East Lothian Council

REPORT TO: Audit and Governance Committee

MEETING DATE: 29 November 2016

BY: Depute Chief Executive – Resources & People Services

SUBJECT: Internal Audit Report – Public Services Network

---

1 PURPOSE

1.1 To inform the Audit and Governance Committee of the recently issued audit report on Public Services Network (PSN) compliance.

2 RECOMMENDATION

2.1 That the Audit and Governance Committee note the contents of the Executive Summary and Action Plan.

3 BACKGROUND

3.1 A high level review of PSN compliance was undertaken as part of the audit plan for 2016/17.

3.2 The main objective of the audit was to ensure that the internal controls in place were operating effectively.

3.3 The main findings from our audit work are outlined in the attached report.

4 POLICY IMPLICATIONS

4.1 None

5 INTEGRATED IMPACT ASSESSMENT

5.1 The subject of this report does not affect the wellbeing of the community or have a significant impact on equality, the environment or economy.

6 RESOURCE IMPLICATIONS

6.1 Financial – None

6.2 Personnel – None

6.3 Other – None

7 BACKGROUND PAPERS

7.1 None

AUTHOR'S NAME	Mala Garden
DESIGNATION	Internal Audit Manager
CONTACT INFO	01620 827326
DATE	17 November 2016

EAST LOTHIAN COUNCIL – INTERNAL AUDIT
PUBLIC SERVICES NETWORK

1. EXECUTIVE SUMMARY

1.1 Introduction

As part of the Audit Plan for 2016/17 a high level review of Public Services Network (PSN) compliance was undertaken. A summary of our main findings is outlined below.

1.2 Areas where Expected Controls were Met

- The Council has successfully achieved the PSN connection compliance certificate for 2016/17 – the certificate was issued on 3 November 2016 following completion of the PSN compliance verification process.
- The Council has a number of policies in place covering information security.
- A unique user ID is assigned to all users with access to the corporate network.
- Access to the Council's data centres is restricted to key members of staff.
- Adequate arrangements are in place to ensure that annual independent IT Health Checks are undertaken to identify ICT security weaknesses.
- A clear audit trail is maintained of all security incidents and of the action taken.
- Remediation Action Plans are prepared to address risks identified by the IT Health Checks.

1.3 Areas with Scope for Improvement

- The existing processes in place for the patching and upgrading of systems and application software require to be formalised. *Risk – an inconsistent approach may be adopted.*
- There was a lack of evidence to demonstrate that regular reviews are undertaken of user accounts and administrator accounts. *Risk – lack of a clear audit trail.*
- The Council's 2015/16 PSN submission records that all employees are required to re-sign the Council's IT Acceptable Use Policy every two years, however we found that this has yet to be actioned. *Risk – failure to ensure staff awareness of Council policy.*
- A Council-wide Information Security Forum has been established to discuss information security issues and to risk assess any new services or systems, however the Forum has not met since 2012. *Risk – failure to meet information security standards.*
- The existing arrangements in place for third party access to Council systems require review. *Risk – lack of a clear audit trail.*
- The draft information security incident procedure requires to be formalised. *Risk – an inconsistent approach may be adopted.*

1.4 Summary

Our review of PSN compliance has identified a number of areas with scope for improvement. Detailed findings and recommendations are contained in our main audit report.

Mala Garden
Internal Audit Manager **November 2016**

EAST LOTHIAN COUNCIL – INTERNAL AUDIT
PUBLIC SERVICES NETWORK

ACTION PLAN

PARA REF	RECOMMENDATION	GRADE	RESPONSIBLE OFFICER	AGREED ACTION	RISK ACCEPTED/ MANAGED	AGREED DATE OF COMPLETION
3.1.2	Management should ensure that all relevant members of staff re-sign the IT Acceptable Use Policy as set out in the Council's PSN submission.	Medium	Service Manager – IT Infrastructure	The Acceptable Use Policy will be reviewed and reissued for all relevant staff to sign.		August 2017
3.1.3	Management should ensure that the Council's Information Security Forum is re-established to ensure compliance with PSN requirements.	Medium	Service Manager – IT Infrastructure	Agreed – this will require support from Senior Management across the Council.		January 2017
3.2.2	Management should ensure that a clear audit trail exists to confirm that user accounts and administrator accounts are regularly reviewed.	Medium	Service Manager – IT Infrastructure	Accounts and privileges are reviewed throughout the year as part of our day to day operations. Providing evidence of this is difficult. We will review our procedures to see if there is a way of evidencing the work done.		March 2017
3.2.3	Management should review the existing arrangements in place for third party access to the Council's infrastructure.	Medium	Service Manager – IT Business Systems & Service Manager – IT Infrastructure	Agreed		June 2017

PARA REF	RECOMMENDATION	GRADE	RESPONSIBLE OFFICER	AGREED ACTION	RISK ACCEPTED/ MANAGED	AGREED DATE OF COMPLETION
3.3.1	**Management should ensure that the existing processes in place for the patching and upgrading of systems and application software are formally documented.**	**Medium**	**Service Manager – IT Infrastructure**	**Agreed**		**March 2017**
3.4.1	**Management should ensure that the draft information security incident procedure in place is formalised.**	**Medium**	**Service Manager – IT Infrastructure**	**Agreed**		**January 2017**

Grading of Recommendations

In order to assist Management in using our reports, we categorise our recommendations according to their level of priority as follows:

Level	Definition
High	Recommendations which are fundamental to the system and upon which Management should take immediate action.
Medium	Recommendations which will improve the efficiency and effectiveness of the existing controls.
Low	Recommendations concerning minor issues that are not critical, but which may prevent attainment of best practice and/or operational efficiency.