

REPORT TO: Audit and Governance Committee

MEETING DATE: 17 September 2013

BY: Depute Chief Executive – Resources and People Services

SUBJECT: Council Resources Risk Register

1 PURPOSE

- 1.1 To present to the Audit and Governance Committee the Council Resources Risk Register (Appendix 1) for discussion, comment and noting.
- 1.2 The Council Resources Risk Register has been developed in keeping with the Council's Risk Management Strategy and is a live document which is reviewed and refreshed on a regular basis, led by the Council Resources Local Risk Working Group (LRWG).

The Council Resources Register presented shows only High and Very High Risks as the Council's Risk Strategy defines these risks as those which should be subject to closer scrutiny by the Audit and Governance Committee.

2 RECOMMENDATIONS

- 2.1 It is recommended that the Audit and Governance Committee notes the content of the Council Resources Risk Register.
- 2.2 In doing so, the Audit and Governance Committee is asked to:
 - note that the relevant risks have been identified following appropriate consultation with all risk contacts;
 - recognise that while this report has been compiled by the Risk Officer, the Risk Register has been compiled by the Council Resources LRWG and the Head of Council Resources has lead responsibility;
 - note that the significance of each risk is appropriate to the current nature of the risk;
 - note that the total profile of the Council Resources risk can be borne by the Council at this time in relation to the Council's appetite for risk; and,
 - recognise that, although the risks presented are those requiring close monitoring and scrutiny throughout 2013/14, many are in fact longer term risks for Council Resources and are likely to be a feature of the risk register over a number of years.

3 BACKGROUND

- 3.1 The Council's Risk Management Strategy was established following Audit Scotland's 2008/09 review of the Council when it was recommended that: "The implementation of the risk management framework be expedited and target dates established".
- 3.2 Responsibility for Risk Management sits within the Corporate Policy and Improvement unit. The Emergency Planning and Risk Manager, supported by a Risk Officer, has implemented the current Risk Management Strategy and set up both an overarching Corporate Risk Management Group (CRMG) together with LRWGs in service areas.
- 3.3 The LRWGs meet on a regular basis to discuss their Risk Register which is also included as a topic in team meetings. They also feed information to the CRMG; this Group is fundamental to the delivery of risk management throughout the Council and ensures that risk management remains high on the corporate agenda.
- 3.4 All LRWG's were revised following the Senior Management and Service restructure of 2012 resulting in eight Risk Registers/Groups being reduced to seven.
- 3.5 A copy of the risk matrix used to calculate the level of risk is attached as Appendix 2.

4 POLICY IMPLICATIONS

- 4.1 In discussing and noting the Council Resources Risk Register the Committee will be affirming the process of embedding risk management principles across the Council in support of the Risk Management Strategy.

5 EQUALITIES IMPACT ASSESSMENT

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

6 RESOURCE IMPLICATIONS

- 6.1 Financial – It is the consideration of the Council Resources LRWG that recurring costs associated with the measures in place for each risk are proportionate to the level of risk. The financial requirements to support the Council Resources Risk Register for 2013/14 should be met within the proposed budget allocations for 2013/14. Any unplanned and unbudgeted costs that arise in relation to any of the risks identified will be subject to review by the Council Management Team.
- 6.2 Personnel – There are no immediate implications.
- 6.3 Other – Effective implementation of this register will require the support and commitment of the Risk Owners identified within the register.

7 BACKGROUND PAPERS

7.1 Appendix 1 – Council Resources Risk Register

7.2 Appendix 2 – Risk Matrix

AUTHOR'S NAME	Scott Kennedy
DESIGNATION	Risk Officer
CONTACT INFO	01620 827900
DATE	05 September 2013

Council Resources Risk Register

Date reviewed: 05 September 2013

Risk ID No. & Status S/C/N (same, changed, new)	Risk Description (Threat/Opportunity to achievement of business objective)	Risk Control Measures (currently in place)	Assessment of Current Risk			Planned Risk Control Measures	Assessment of Residual Risk [With proposed control measures]			Risk Owner	Timescale for Completion / Review Frequency	Single Outcome Agreement Outcome Number Link	Evidence held of Regular Review
			Likelihood (Probability)	Impact (Severity)	Risk Rating		Likelihood (Probability)	Impact (Severity)	Residual Risk Rating				
			L	I	L x I		L	I	L x I				
CR 1	<p>Welfare reform</p> <p>The UK Government is introducing a range of measures to reform the welfare system and reduce the budget for welfare benefits by at least £11 billion annually. It has been estimated (Scottish Local Government Forum Against Poverty, Sept 2010) that the changes could result in the loss of £8m - £9.5m annually from welfare benefits paid to East Lothian residents.</p> <p>Within the business areas covered by Council Resources, the changes could lead to:</p> <ul style="list-style-type: none"> Increase in rent arrears from reduced Housing Benefits and possible increase in evictions increased pressures on rent collection teams increase in Council Tax arrears and non-payment of Council Tax increase in Business Rates arrears and non-payment of Business Rates loss of income the Council currently receives for administering Housing Benefits 	<p>The Council has received several update reports and will continue to be updated.</p> <p>The Council has established a Welfare Reform Task Group to plan for the changes to the welfare system. The Task Group has four workstreams:</p> <ul style="list-style-type: none"> Communications Data Sharing Training Migration <p>The Task Group and workstreams are meeting regularly and will continue to report back to the CMT.</p> <p>The Council endorsed the work of the Tackling Poverty Theme Group to refocus the work of the group on a single headline outcome: 'Fewer People in East Lothian will experience poverty'. The Fairer East Lothian Fund (£476,000 in 2011/13) funds projects to deliver on the following key outcomes:</p> <ol style="list-style-type: none"> Fewer people in East Lothian will be financially excluded. Financial capability in East Lothian will be improved. The life chances of people at risk of falling into poverty, or already living in poverty, will be improved. People in East Lothian will have better access to advice and information services, including debt and money advice. 	4	4	16	<p>The Council's Welfare Reform Task Group and four workstreams will develop a detailed action plan that will ensure the Council takes necessary measures to prepare for the changes in the welfare system.</p> <p>A Tackling Poverty Strategy and Action Plan are being prepared detailing how the Council and the Community Planning Partnership aims to achieve the outcome: 'Fewer People in East Lothian will experience poverty'.</p> <p>Proposals for targeting the Fairer East Lothian Fund in 2013/14 to assist in achieving the Strategy and Action Plan will be considered.</p>	4	3	12	Depute Chief Executive – Resources and People Services	Under constant review.	N/A	

Risk ID No. & Status S/C/N (same, changed, new)	Risk Description (Threat/Opportunity to achievement of business objective)	Risk Control Measures (currently in place)	Assessment of Current Risk			Planned Risk Control Measures	Assessment of Residual Risk [With proposed control measures]			Risk Owner	Timescale for Completion / Review Frequency	Single Outcome Agreement Outcome Number Link	Evidence held of Regular Review
			Likelihood (Probability)	Impact (Severity)	Risk Rating		Likelihood (Probability)	Impact (Severity)	Residual Risk Rating				
			L	I	L x I		L	I	L x I				
CR 2	<p>Financial pressures:</p> <p>If the council's financial pressures were not to be successfully planned for and managed effectively over the medium to longer term (i.e. the next 3 and possibly up to 7 years), there would be a serious risk of unplanned/ reactive budget realignments with significant adverse impact on availability and quality of both front-line services and required investment in the Council's infrastructure and asset base.</p> <p>Over the medium term it is highly likely that the Council's income will remain static. At the same time it will have specific cost pressures to deal with. These include:</p> <p>(1) demographic change and social-economic pressures - increasing pupil and elderly numbers;</p> <p>(2) general inflationary pressures;</p> <p>(3) specific cost pressures such as the affordability of the increasing number of high-cost individual care packages; and</p> <p>(4) potential financial costs associated with legislative changes such as a number of environmental issues.</p>	<p>The Council has well developed short to medium term financial planning arrangements and financial management arrangements for managing in year budget performance, both of which provide mitigating controls in terms of the immediate financial risk and pressures the Council is faced with.</p> <p>Long-term modelling is deemed to be of little value as the public sector financial environment is unlikely to be stable in other than the short and medium term. Focus is on creating a programme of short and medium term organisational change that can be adapted to match the Councils position as that emerges.</p> <p>The Chief Social Work Officer also has a role to play in overall performance improvement and the identification and management of corporate risk in so far as they relate to social work services.</p>	3	5	15	<p>CMT/Managers continue to follow the financial strategy i.e. cost control/cost minimisation/deliver on agreed savings.</p> <p>Through the Corporate Asset Group, the Council implements the approved Asset Management Strategy and related action plan.</p> <p>CMT to consider a more strategic approach to Procurement and/or a different Procurement Strategy.</p>	3	4	12	<p>Chief Executive</p> <p>Depute Chief Executive – Resources and People Services</p> <p>Head of Council Resources</p>	<p>Action ongoing.</p> <p>Control measures approved by Council, October 2012. Monitoring arrangements will continue to be applied.</p> <p>Risk to be reviewed Dec 2013</p>	N/A	
CR 3	<p>Failure of power and/or cooling in the John Muir House Server Room has the potential to cause major loss of network, application and Internet services for a prolonged period of time as has happened previously. This would have a serious impact on the business of the Council.</p>	<p>Key systems (Email & Social Care) are replicated at Penston House. However access to the Internet and other network services will be severely restricted.</p>	3	5	15	<p>Awaiting budget approval to upgrade power and cooling facilities in the room. To date no budget has been allocated.</p>	2	3	6	Head of Council Resources	Ongoing	N/A	

Risk ID No. & Status S/C/N (same, changed, new)	Risk Description (Threat/Opportunity to achievement of business objective)	Risk Control Measures (currently in place)	Assessment of Current Risk			Planned Risk Control Measures	Assessment of Residual Risk [With proposed control measures]			Risk Owner	Timescale for Completion / Review Frequency	Single Outcome Agreement Outcome Number Link	Evidence held of Regular Review
			Likelihood (Probability)	Impact (Severity)	Risk Rating		Likelihood (Probability)	Impact (Severity)	Residual Risk Rating				
			L	I	L x I		L	I	L x I				
CR 4	Breach of Data Protection or other confidentiality requirements through the loss or wrongful transmission of information (including information stored electronically). This could occur through: - private committee reports, minutes or constituent correspondence not being stored or disposed of appropriately; - loss of material during transit; - individuals not being aware of their responsibilities in respect of confidential material; - lack of appropriate facilities for storage or disposal of material; Effects could include: - breach of relevant laws; - breach of duty of care; - harm to individuals; - legal action; - fines; - requirement to pay compensation; - adverse publicity; - damage to the Council's reputation.	Arrangements for secure filing and storage of confidential papers when not in use. Disposal of confidential waste separately from other papers. Internal mail and/or Council Contractor used to transport Private & Confidential materials. Council PCs and laptops do not accept unencrypted external storage devices. Committee documents dealing with sensitive personal information (e.g. criminal convictions) are now issued only in hard copy, not electronically. Checks on licensing sub-committee documents are made by a second clerk when relevant documents are uploaded. Data Compliance Officer is carrying out a programme of data protection health checks. The Data Protection Policy has been approved. Revenues Information Security Procedure in place.	3	4	12	Continual reviewing of arrangements. Maintaining staff awareness through team meetings, briefing sessions and health checks. Online Data Protection Training to be rolled out to all employees over the next year and then repeated every 2 years.	3	3	9	All managers.	Review Annually	N/A	
CR 5	An inability to meet an increase in competing demands from various services due to a lack of a sufficient staff resource could lead to a failure to provide an adequate service.	An ability to employ temporary employees if required. Ongoing monitoring of team workloads.	3	4	12	Liaison with departmental management teams to discuss future work demands and improve service delivery.	3	3	9	Head of Council Resources	Review Annually	N/A	
CR 6	Efficient Workforce Management, VERS, restructures and budget restrictions could result in the service not being able to maintain a level of staff to allow the service currently provided to continue in its present form.	Two way communication between CMT and all employees regarding the impact of change. All VERS decisions were made following business impact assessments, with support given only to those applications with minimum business impact.	3	4	12	CMT to work with managers to redesign services within resources.	2	4	8	Head of Council Resources	August 2014	N/A	
CR 7	Failure to comply with our procurement processes and/or also business failure of key suppliers leads to service failure, poor value for money, fraud, loss of reputation and/or legal action.	Corporate Procurement Strategy and Procedures including pre-qualification of suppliers. Purchase Card Procedures Procurement Improvement Panel (PIP). Reporting to PIP and CMT. Procurement Skills Training. Regular Internal Audits. Controls over New Suppliers. Supplier Finder on Intranet. Close working with legal services, internal audit and departments. Annual Procurement Capability. Assessment in place and action plan progressed.	3	4	12	CMT ensuring improved compliance with existing Procurement Procedures by championing them and taking action when breaches are found. Improved contract management procedures to be put in place. Continue to improve procurement practices with a view to securing an improved PCA score.	2	4	8	Head of Council Resources	Ongoing	N/A	

Risk ID No. & Status S/C/N (same, changed, new)	Risk Description (Threat/Opportunity to achievement of business objective)	Risk Control Measures (currently in place)	Assessment of Current Risk			Planned Risk Control Measures	Assessment of Residual Risk [With proposed control measures]			Risk Owner	Timescale for Completion / Review Frequency	Single Outcome Agreement Outcome Number Link	Evidence held of Regular Review
			Likelihood (Probability)	Impact (Severity)	Risk Rating		Likelihood (Probability)	Impact (Severity)	Residual Risk Rating				
			L	I	L x I		L	I	L x I				
CR 8	Council IT systems are compromised by internal employee - causing the loss of a system, virus/trojan infection or loss/disclosure of data. This potentially would have a serious impact on the business of the Council.	<p>Internal IT Systems are protected by antivirus, group policy etc. Employees sign the Acceptable Usage Policy and are party to various HR policies and legislation such as the Data Protection Act and Computer misuse act. Info security awareness, HR and Data Protection training etc is provided for employees. Continue to take regular software and data backups to allow systems and data to be restored, following any failure.</p> <p>Continue and constantly improve security measures. Keep up to date with new and emerging threats. Ensure we purchase secure systems and maintain security throughout the system life cycle.</p> <p>The Council complies with ISO27001 the International standard for Information Security (which sets out a risk based approach to ensure the confidentiality, integrity and availability of Council held information & information systems).</p>	3	4	12	Make Information Security awareness training mandatory for employees' council wide.	2	3	6	Head of Council Resources	December 2013	N/A	
CR 9	Mismanagement of the Council's bank accounts or failure of the Council's bank leads to the Council having no funds available to pay staff or suppliers.	<p>Contract in place with our bank. Daily cash flow forecasting and monitoring of bank accounts. Treasury Strategy approved by ELC. Treasury Management Advisor in place.</p>	2	5	10		2	5	10	Head of Council Resources	Continue with level of risk.	N/A	
CR 10	Council IT systems are compromised by criminal 3rd party (e.g. hacker, terrorism) - causing the loss of a system, virus/trojan infection or loss/disclosure of data. This potentially could have a serious impact on one or more Council services.	<p>Systems are protected from outside world by firewall. All external facing systems are vulnerability tested once a year and extra testing takes place on any change to form or function. Comprehensive change control and IT security measures also in place to ensure confidentiality, integrity and availability of systems. All IT staff are trained in the change control procedure. Info sec awareness training of employees to ensure they are aware of risks. Continue to take regular software and data backups to allow systems and data to be restored, following any failure. Regular awareness training of employees' council wide.</p> <p>Continue and constantly improve security measures. Keep up to date with new and emerging threats. Ensure all IT employees take part in regular training in the change control procedures. Ensure we purchase secure systems and maintain security throughout the system life cycle.</p>	2	5	10	Make Information Security awareness training mandatory for employees' council wide.	1	5	5	Head of Council Resources	December 2013	N/A	

Risk ID No. & Status S/C/N (same, changed, new)	Risk Description (Threat/Opportunity to achievement of business objective)	Risk Control Measures (currently in place)	Assessment of Current Risk			Planned Risk Control Measures	Assessment of Residual Risk [With proposed control measures]			Risk Owner	Timescale for Completion / Review Frequency	Single Outcome Agreement Outcome Number Link	Evidence held of Regular Review
			Likelihood (Probability)	Impact (Severity)	Risk Rating		Likelihood (Probability)	Impact (Severity)	Residual Risk Rating				
			L	I	L x I		L	I	L x I				
		The Council complies with ISO27001 the International standard for Information Security (which sets out a risk based approach to ensure the confidentiality, integrity and availability of Council held information & information systems).											
CR 11	Complete loss of ELC's circuit to the Internet, resulting in no access to external systems which include but not limited to Pecos, SEEMIS (schools management system) external email, home working access etc. This would have a serious impact on the business of the Council.	SLA's in place with supplier. Supplier has resilient backbone in place.	2	5	10	Introduce a second link to Internet from network outwith Haddington.	1	4	4	Head of Council Resources	Review after all corporate sites on new network, expected to be around December 2013.	N/A	
CR 12	Council wide Catastrophic failure of central IT systems (inc Telephony) which could be caused by a fire/flood event, terrorist attack or a major virus. This would have a serious impact on the business of the Council.	IT Disaster Recovery plan in place - backup site for systems identified and core system backup plan created.	2	5	10	Improve and develop disaster recovery plan based on lessons learned from regular testing of existing plan. Ensure IT Staff are trained and know their role in event of a disaster.	1	4	4	Head of Council Resources	December 2013	N/A	
Original date produced (Version 1)		19th December 2011									Risk Score	Overall Rating	
File Name		CH&PM Risk Register									20-25	Very High	
Original Author(s)		Scott Kennedy, Risk Officer									10-19	High	
Current Revision Author(s)		Scott Kennedy, Risk Officer									5-9	Medium	
Version		Date	Author(s)		Notes on Revisions							1-4	Low
1		19/12/2011	S Kennedy		Original Version								
2		31/05/2012	S Kennedy		IT Risks updated by S Buczyn and Register revised following Senior Management Restructure								
3		19/11/2012	S Kennedy		Updated following update of Risk Strategy								
4		Jan-June 2013	S Kennedy		Updated following review of Legal Services Risks.								
5		Feb – May 2013	S Kennedy		H&S transferred to Policy & Partnerships, IT and HR risks updated and Welfare Reform risk added.								
6		June-July 2013	S Kennedy		Revenues & Benefits and Finance Risks updated.								

Appendix 2
East Lothian Council
Risk Matrix

Likelihood Description

Likelihood of Occurrence	Score	Description
Almost Certain	5	Will undoubtedly happen, possibly frequently >90% chance
Likely	4	Will probably happen, but not a persistent issue >70%
Possible	3	May happen occasionally 30-70%
Unlikely	2	Not expected to happen but is possible <30%
Remote	1	Very unlikely this will ever happen <10%

Impact Description

Impact of Occurrence	Score	Description						
		Impact on Service Objectives	Financial Impact	Impact on People	Impact on Time	Impact on Reputation	Impact on Property	Business Continuity
Catastrophic	5	Unable to function, inability to fulfil obligations.	Severe financial loss (>5% budget)	Single or Multiple fatality within council control, fatal accident enquiry.	Serious - in excess of 2 years to recover pre-event position.	Highly damaging, severe loss of public confidence, Scottish Government or Audit Scotland involved.	Loss of building, rebuilding required, temporary accommodation required.	Complete inability to provide service/system, prolonged downtime with no back-up in place.
Major	4	Significant impact on service provision.	Major financial loss (3-5% budget)	Number of extensive injuries (major permanent harm) to employees, service users or public.	Major - between 1 & 2 years to recover pre-event position.	Major adverse publicity (regional/national), major loss of confidence.	Significant part of building unusable for prolonged period of time, alternative accommodation required.	Significant impact on service provision or loss of service.
Moderate	3	Service objectives partially achievable.	Significant financial loss (2-3% budget)	Serious injury requiring medical treatment to employee, service user or public (semi-permanent harm up to 1yr), council liable.	Considerable - between 6 months and 1 year to recover pre-event position.	Some adverse local publicity, limited damage with legal implications, elected members become involved.	Loss of use of building for medium period, no alternative in place.	Security support and performance of service/system borderline.
Minor	2	Minor impact on service objectives.	Moderate financial loss (0.5-2% budget)	Lost time due to employee injury or small compensation claim from service user or public (First aid treatment required).	Some - between 2 and 6 months to recover.	Some public embarrassment, no damage to reputation or service users.	Marginal damage covered by insurance.	Reasonable back-up arrangements, minor downtime of service/system.
None	1	Minimal impact, no service disruption.	Minimal loss (0.5% budget)	Minor injury to employee, service user or public.	Minimal - Up to 2 months to recover.	Minor impact to council reputation of no interest to the press (Internal).	Minor disruption to building, alternative arrangements in place.	No operational difficulties, back-up support in place and security level acceptable.

Risk	Impact				
	None (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Almost Certain (5)	5	10	15	20	25
Likely (4)	4	8	12	16	20
Possible (3)	3	6	9	12	15
Unlikely (2)	2	4	6	8	10
Remote (1)	1	2	3	4	5

Key

Risk	Low	Medium	High	Very High
------	-----	--------	------	-----------