HOUSE OF LORDS

Management Board

Records Management in the House of Lords:
Results of the Compliance Audit 2009-10

Responsible Board Member(s)   Elizabeth Hallam Smith
Paper prepared by   Alex Daybank, Shona Robertson

Date   6 May 2010

Summary: This paper reports the overall findings, associated risks and recommendations of the Records Management Compliance Audit carried out across the House of Lords administration between October 2009 and March 2010. The paper reflects the comments of the Audit Steering Group[1].

Annex 1 reports the levels of assurance assigned to each office.
Annex 2 provides the definitions of the levels of assurance used.

Summary of actions requested: The Board is invited to:
- note the findings of the audit and risk issues raised.
- approve that a follow-up to the audit is carried out in Autumn 2010.

Background

1.   This paper presents the findings of an audit to evaluate compliance with the *Parliamentary Records Management Policy* across the administration. The audit also assessed the level of risk the administration may be exposed to in relation to information security.

2.   The audit examined whether records[2] documenting the administration's activities are created as appropriate, captured into corporate record keeping systems, can be identified, located and retrieved in a timely fashion, that sensitive information is handled appropriately, and that all copies of records are disposed of in accordance with the *Authorised Records Disposal Practice* and relevant legislation.

3.   Failure to manage records effectively can affect the administration's ability to make informed decisions based on accurate and complete information. It can also result in financial or reputational damage, or failure to meet legislative obligations if information required is not available and the administration cannot account for its actions.

Methodology

4.   Office nominated Records Management Champions, supported by the Parliamentary Archives, completed a self-assessment of their office's current records management

---

[1] Elizabeth Hallam-Smith (Director of Information Services (Chair)); Rhodri Walters (Reading Clerk and Senior Information Risk Owner); Paul Thompson (Head of Internal Audit); John Pullinger (Director of Information Services, HC); Joan Miller (Director of PICT); Helen Wood (Director of SPIRE); Frances Grey (Assistant Clerk of the Records)
[2] Records are defined in the policy as "…*information, irrespective of format or the media on which it is held, created, received and maintained as evidence and information by both Houses, in the transaction of business or in pursuance of legal obligations.*"

practices, a survey of databases and a survey of sensitive information. Follow-up interviews were conducted where necessary. The information provided was used to assess compliance with policy and identify any risk issues and areas for improvement. Due to time and resource constraints, detailed testing of records management practices at operational levels was not possible.

5.   A report summarising findings, risks and recommendations for improvement for each office was submitted to Heads of Office.

Overall assessment of compliance

6.   The majority of offices are complying with the requirements of the *Parliamentary Records Management Policy* and procedures for information security and have sufficient controls in place for the types of records held. There are examples throughout the administration of exemplary records management and information security practices. Assurance levels achieved by individual offices are at Annex 1.

7.   Levels of assurance assigned to individual offices reflect whether non-compliance with policy and ineffective management of records constitutes a higher risk to the administration. Particular attention was given to the management of key record series that relate to Members' use of parliamentary services and facilities (i.e. expenses, functions, accommodation, etc) and the administration's statutory obligations (i.e. contractual obligations, *Data Protection Act 1998*, and employment law); records containing sensitive information; and offices which are subject to a higher than average volume of Freedom of Information requests.

8.   Some significant weaknesses and poor compliance were identified in two high risk areas, the Human Resources Office and the Refreshment Department. The management responses received from these offices take on board the risks raised and provide a practical reply to the recommendations made. Both offices have started work to implement key recommendations and lay the foundations for sustainable improvement in their level of compliance.

9.   However full assurance on the adequacy of practices to mitigate risks across the administration at this current time cannot be given and an overall level of **limited assurance** is therefore assigned.

Issues raised

10. The audit revealed examples of the following issues:

- Records management is frequently perceived as additional to 'business as usual'. Staff do not always recognise that records and information are assets which underpin effective corporate governance, accountability and business efficiency.

- Appropriate understanding of records management requirements and individuals' responsibilities varies widely across the administration. Records management is sometimes regarded as an activity undertaken by designated members of staff only. Attendance by staff at records management training is low.

- Some staff do not recognise that the information they create or receive daily in the course of their work, including electronic documents and email correspondence, are records which must be managed in line with corporate policy.

- There are cases where records are held in personal silos (e.g. personal email accounts, *My documents* folders etc) where they are inaccessible to others who have a business need to access the information.

- Procedures for the effective management of records are not always well integrated into day-to-day business processes and activities.

- The policy requirement that all substantive records must be printed and filed is not consistently implemented.

- Records held electronically on network drives and as email in Outlook accounts are not well managed; this is partly due to a misconception that these are not 'records'.

- Information held in databases, including personal data, is frequently being retained indefinitely. There is a common assumption that PICT are responsible for managing and deleting information held in databases in line with records management policy.

- Insufficient awareness and understanding of the requirements for managing personal information.

Conclusions

11. Records management is often considered a low priority activity and not all staff have the knowledge or skills to ensure compliance with policy. This can result in inadequate practices in the areas of records creation, retrieval and retention putting offices, or the administration more widely, at risk.

12. The issues raised in the audit need to be addressed by refocusing on the processes by which records are managed, particularly at the point of creation (i.e. as early as possible in the business process).

13. There is also a need for offices to recognise that they, as information owners, are ultimately responsible for the management of information, including that which is held in systems and databases. There is a need to develop and implement policies and procedures in this area.

14. To achieve full compliance across the administration, the records management 'culture' needs to evolve to close gaps caused by embedded personal and/or office work habits. These gaps can be eliminated by extending understanding and awareness across all staff, through training and by implementing enabling technologies so staff will be motivated to undertake new practices in compliance with policy and procedures. In particular, staff at senior and middle management levels have to demonstrate their commitment to these practices and embed them into the everyday culture of their offices and teams.

Implementation of recommendations

15. Recommendations made to each office provide the framework for sustainable improvement. Some targets are given a higher priority and urgency than others, based on business need or the perception of risk to the office or the administration.

16. Some recommendations will be more easily implemented by individual offices than others. Offices will be supported throughout this process by the Parliamentary Archives and the Information Compliance Manager. Other findings require unified working across the administration to achieve the necessary outcome (i.e. the effective management of electronic records).

17. The Parliamentary Archives will shortly release a series of brief guidance cards on day-to-day records management practices, develop a short training session covering both records management and information security, and review procedures and training for information security and Data Protection.

18. The Human Resources Office and the Parliamentary Archives will review the competency framework for information management (including records management, knowledge management and information risk and security) to support the inclusion of these in relevant role descriptions and forward job plans.

19. The implementation of both an Electronic and Document and Records Management System (through the SPIRE programme) and a solution for digital preservation will enable records created electronically (including email) to be managed electronically both in the short and long term. However, full benefits will not be realised unless areas of weakness highlighted in this audit are addressed.

20. Procedures will be developed to ensure issues related to poor record keeping identified by Internal Audit are raised with the Parliamentary Archives to ensure offices are supported in resolving these promptly.

21. The Information Compliance Manager is already working on behalf of the Senior Information Risk Owner to ensure that the administration has procedures in place to mitigate information risk. The issues raised in the audit will further inform this work.

Next steps

22. It is necessary to agree a means to ensure offices are held accountable for implementing recommendations for improvement made in this audit.

   The Board is invited to approve a 'records management health-check' is carried out in October 2010, to assess progress against audit recommendations.

Annex 1

Assurance levels and high priority recommendations by office

Black Rod's Department	Substantial assurance
Clerk of the Parliaments' Office	Moderate assurance
Committee Office	Moderate assurance
Delegated Legislation Office	Full assurance
Department of Facilities	Moderate assurance
Finance Department	Substantial assurance
Human Resources Office	No assurance
Information Office	Moderate assurance
Journal Office	Moderate assurance
Library	Moderate assurance
Lord Speaker's Office	Moderate assurance
Official Report (Hansard)	Substantial assurance
Overseas Office	Moderate assurance
Parliamentary Archives	Substantial assurance
Printed Paper Office	Moderate assurance
Public and Private Bill Office	Substantial assurance
Refreshment Department	No assurance

Annex 2   **Levels of Assurance**

Full assurance
There is evidence of full compliance with the *Parliamentary Records Management Policy (2006)*; the *Authorised Records Disposal Practice* and relevant procedures, including those for information security. These are being consistently applied throughout the office and management are fully engaged in ensuring this remains the case. There will be no significant recommendations for change although minor procedural improvements may be suggested to further aid compliance.

Substantial assurance
There is evidence of widespread compliance with the *Parliamentary Records Management Policy (2006)* and information security procedures across the office with few areas of weakness. Principal controls are being applied by management who are engaged in the process and recognise their responsibilities to lead in this area. Some improvements can be made to ensure full compliance and recommendations will be made to this end.

Moderate assurance
Evidence shows that there is reasonable compliance across the office with the majority of key requirements of the *Parliamentary Records Management Policy (2006)* and information security procedures. However there are weaknesses in the application of relevant procedures exposing the administration to increased risk. Management are aware of the need to foster compliance. Recommendations for improvement will be made.

Limited assurance
Although there is compliance in certain areas of the office or with certain aspects of relevant policies and procedures there is significant evidence of non-compliance and as a result the administration is exposed to substantial risk. Recommendations for improvement will require high priority implementation.

No assurance
There is little or no evidence of compliance, exposing the administration to unacceptable risks which are not being managed. Urgent action must be taken to bring the office up to an acceptable level of assurance and meet the minimum requirements of the *Parliamentary Records Management Policy (2006)* and information security procedures.