

Electoral Office for Northern Ireland

Audit fieldwork 2011/12

IT security and information assurance

1 February 2012



Ref: BC/PP/am

Private and Confidential

Mr G Shields
Chief Electoral Officer
The Electoral Office for Northern Ireland
2nd Floor
St Anne's House
15 Church Street
Belfast
BT1 1ER

ASM
20 Rosemary Street
Belfast
BT1 1QD

1 February 2012

Dear Sir

Re: Fieldwork visit – IT security and information assurance

Introduction

1. We have completed our internal audit fieldwork visit in relation to the Electoral Office for Northern Ireland's ("EONI's") systems for IT security and information assurance. This report summarises our findings.

Background

2. EONI's Assistant Chief Electoral Officer (Elections) has overall responsibility for EONI's IT section which currently comprises a Head of Information Services, a Senior IT Officer and an Information Officer. A further IT Officer post has been vacant since May 2011.

3. EONI achieved security accreditation in respect of its IT systems and resources in December 2010. We understand that a reassessment of this accreditation will be undertaken in November 2011.

4. On an annual basis, EONI also engage independent IT consultants to undertake an assessment of the security of EONI's IT systems. The most recent assessment, undertaken in December 2010, identified that whilst EONI has a number of good practices in place in respect of IT security, a number of improvements could be made. We note that recommendations were made in relation to patching, shared passwords, boot security and voice network segregation. We were advised by management that these recommendations have been implemented.

5. We understand that representatives from the Northern Ireland Office provided Information Assurance training to EONI staff during September 2011. We also understand that EONI are currently developing an Information Asset Register and that staff are provided with EONI's 'Security Operating Procedures' on induction and that all staff are required to undertake an annual e-learning assessment in respect of information assurance.

Scope

6. This review was undertaken in accordance with EONI's Strategic Internal Audit Plan, approved by the Management Committee on 18 August 2011. The fieldwork visit focussed on assessing the following controls in respect of the systems operating in respect of IT security and information assurance:

- a) to ensure that adequate IT security and information assurance policies and procedures are in place and are in accordance with best practice guidance;
- b) to ensure that physical controls and access controls are in place to safeguard the confidentiality, integrity and availability of EONI data;
- c) to ensure that data is backed-up regularly;
- d) to ensure that a business continuity plan is in place, has been tested and is subject to adequate monitoring and review; and

e) to ensure that an adequate management audit trail exists.

7. The following corporate risk, and associated controls, within EONI's corporate risk register, dated 23 June 2011, were considered as part of this review:

- a) loss of IT or accommodation; and
- b) loss of personal data.

8. This report is addressed to the Chief Electoral Officer and it is not to be released beyond EONI's management and staff, without our prior written consent. 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

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

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

Findings

11. Our review identified that EONI has adequate access and physical controls in place to safeguard the confidentiality, integrity and availability of EONI's electronic data. We also noted that electronic data is backed up on a regular basis.

12. However, our review identified that EONI do not currently have an Information Assurance Policy and that while a Business Continuity Plan is in place, there is a need to review and update the plan.

13. We have attached at **Appendices A** to **B** the key findings identified in the course of our work. These are set out as follows:

Weaknesses	Appendix	Priority
Information Assurance Policy	A	High
Business Continuity Plan	B	Medium

14. These findings were discussed with Mr Graham Shields (Chief Electoral Officer), Mrs Margaret McMullen (Head of Corporate Services), Mr Peter Mullan (Finance Officer), Ms Jocelyn McCarley (Assistant Chief Electoral Officer (Registration)) and Mrs Liz Murray (Assistant Chief Electoral Officer (Elections)) on 6 October 2011.

15. A draft of this report was issued on 25 October 2011. A revised draft of this report was issued on 24 November 2011. Client comments were received on 1 February 2012.

Assurance rating – Satisfactory

16. In our opinion, there are a number of improvements which could be incorporated within EONI's system for risk management, control and governance in respect of IT security and information assurance, particularly in relation to the development of an Information Assurance Policy and the need to review and update the Business Continuity Plan.

17. However, the existing risk management, control and governance systems in place in respect of IT security and information assurance are basically sound and provide **satisfactory** assurance regarding the effective and efficient achievement of EONI's objectives in relation to IT security and information assurance.

18. We have attached definitions of the assurance ratings and our priority levels at **Appendices C** and **D**.

Other matters

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

20. If you have any queries in relation to this correspondence, please do not hesitate to contact Brian Clerkin or Amanda McMaw.

Yours faithfully

ASM

Email: brian.clerkin@asmbelfast.com
amanda.mcmaw@asmbelfast.com

Information Assurance Policy

A

Weaknesses

- A1. Our review identified that while the Northern Ireland Office's ("NIO's) Information Assurance Policy (dated October 2008) is available to staff via EONI's document management system, EONI does not currently have its own Information Assurance Policy in place reflecting its specific circumstances.
- A2. We understand that, in January 2010, EONI's previous Chief Electoral Officer commenced the development of an Information Assurance Policy which was broadly based on the the NIO's Policy. However, we note that this document has not yet been completed.
- A3. We note that HM Treasury best practice guidance states that organisations should have an Information Assurance Policy in place which sets out how it manages and controls information risks.

Effects

- A4. In the absence of an EONI-specific Information Assurance policy, there is a risk that information risks may not be effectively managed.

Recommendations and management action plans

Recommendations	Status (Recommendation accepted / not accepted)	Comment	Responsibility	Timeframe
A5. We recommend that an Information Assurance Policy be developed.	<i>Accepted</i>	<i>Information Assurance Policy to be developed in line with the NIO Policy.</i>	<i>IT Security Officer</i>	<i>Completed and circulated to all staff 9 December 2011</i>

Business Continuity Plan

B

Weaknesses

B1. Our review identified that EONI have a Business Continuity Plan ("BCP") (dated February 2010) which sets out areas of responsibility in respect of business continuity planning within EONI along with details of EONI's disaster recovery site, incident management and reporting procedures, emergency response procedures and procedures for the storage, review and testing of the BCP.

B2. We understand that this document was developed by the then Assistant Chief Electoral Officer (Elections) ("ACEO") during the 2006/07 year and was approved by the Management Board and issued to staff in July 2007. We note that since the previous ACEO's departure from EONI in September 2009, responsibility for reviewing, monitoring and testing the BCP has been allocated to EONI's Head of Information Services who is currently acting up to the position of Assistant Chief Electoral Officer (Elections).

B3. Our review identified that the BCP was most recently tested in March 2010. However, we noted that the key contacts noted within the document include staff who are no longer employed by EONI. We also noted that while EONI's IT Disaster Recovery Plan has been subject to ongoing monitoring, review and updating (most recently in August 2011) the BCP still contains, as an appendix, a previous version of the IT Disaster Recovery Plan.

B4. We consider that a review and update of the BCP is required. Our subsequent discussions with management identified that this process is currently ongoing.

Effects

B5. In the absence of an up to date BCP, there is a risk that if a disaster was to occur, business may not be able to continue.

Business Continuity Plan (cont'd)

B

Recommendations and management action plans				
Recommendations	Status (Recommendation accepted / not accepted)	Comment	Responsibility	Timeframe
B6. We recommend that all necessary steps are taken to ensure that the BCP is reviewed, updated and subject to testing as soon as possible.	Accepted	<i>Business and IT Disaster Recovery Plan to be reviewed, updated and approved by the Management Board.</i>	<i>IT Security Officer</i>	<i>1 February 2012</i>
		<i>Business Continuity Plan to be tested through a desk exercise and contact details updated quarterly.</i>	<i>ACEO (Elections) and IT Security Officer</i>	<i>7 February 2012 and annually thereafter</i>
		<i>A full IT Disaster Recovery 'live' test to be carried out on an annual basis, a 'Live' test was carried out on 14 October 2011.</i>	<i>IT Security Officer</i>	<i>Annually</i>
		<i>'Out of hours' tests to be carried out three times per annum, 'out of hours' tests were carried out on 8 October 2011 and 8 January 2012.</i>	<i>IT Security Officer</i>	<i>Three times per annum</i>
		<i>Revisions and testing of the plan to be reported quarterly to the Management Board and recorded on EONI Strategic Risk Register.</i>	<i>IT Security Officer</i>	<i>26 April 2012 and quarterly thereafter</i>
		<i>Quarterly reviews to ensure the Plan is reviewed, tested and kept up-to-date.</i>	<i>ACEO (Registration)</i>	<i>1 May 2012 and quarterly thereafter</i>

Assurance rating definitions

C

Level of assurance	Definition
Substantial	There is a robust system of risk management, control and governance which should ensure that objectives are fully achieved.
Satisfactory	There is some risk that objectives may not be fully achieved. Some improvements are required to enhance the adequacy and / or effectiveness of risk management, control and governance.
Limited	There is considerable risk that the system will fail to meet its objectives. Prompt action is required to improve the adequacy and effectiveness of risk management, control and governance.
Unacceptable	The system has failed or there is a real and substantial risk that the system will fail to meet its objectives. Urgent action is required to improve the adequacy and effectiveness of risk management, control and governance.

Priority ratings

D

In prioritising recommendations for action, we have used the following definitions:

Priority rating	Definition
High	Significant weaknesses which could threaten the achievement of the organisation's objectives or the maintenance of an appropriately robust control environment. Remedial action by senior management is required.
Medium	Weaknesses which could threaten the achievement of objectives. Remedial attention by management is required.
Low	Some weaknesses which could have an impact on the achievement of objectives. Action is required to monitor the situation and improve control.