quickly as possible to the ICT Service Desk.

Responsibilities are assigned and procedures are in place to handle information security incidents and to assess weaknesses effectively once they have been reported. A process of continual improvement is applied to; protective monitoring, incident evaluation and response, incident containment, eradication and recovery and the overall management of information security incidents.

Please refer to Appendix F for a list of relevant information security incident management documents, procedures and guidelines.

### 4.4 ICT Service

Central Bedfordshire Council acknowledges that information is a valuable asset, it is therefore wholly in its interest to ensure that the information it holds, in whatever form, is appropriately governed, in terms of protecting the interests of all its stakeholders.

The purpose of the Central Bedfordshire Council ICT Acceptable Use Policy (CBC ICT AUP) and other ICT security policies, standards and baselines which govern how the Council's technology is deployed and managed is to ensure that information assets are reliably protected. The policies, standards and baselines apply to all employees, members, contractors and third parties at any location with access to CBC's computing resources and information.

ICT Security and Information security is the responsibility of every employee, member, contractor and authorised 3rd party.

The Council reserves the right to monitor ICT use for compliance with their ICT security policies. Consequences of ICT security policy violations may lead to disciplinary action against employees and the termination of contracts under which contractors and third parties provide services to CBC.

Please refer to Appendix G for a list of relevant policies, procedures and guidelines which when combined govern CBC ICT Systems and their use. These are categorised into:

- ICT End-Users Security Policies, such as the ICT Acceptable Use Policy and Members ICT Acceptable Use Policy; and
- ICT Security Management policies (which govern how ICT Services are implemented and managed)

### 4.5 Properties & Facilities

The Properties and Facilities service has responsibility for delivering various services to the Council in relation to Information Governance, in particular providing a secure environment in which Council staff and members can work.

The Service ensures that each council building is appropriately physically secured and ensures safety systems are in place and operational, including fire alarms.

At the Council's main buildings access control systems have been implemented to control who has access to various parts of each building and at which times of day they have access. The Service issue security passes, for the access control system, to permanent staff and authorised contractors and will revoke access for people when they leave. The Service also provides reception security staff that sign visitors in and out of the buildings and issue visitor passes.

The Service facilitates the provision of additional levels of security to ensure specific rooms are appropriately protected, for example. ICT data centre rooms.

The Properties and Facilities service are also responsible for the implementation, management and operation of surveillance systems (e.g. CCTV), where there is a business need and for ensuring buildings are maintained at an appropriate level.

Please refer to Appendix H for a list of relevant policies, procedures and guidelines.

### 4.6 Human Resources Service

The Human Resource Service provides a range of services to support the Council directorates to achieve their goals, bringing the Council's vision to life. These include; recruitment, learning & development, workforce planning, employee relations support, provision of management information, corporate induction and setting HR policies which facilitate the retention of the right people to deliver a first class service to the residents of Central Bedfordshire.

To help protect the Council's information assets, all employees must clearly understand their security responsibilities. For some roles, these should be

addressed in the job description, but in general terms, employees will sign up to their responsibilities through their terms and conditions of employment. HR must ensure every employee has signed a contract of employment and that all employees that use ICT Services, in their role, additionally sign a declaration to comply with CBC's ICT Acceptable Use Policy (AUP).

For new starters, HR are responsible for ensuring that employees, contractors and third party users are recruited through a robust agreed process, are issued with a contract of employment, and associated ICT AUP (where appropriate). Additionally, corporate and local induction will help to ensure that all new starters clearly understand their responsibilities.

To help reduce the risk of theft, fraud, misuse of Council facilities or reputational damage to the Council and to help ensure that candidates are suitable for the role they are being recruited for, all prospective employment candidates, contractors and third party users must be appropriately background checked by HR prior to commencing their employment with CBC. The level of background checks required for each role is clearly documented in the recruitment procedures, and the process is routinely audited.

The HR team produces regular and ad hoc management information for managers, and is responsible for the accuracy, relevance and validity of that information.

HR has clearly documented procedures for managing processes in relation to starters, leavers and changes, and the associated work relating to payroll. In relation to leavers, there is a process that managers use to ensure that CBC equipment /assets, ID badges are returned, and that system access rights are removed.

HR has established policies e.g. disciplinary procedure, to ensure, in relation to information governance (in this case), that breaches in information governance or security arrangements can be dealt with appropriately. HR must also provide appropriate guidance and training to all managers to ensure the disciplinary procedure is applied consistently across the Council.

HR is also responsible for setting and overseeing policy to govern employees' behaviour whilst employed by CBC. Please refer to Appendix I for a list of relevant policies, procedures and guidelines to facilitate the governance of employees.

### 4.7 Risk Management

CBC acknowledges its ongoing responsibility to afford a high priority to the development and implementation of robust and integrated processes that will ensure that risks are identified, assessed, prioritised, managed and recorded in a consistent and holistic way, and wherever reasonably practicable, eliminated or controlled.

CBC has a Corporate Risk Management Strategy that ensures that all parts of the organisation identify and prioritise risks, and that the strategic, directorate and service level Risk Register capture risks and have mechanisms to determine acceptable levels of risk and to describe, implement and monitor mitigating and remedial actions.

CBCs Corporate Risk Management process and strategy is overseen by the Corporate Risk Management Group which is mandated to meet at least four times a year. Additional meetings can be held if considered necessary.

Please refer to Appendix J for a list of relevant strategies, policies, procedures and guidelines.

Audit & Assurance

It is the policy of Central Bedfordshire Council that aspects of the Information Governance Framework will be subject to an internal audit from time to time. Due to the size of the Council and the number of sites that it operates from this will be conducted on a rolling basis, with a number of areas being selected to be audited each year, using a risk based approach. This will help ensure that not only policies and procedures are being applied appropriately but also that changes in best practice are implemented and policies and procedures regularly reviewed and updated.

The Internal Audit Service has developed and maintains an Audit Plan, which aims to cover major risk aspects of compliance with CBC's information governance policies.

Sites and/or aspects of the IG Framework may receive an audit visit more than once in the three year period where there are deemed to be critical functions or where previous audits have revealed serious or numerous non conformities to recognised standards or best practice.

Additionally, aspects of ICT Security will be audited (by Internal Audit, external consultants etc) as part of Central Bedfordshire Council's ongoing audit process.

In addition to formal audit checks, the ICT Service works with external agencies each year to conduct assessments for compliance to the following standards and codes of connection:

- Government Connect Code of Connection (GCSx CoCo)
- Payment Card Industry Data Security Standard (PCI-DSS)

Please refer to Appendix J for a list of relevant policies, procedures, guidelines and reports which contribute to CBC Information Governance.

### 4.8 Legal Service

The Legal Services team do not directly provide policies, procedures and guidelines with respect to CBC information governance management. They do however provide a consultative service to all directorates across the council,

and will apply their legal knowledge to contribute to Council policy when requested.

# 5 Guidance on Implementation

## 5.1 Information Governance Framework - Target Audience

The Information Governance Framework must be understood by all information asset owners and also all officers of the Council that have supervisory duties, within Services that handle sensitive (Protected or Restricted) data which if mishandled could cause damage to the council.

The Information Governance Framework is an over-arching framework that aims to pull together the various components that contribute to Information Governance across the Council, so that information asset owners and line managers have a single source of reference regarding CBC's Information Governance policies.

The Information Governance Framework document is not a protected document and is accessible on the CBC intranet.

## 5.2 Information Governance Framework - Awareness Training

While safeguarding the Council's information is every council employee, contractor and member's responsibility, specific training on the Information Governance Framework is not required for all staff.

Programmes of awareness and training are run, from time to time, within each of the Services that contribute to CBC's Information Governance policies, for instance,

- HR regularly run training and briefing sessions on HR policies and procedures for new line managers and refresher sessions for existing managers (where required). These sessions are normally scheduled through the Academy website and are regularly advertised within Be Inspired.

- Staff that handle information and/or use ICT systems will receive regular awareness training, in the form of ICT AUP acceptance or Information Security awareness training (planned from summer 2010).

- The Information Records Management team are also developing plans to roll out a training programme to ensure all staff are aware of CBCs Information Handling Policies.

Consideration should be give to providing a programme of training for Information Asset Owners and line managers to ensure relevant staff are appropriately trained in policy creation, management and monitoring, to ensure the Plan / Do / Check / Act continuous improvement model is successfully implemented..

# Appendix A – Information Governance Framework Diagram

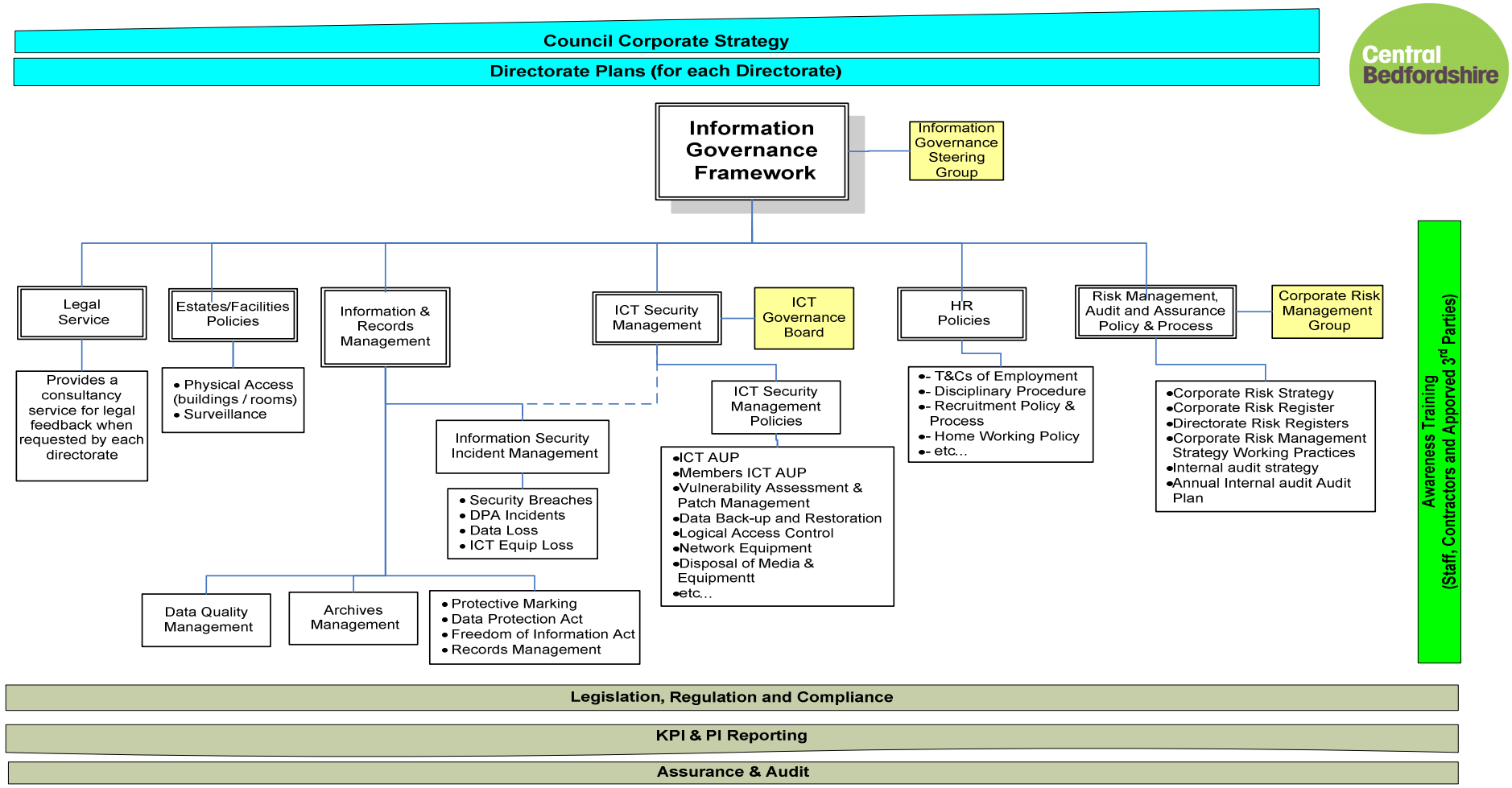



**Figure 2 – Information Governance Framework**

# Appendix B – Detail Responsibilities of the IAOs

**(Senior individuals involved in running the Council)**

To ensure the governance of Central Bedfordshire Councils information all information assets must have an owner (an Information Asset Owner – IAO).

Members of staff at Head of Service level within the Council would typically be Information Asset Owners and the role can be described as:

- To understand and address risks to the information assets they and their team(s) 'own' and provide assurance to the SIRO on the security and use of these assets (understands the Council's plans to achieve and monitor the right Information Governance culture, across the Council and with its business partners and to take visible steps to support and participate in that plan (including completing own training)).
- Knows what information the Asset holds, and what enters and leaves it and why (maintains understanding of 'owned' assets and how they are used up to date; approves and minimises information transfers while achieving business purposes; approves arrangements so that information put onto portable or removable media like laptops, USB sticks and CD/DVD roms is minimised and are effectively protected to Information Governance standards; approves and oversees the disposal mechanisms for information of the asset when no longer needed).
- Knows who has access and why, and ensures their use is monitored and compliant with policy (understands the organisation's policy on access to and use of information; checks that access provided is the minimum necessary to satisfy business objectives; receives records of checks on use and assures self that effective checking is conducted regularly).
- Responsible for the authorisation of access to the assets, including the management of any authorised 3rd parties who are granted access to the information assets (or systems that they reside in).
- Understands and addresses risks to the asset, and provides assurance to the SIRO (conducts quarterly reviews of information risk in relation to 'owned' assets; makes the case where necessary for new investment or action to secure 'owned' assets; provides an annual written risk assessment to the SIRO for all assets 'owned' by them).
- Ensures the asset is fully used for the benefit of the organisation and its customers, including responding to requests for access from others (considers whether better use of the information is possible or where information is no longer required); receives, logs and controls requests from others for access; ensures decisions on access are taken in accordance with Information Governance standards of good practice and the policy of the organisation.

## Appendix C – Information & Records Management

1. Information and Records Management Policy
2. Freedom of Information Policy
3. Data Protection Policy
4. Environmental Information Regulations Policy
5. Reuse of Public Sector Information Regulations Policy
6. Information Governance and Security Policy
7. How to use Information Guidelines
8. Service Level Agreement BBC005 for Archives and Records between Bedford Borough Council and Central Bedfordshire Council

## Appendix D – Applicable Legislation

- Data Protection Act 1998
- Data Protection (Processing of sensitive personnel data) Order, 2000
- Computer Misuse Act 1990
- Copyright Designs and Patents Act, 1998 the Copyright (Computer Software) Amendment Act
- The Obscene Publications Act
- Regulation of Investigatory Powers Act (RIPA) 2000
- The Telecommunications Act (Lawful Business Practice Regulations 2000)
- Crime and Disorder Act, 1998
- Criminal Procedures And Investigations Act, 1996
- Health & Safety at Work Act 1974
- Freedom of Information Act 2000
- Children's Act 2004
- Environmental Information Regulations, 1992
- Human Rights Act 1998
- Limitations Act 1980
- Local Authorities (Access to Information) Act 1985
- Local Government Act 1972
- Re-use of Public Sector Information Regulations 2005
- Taxes Management Act 1970
- Common Law (The rights of citizens to have their information treated as confidential is enshrined in the law of the land. Individuals may be personally liable if they contravene this law).

Principal standards affecting CBC:

- GCSx CoCo (Government Connect Code of Connectivity)
- PCI-DSS (Payment Card Industry Data Security Standard)

- HMG Security Policy Framework (SPF)
- ISO/IEC 27001/2-2005 (Information Security)
- BS 15489-1:2001 (Information and Documentation. Records Management. General)
- ISO/IEC 25999 (Business Continuity)
- DETR/LGA guidance notes on 1972 s.224 'proper arrangements' 1999
- Lord Chancellor's Codes of Practice under ss.45-46 of the FOI Act , 2002

## Appendix E – Performance Management & Data Quality

1. Performance Manual – containing the performance framework and the performance strategy, policy and action plan

## Appendix F – Information Security Incident Management

1. Information Security Incident Management Process (update drafted, sign-off expected summer 2010)
2. ICT Service Desk Policy Procedures (expected summer 2010)
3. Data Protection Policy (Ref Appendix C)

# Appendix G – ICT Service

ICT End-User Security Policies

1. ICT Acceptable Use Policy (AUP)
2. GCSx Acceptable Use Policy (AUP)
3. Members ICT Acceptable Use Policy (AUP)
4. Information Governance & Security Policy (Ref Appendix C)

ICT Security Management Policies/Standards and Processes

5. ICT Change Management Process
6. 3rd Party Remote Access Standard
7. Information Security Awareness Training
8. ICT Vulnerability Assessment & Patch Management
9. ICT Disposal of Media and Equipment
10. ICT Corporate Induction Security Awareness
11. ICT Security Incident Response (drafted, sign-off summer 2010)
12. ICT Data Backup & Restoration (drafted, sign-off summer 2010)
13. ICT Content Filtering & Malware Protection (drafted, sign-off summer 2010)
14. ICT Online Social Network (drafted, sign-off summer 2010)
15. ICT Workstation/Laptop configuration (drafted, sign-off summer 2010)
16. ICT Physical Security (drafted summer 2010)
17. ICT Penetration Testing (inc. IT Health Checks) (drafted, sign-off summer 2010)
18. ICT Logical Access Control (drafted, sign-off autumn 2010)
19. ICT Network Equipment Configuration (drafted, sign-off autumn 2010)
20. ICT Networks & Firewall Management (expected autumn 2010)
21. ICT Server Windows 2003/2008 Configuration (expected autumn 2010)
22. ICT Logging and Monitoring (expected autumn 2010)
23. ICT Cryptographic Key Management (expected autumn 2010)
24. ICT Software Acquisition and Acceptance Policy (expected winter 2010)
25. ICT Software Development Lifecycle (expected winter 2010)
26. Wireless Configuration (expected winter 2010)

## Appendix H – Properties & Facilities

1. Procedures for issuing, updating and revoking swipe cards
2. Access to buildings request form
3. Policy for granting access to building (expected December 2010)
4. Policy for Surveillance systems (e.g. CCTV) (expected December 2010)

## Appendix I – Human Resources Service

1. Terms & Conditions of Employment
2. Disciplinary Procedure
3. Recruitment Policy and Process
4. Leavers Process
5. Baseline Personnel Security Standard (BPSS) Recruitment Clearances Verification for GCSx Authorisation record
6. Home Working Policy

## Appendix J – Risk Management, Audit & Assurance

1. Corporate Risk Management Strategy
2. Corporate Risk Management Policy Statement
3. Corporate Risk Management Strategy Working Practices 2009/10
4. Strategic Risk Register
5. Directorate Risk Registers
6. Service Risk Registers
7. Internal Audit Strategy
8. Internal Audit Charter
9. Strategic Internal Audit Plan
10. Annual Internal Audit Plan
11. Outcomes of internal and external audit reviews and other inspections
12. Corporate Health and Safety Policy Statement

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank