East Lothian Council

REPORT TO:	Audit and Governance Committee
MEETING DATE:	20 January 2015
BY:	Depute Chief Executive – Resources & People Services
SUBJECT:	Internal Audit Report – IT Disaster Recovery and Business Continuity

1 PURPOSE

1.1 To inform the Audit and Governance Committee of the recently issued audit report on IT Disaster Recovery and Business Continuity.

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 review of IT Disaster Recovery and Business Continuity was undertaken as part of the audit plan for 2014/15.

3.2 The main objective of the audit was to ensure that the Council has appropriate IT Disaster Recovery and Business Continuity arrangements in place.

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

4 POLICY IMPLICATIONS

4.1 None

5 EQUALITIES IMPACT ASSESSMENT

5.1 This report is not applicable to the well being of equalities groups and Equality Impact Assessment is not required.

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	8 January 2015

EAST LOTHIAN COUNCIL – INTERNAL AUDIT
IT DISASTER RECOVERY AND BUSINESS CONTINUITY

1. EXECUTIVE SUMMARY

1.1 Introduction

As part of the Audit Plan for 2014/15 a review was undertaken of the Council's IT Disaster Recovery and Business Continuity arrangements.

1.2 Areas where Expected Controls were Met

- An IT Business Continuity Plan is in place and testing/reviews of the Plan are formally recorded.
- A Corporate Server Back-up Policy is in place to ensure that all servers and databases are properly and routinely backed up **–** the success of overnight back-ups is checked each morning.
- A formal 'significant change' control procedure to assess and approve all changes to live systems has been implemented. This procedure aims to identify and then mitigate risks associated with changes. Contingency measures have been agreed and documented as part of the procedure.
- Key IT risks have been identified and are set out in the IT risk register, together with details of risk control measures currently in place and planned risk control measures.

1.3 Areas with Scope for Improvement

- While an IT Business Continuity Plan is in place, no separate IT Disaster Recovery Plan has been developed clearly outlining the procedures to be followed for responding to a significant disruption in IT capabilities. *Risk – inability to respond effectively and efficiently to a disaster.*
- The Business Continuity Plan prepared by IT and the Business Continuity Plans prepared by some service areas require review – at present the Plans are not aligned to clearly reflect the IT priorities within the Council. *Risk – IT recovery time objectives may not be in line with overall Council priorities.*
- For a number of key systems, no formal arrangements are in place with existing suppliers, specialist contractors or other organisations to provide emergency facilities to the Council in the event of a disaster. *Risk – inability to provide key services.*
- The existing arrangements in place for undertaking routine tests to restore back-ups require review. *Risk – back-ups may not be successfully restored.*

1.4 Summary

Our review of IT Disaster Recovery and Business Continuity 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 **January 2015**

ACTION PLAN

PARA REF	RECOMMENDATION	GRADE	RESPONSIBLE OFFICER	AGREED ACTION	RISK ACCEPTED/ MANAGED	AGREED DATE OF COMPLETION
3.1.1	Management should ensure that an IT Disaster Recovery Plan is developed – the Plan should outline the sequence of events that should be followed in responding to a significant disruption in IT capabilities.	Medium	Service Manager – IT Infrastructure / Service Manager – IT Business Services	Agreed – to form part of the 2015/16 IT Business Continuity Plan.		September 2015
3.1.2	Appropriate consultation should be undertaken between service areas and the IT section to ensure that Business Continuity Plans are properly aligned.	Medium	Emergency Planning and Risk Manager / Business Continuity Single Points of Contact	In place – this now forms part of the Business Continuity Peer Review process.		In Place
3.1.3	Management should ensure that the IT Disaster Recovery Plan includes recovery and salvage procedures in the event of a disaster.	Medium	Service Manager – IT Infrastructure / Service Manager – IT Business Services	Agreed – to form part of the 2015/16 IT Business Continuity Plan.		September 2015
3.1.4	Consideration should be given to having arrangements in place with an external organisation for the provision of emergency IT services in the event of a disaster.	Medium	Head of Council Resources	Agree to explore reciprocal arrangements with suitable partners.		September 2015

PARA REF	RECOMMENDATION	GRADE	RESPONSIBLE OFFICER	AGREED ACTION	RISK ACCEPTED/ MANAGED	AGREED DATE OF COMPLETION
3.2.1	Management should ensure that the risk register in place is reviewed and updated to include all key IT risks – appropriate control measures should be put in place for all risks identified.	Medium	Service Manager – IT Infrastructure / Service Manager – IT Business Services	IT risk register has been reviewed and updated.		In Place
3.3.2	Consideration should be given to introducing a timetable or programme to test that back-ups can be successfully restored.	Medium	Service Manager – IT Infrastructure / Service Manager – IT Business Services	Consideration will be given to programme of back-up testing.		September 2015
3.4.1	Management should ensure that adequate staff training is provided to key staff with responsibility for disaster recovery.	Medium	Service Manager – IT Infrastructure / Service Manager – IT Business Services	Training requirements for key staff will be reviewed.		September 2015

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.