

The Electoral Office for Northern Ireland

Audit fieldwork report 2006/07

Information Technology Systems

25 June 2007

Our ref: BC/PP/ck

Private and confidential

D Bain Esq
Chief Electoral Officer
Electoral Office for Northern Ireland
2nd Floor
St Anne's House
15 Church Street
Belfast
BT1 1ER

25 June 2007

Dear Sir

Re: Fieldwork visit 2006/07 – Information Technology Systems

Introduction

1. We recently completed our internal audit fieldwork in respect of the 2006/07 financial year in relation to Electoral Office for Northern Ireland's ("EONI's") Information Technology ("IT") Systems. This report summarises our findings.

Background

2. EONI uses the following IT systems for the maintenance of the electoral register, financial accounting records and personnel and payroll details:

- a) *Electoral Registration Operating System ("EROS")*: EROS is used for the maintenance of an integrated election and registration management system. EROS has been tailored and refined to meet the specific needs of the Northern Ireland registration system (Northern Ireland's information is maintained by elector, while the rest of the United Kingdom information is maintained by household). We note that a contract is in place with Hewlett Packard ("HP") for the maintenance of EROS;
- b) *SUN accounting system*: EONI maintains separate election and non election related chart of accounts on SUN. The EONI Finance section produces monthly management information packs which provide details of all election and non related income and expenditure. The system is maintained by SYSCO Software Solutions ("SYSCO"); and
- c) *UNIPIMS system*: UNIPIMS is EONI's human resource management system and facilitates a full range of personnel functions, including personnel management, payroll management, absence management, recruitment management, training and full payroll processing. The UNIPIMS payroll system is administered by ICS Payroll (a third party payroll bureau service).

3. IT systems within EONI are managed by the Information Services Department, which comprise three full time members of staff. The budgeted expenditure (excluding salaries) in relation to IT for the 2006/07 financial year (including software, hardware maintenance and line rental) was £242,000, compared to budgeted expenditure of £250,000 in respect of the 2007/08 financial year.

4. The main responsibilities of the Information Services Department include:

- a) IT security: ensuring that no unauthorised users obtain access to the system. The Department is responsible for the installation and maintenance of firewalls, reviewing access levels for different parts of the system and ensuring that no staff member is cleared for the system until they have signed the security operating procedures;
- b) installing and administering of IT hardware and software;
- c) backing up the data on a working day basis; and
- d) compiling and producing reports and statistical analysis from the electoral register using standard report generators.

5. We note that a number of external organisations have undertaken detailed technical testing and review of EONI's systems over the last year. These include the following:

- a) *IT Systems health check*: this health check was performed by Selex Communications. Following the health check, a report was produced, which concluded that the EONI network was well configured and secure and was adequately protected from the risk of external attack. A number of network issues were identified and recommendations made. Our discussions with EONI management indicated that these recommendations should be implemented by the Information Technology Department by April 2007;
- b) *the Accreditation Authority*: the Accreditation Authority (the Departmental Security Officer from the Northern Ireland Office ("NIO")) undertook a review of EONI's IT systems during 2006. Our discussions with EONI management indicated that EONI's accreditation certificate will be renewed in June 2007; and
- c) *the Department for Work and Pensions ("DWP")*: we note that DWP undertakes a comparative review between DWP internal records and the electorate's "personal identifiers". We note that this check is undertaken three times per annum.

Scope

6. In line with the agreed terms of reference for this review the fieldwork focussed on assessing EONI's controls in relation to:

- a) ensuring that data is backed-up regularly;
- b) ensuring that adequate IT security policies and procedures are in place;
- c) ensuring that adequate contingency/recovery plans are in place;
- d) ensuring that access controls or physical security controls are in place;

- e) ensuring that the requirements of the data protection legislation are adhered to;
- f) ensuring that only licensed software is used; and
- g) ensuring that the service level agreement in respect of outsourcing payroll is appropriate and adequately reviewed.

7. This report is addressed to the Chief Electoral Officer and as required by our terms of appointment, copies of all finalised reports will be issued to the NIO's Head of Internal Audit, the Northern Ireland Audit Office ("NIAO") and the RIR division within the NIO. No duty of care is accepted to any party other than those to whom the report is addressed. No responsibility is accepted for any reliance placed upon our report, should it be used for any purpose other than that stated above.

Basis of assurance

8. We conducted our internal audit work in accordance with the Government Internal Audit Manual ("GIAM"). Our work included an examination, on a test basis, of EONI's system of internal control.

9. This review has been conducted within the context of an internal audit review process designed to address key risks on an annual basis. Only two and a half days were allocated to this review, which included the provision of advice and guidance with respect to the development of a business continuity plan. Consequently there was a requirement to conduct a general assessment of the key aspects of the systems and focus on a limited number of specific areas. In these circumstances, this review should not be regarded as being an extensive and detailed review sufficient to test and assess all aspects of EONI's IT systems.

10. We planned and performed our internal audit work to obtain reasonable assurance that the systems were operating as described and that the accounting records were not materially misstated on account of fraud or error. However, you should not rely on our work to identify all instances of fraud or error. The responsibility for these matters rests with management and the Chief Electoral Officer.

Findings

11. At the time of undertaking our review, January 2007, we identified that a business contingency plan had not yet been fully developed in EONI. We also noted that agreements in place with external providers in respect of the SUN accounting system and the UNIPIMS payroll system were not being reviewed on a regular basis. We also identified that recommendations made in a recent review undertaken by SELEX Communications, had not yet been fully implemented. EONI management indicated that these recommendations should be implemented by April 2007.

12. We have attached the key findings identified in the course of our work at *Appendices A to C*. These appendices are broadly analysed by category of weakness as follows:

Weakness	Appendix
Development of a business continuity plan	A
Review of maintenance agreements	B
Review by SELEX Communications	C

13. This report was issued in draft on 11 June 2007. The findings included in this report were discussed with the Head of Corporate Services on 11 June 2007.

Management Responses

14. We have attached an implementation table at *Appendix D* for management to record their responses and implementation dates for each of the audit recommendations. Responses should confirm if each recommendation is accepted, partially accepted or not accepted and, if accepted, management should provide detail of their strategy for implementing each recommendation.

Assurance rating - reasonable

15. In our opinion, there are a number of improvements which could be incorporated within EONI's internal control system for IT Systems, particularly in relation to the development and implementation of a business continuity plan. However, the existing controls in place within EONI are basically sound and provide **reasonable** assurance regarding the effective and efficient achievement of EONI's objectives in relation to IT systems.

16. We have attached a definition of our assurance ratings at *Appendix E*.

Other matters

17. We would like to take this opportunity to thank EONI's management and staff for their assistance and co-operation during the course of this assignment.

18. If you have any queries in relation to this correspondence, please do not hesitate to contact Brian Clerkin or Pauline Poots.

Yours faithfully

ASM Horwath

e-mail: brian.clerkin@asmhorwath.com
pauline.poots@asmhorwath.com

Development of a business continuity plan

A

Weakness

A1. Our discussions with EONI management identified that responsibility has been assigned for the development of a business continuity plan. We note that while undertaking our review, we provided advice and guidance in relation to the content of this plan. At the time of undertaking our detailed testing in January 2007, we noted that work on this plan had been postponed until the completion of the elections in March 2007.

Effect

A2. Failure to ensure that a business contingency plan is developed for the organisation increases the risk of non-continuation of business operations should a disaster occur and a lack of staff knowledge of the procedures in the event of such a disaster.

Recommendations

A3. We recommend that the business contingency plan for EONI be completed as soon as possible.

A4. We recommend that the business contingency plan should be maintained and tested on an annual basis to ensure that it remains current.

Review of maintenance agreements

B

Weakness

B1. While undertaking our detailed testing we requested copies of all maintenance contracts and service level agreements established in respect of EROS, the Sun accounting system and the UNIPIMS Payroll System. Whilst we noted that agreements have been established in respect of the maintenance of these systems and responsibility has been formally assigned for the monitoring and review of these agreements, we noted that the agreements in relation to the Sun accounting system and the UNIPIMS payroll system have not been formally reviewed since 2002.

Effect

B2. Failure to ensure that agreements are formally reviewed on a regular basis may increase the risk that EONI will not achieve value for money in respect of current agreements.

Recommendation

B3. We recommend that EONI ensure that all maintenance agreements are formally reviewed on a regular basis.

Review by SELEX Communications

C

Weakness

C1. Our discussions with EONI management identified that an external organisation, “SELEX Communications” undertook a detailed review of EONI’s local area network (“LAN”) during December 2006. Whilst we note that the overall conclusion of this report was positive insofar as it stated “the EONI network was found to be very well configured”, a number of issues were identified in relation to software patch and upgrade management, user management and associated controls and we note that a number of recommendations were made in this regard (3 high priority recommendations, 5 medium priority recommendation and 3 low priority recommendations).

C2. At the time of undertaking our review, January 2007, EONI management indicated that these recommendations had not yet been implemented, but that all recommendations should be fully implemented by the end of April 2007.

Effect

C3. Failure to ensure that all recommendations identified in this report may result in the security of EONI’s network being compromised.

Recommendation

C4. We recommend that EONI ensure that all recommendations identified in this report are fully implemented as soon as possible.

Summary of recommendations and implementation schedule

D

Reference	Recommendation	Management response	Action Taken / To be Taken	Implementation Date
A3.	We recommend that the business contingency plan for EONI be completed as soon as possible.	Accepted	Draft Business Continuity Plan (incorporating IT Disaster Recovery Plan) was presented to the Management Board on 21 June 2007	1 August 2007
A4.	We recommend that the business contingency plan should be maintained and tested on an annual basis to ensure that it remains current.	Accepted	Incorporated in the Draft business Continuity Plan	1 December 2007
B3.	We recommend that EONI ensure that all maintenance agreements are formally reviewed on a regular basis.	Accepted	Contracts extended to 31 December 2007. Need for these systems is under review. Maintenance agreement reviews will be built into any future contracts.	Periodic reviews in accordance with any future contracts
C4.	We recommend that EONI ensure that all recommendations identified in this report are fully implemented as soon as possible.	Accepted	The 3 high recommendations have been implemented. 4 out of 5 medium recommendations have been implemented with exception of number 7 which was not technically feasible. It has been noted that any future passwords will be generated using HP Protect Tools. The 3 low recommendations have been implemented.	April 2007

Assurance rating and prioritisation definitions

E

Assurance rating definitions

Substantial assurance

Very sound control system, i.e. controls established and operating effectively which address all of the key risks that threaten achievement of aims and objectives. No control weaknesses identified and any recommendations made relate to potential enhancements in control.

Reasonable assurance

System is basically sound, i.e. the majority of the controls required to address the key risks are present and operating effectively and the absence of, or ineffective application of control(s) does not create any material weaknesses that threaten the achievement of aims and objectives. Recommendations are made to address any control omissions and to enhance control.

Limited assurance

System has material weaknesses primarily due to non-compliance, i.e. the majority of the controls required to address the key risks are present but they are not operating effectively or consistently which threatens achievement of aims and objectives.

System has material weaknesses due to the absence of some key controls that threaten the achievement of aims and objectives, i.e. some effective controls established but the controls required to address other key risks are absent.

Recommendations are made to address areas of non-compliance and highlight any control omissions.

No assurance

Poor system, i.e. few or none of the key controls required to address the key risks are present. The weaknesses are very significant and represent a major threat to the achievement of aims and objectives.