East Lothian Council

REPORT TO: Audit and Governance Committee

MEETING DATE: 28 November 2017

BY: Chief Executive

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).

2 RECOMMENDATIONS

2.1 It is recommended that the Audit and Governance Committee notes the Council Resources Risk Register and in doing so, the Committee is asked to note that:

- the relevant risks have been identified and that the significance of each risk is appropriate to the current nature of the risk.
- 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.
- although the risks presented are those requiring close monitoring and scrutiny over the next year, 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 Risk Register has been compiled by the Council Resources LRWG. All risks have been evaluated using the standard (5x5) risk matrix which

involves multiplying the likelihood of occurrence of a risk (scored 1-5) by its potential impact (scored 1-5). This produces an evaluation of risk as either 'low (1-4)', 'medium' (5-9), 'high' (10-19) or 'very high' (20-25).

3.2 The Council's response in relation to adverse risk or its risk appetite is such that:

- Very High risk is unacceptable and measures should be taken to reduce, transfer or treat the risk to a more tolerable position;
- High risk may be tolerable providing the Council is assured that adequate and effective control measures are in place;
- Medium risk is tolerable with control measures that are cost effective;
- Low risk is broadly acceptable without any further action to prevent or mitigate risk.

3.3 The current Council Resources Risk Register includes 3 Very High risks, 7 High risks, 26 Medium risks and 12 Low Risks. As per the Council's Risk Strategy, only the Very High and High risks are being reported to the Committee.

3.4 A copy of the risk matrix used to calculate the level of risk is attached as Appendix 2 for information.

4 POLICY IMPLICATIONS

4.1 In noting this report the Council will be ensuring that risk management principles, as detailed in the Corporate Risk Management Strategy are embedded across the Council.

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 - It is the consideration of the Council Resources Local Risk Working Group that the recurring costs associated with the measures in place for each risk are proportionate to the level of risk. The financial requirements to support the Risk Register for the year ahead should be met within the proposed budget allocations. Any unplanned and unbudgeted costs that arise in relation to any of the corporate risks identified will be subject to review by the Corporate 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	Emergency Planning and Risk Officer
CONTACT INFO	skennedy@eastlothian.gov.uk 01620 827900
DATE	16 November 2017

Council Resources Risk Register

Date reviewed 09 November 2017

Risk ID	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	Impact	Risk Rating		Likelihood	Impact	Residual Risk Rating				
			L	I	L x I		L	I	L x I				
CR 1	**Welfare Reform** The rollout of Universal Credit, (UC) in East Lothian started in April 2015. Whilst initially involving only a small number of cases the subsequent rollout by JCP/DWP of the Universal Credit Full (Digital) Service in East Lothian on 23rd March 2016 has seen a significant number of households migrate from legacy benefits to UC. This phase is called "Natural Migration". It will be followed by a "Managed Migration" phase during which all remaining working age HB cases will migrate to UC Housing. In spite of a reducing HB caseload, there has been a significant increase in workload as a result. The main risks/issues associated with the UC rollout include: • A wider range of people in scope for claiming UC & higher volume of cases as a consequence • Additional demand for (SWF) Crisis Grants. (Risk of overspend) • % increase in current tenant rent arrears • An increased risk of lowered take up of Council Tax Reduction and increased arrears • Increased risk of DWP Admin Subsidy reduction • Temporary Accommodation management charges not being covered by UC Housing Costs. • Increased demand for Discretionary Housing Payments, (DHP) risk of funding gap. A reduction in DWP (UC related) funding which has been supporting, the Welfare Development Officer and additional Benefit Officer posts along with Personal Budgeting Support and Digital Assistance for UC claimants could jeopardise these elements of service delivery.	The Council has established a Welfare Reform Task Group to plan for the changes to the welfare system. The Benefit Service is continuing to make full use of additional Discretionary Housing Payment, (DHP). Council has actively lobbied in various relevant arenas – UK and Scottish Governments both directly and via COSLA which has included the Council Leader writing to both the DWP Secretary of State and Scottish Government ministers highlighting the impacts of the UCFS rollout of EL residents and Council Services. The Benefit Service continues to liaise with the DWP Housing Delivery Performance Team The Benefit Service continues to monitor its SWF & DHP expenditure. Revenues & Benefits Services engage with colleagues in other LAs/RSLs, CoSLA and DWP UC/Job Centre Plus officers to ensure a managed transition to Universal Credit is achieved. Castle Rock HA providing personal budgeting support for East Lothian UC claimants. Additional resource facilitated the purchase of software deployed to assist the Rent Income team to help manage the impact of UC on rent collection. Promotion of ELC 'Right Benefit Campaign'. DWP funding has been utilised to appoint a Welfare Development Officer and an additional Benefit Officer to assist in responding to UC pressures. Both posts are temporary for 1 year. Council Officers continue to engage with Scottish Government, MSPs/Members of the Scottish Parliament's Social Security Committee in relation to development of devolved welfare administration. Additional £100k was allocated in the Administration budget 2017/18 to help mitigate the impact of UC on rent arrears.	5	4	20	Council services will continue to work with the UC Project Team and continue lobbying of UC. The Benefits Service and Homelessness Team have agreed a methodology to disburse additional Scottish Government funding provided for DHP mitigation of Temp' Accommodation management fees and for the prevention of homelessness. Council services will continue to take an active role in discussions with the Scottish Government in the development of the Scottish Social Security Agency. ELC Management & staff will continue to engage with other LAs, JCP/DWP, CoSLA and Scottish Government at a range of levels.	4	4	16	Depute Chief Executive – Resources and People Services Depute Chief Executive – Partnerships and Community Services Welfare Reform Task Group	Scottish Social Security Bill approval date May 2018. DHP & Homelessness Prevention budget review December 2017 All other measures involve meetings over the next 9 months with Scottish Government and other groups as mentioned within the measures.	9	Risk refreshed by Service Managers – Benefits & Financial Assessments and Revenues & Welfare Support October 2017 with no change to assessment of current scores. Risk refreshed by Service Manager – Benefits, November 2016 with Current Risk Score increased from 16 to 20 due to the introduction of the Universal Credit "Full Service" since March 2016 with its inherent, underdeveloped processes etc. along with other reforms coming on line, (such as Benefit Cap etc.) all bringing a greater likelihood of detriment occurring, (should mitigating actions not be possible or fail to mitigate). Risk refreshed by Service Managers – Revenues & Benefits March 2016 with both current and planned scored increased to 16 due to current uncertainty.

Risk ID	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	Impact	Risk Rating		Likelihood	Impact	Residual Risk Rating				
			L	I	L x I		L	I	L x I				
CR 2	Council IT systems are compromised by criminal **3rd party** (e.g. hacker, terrorism) - causing the loss of a system, virus/Trojan/ransomware infection or loss/disclosure of data. This potentially could have a serious impact on one or more Council services. The Council's increased participation in shared services escalates this risk as the council's network boundaries are being opened up to enable data sharing with other agencies.	Systems are protected from the 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. Security logs are reviewed daily by IT staff. 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. Information security awareness training of employees provided council wide to ensure they are aware of risks. Take regular software and data backups to allow systems and data to be restored. Keep up to date with new and emerging threats. Ensure purchase of secure systems and maintain security through system life cycle. 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). Continual vulnerability testing. Continual review of security systems to ensure they are still capable of controlling new and emerging threats. Security systems are patched regularly every 2 months and reviewed to see if the hardware is fit for purpose. Receive and share information on cyber risk from UK Governments National Cyber Security Centre. The Council has carried out a programme of Information Security Awareness sessions within all schools. Procurement Initiation documents check whether IT issues have been considered by new procurements. All known proposals to share information are scrutinised by the IT Security Officer and Information Governance Compliance Officer.	4	5	20	Acceptable use policy for all ELC employees is to be refreshed by March 2018 and all employees will be expected to re-sign.	3	5	15	Head of Council Resources Service Manager - IT	March 2018		Risk reviewed and updated by IT management October 2017 with no change to score. Risk reviewed and updated by IT following delivery of training programme to staff, October 2016. Risk refreshed December 2015 with Current score increased from 15 to 20 and residual from 12 to 15 due to recent breach. Risk refreshed November 2014. Current Risk Score increased from 10 to 15 and Residual Risk score increased from 5 to 12 due to heightened risk.

Risk ID	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	Impact	Risk Rating		Likelihood	Impact	Residual Risk Rating				
			L	I	L x I		L	I	L x I				
CR 3	Council IT systems are compromised by the actions of an internal employee - causing the loss of a system, virus/trojan/ransomware infection or loss/disclosure of data. This potentially would have a serious impact on the business of the Council. HMG and UK Governments National Cyber Security Centre class the risk of cyber-attack in the UK as severe and threat from internal has risen due to ransomware attack increase.	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. Information security awareness, HR and Data Protection training etc. is provided for employees. Continue to constantly improve security measures and keep up to date with new and emerging threats. Security logs are reviewed daily by IT staff. Comprehensive change control and IT security measures also in place to ensure confidentiality, integrity and availability of systems while all IT staff are trained in the change control procedure. Take regular software and data backups to allow systems and data to be restored. Keep up to date with new and emerging threats. Ensure we purchase secure systems and maintain security throughout the system life cycle. 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). Continual vulnerability testing. Continual review of security systems to ensure they are still capable of controlling new and emerging threats. Security systems are patched regularly every 3 months and reviewed to see if hardware fit for purpose. The Council has carried out a programme of Information Security Awareness sessions within all schools.	5	4	20	Acceptable use policy for all ELC employees is to be refreshed by March 2018 and all employees will be expected to re-sign.	3	4	12	Head of Council Resources Service Manager - IT	March 2018	N/A	Risk reviewed and updated by IT management October 2017 with no change to score. Risk reviewed and updated by IT management October 2016 and with Current Risk score raised from 16 to 20 and residual score from 9 to 12 due to increase in current attacks in the UK. Risk refreshed December 2015 with Current score increased from 12 to 16 due to recent breaches. Risk refreshed November 2014 and Residual Risk Score increased from 6 to 9.
CR 4	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 who has resilient backbone in place.	3	5	15	Introduce a second link to Internet from network outwith Haddington. Note: Funding bid not successful in 2016/17 or 17/18.	1	5	5	Head of Council Resources Service Manager - IT	A bid will be made as part of current budget considerations for 2018/19.	N/A	Risk reviewed and updated by IT, October 2017 with no change to scores. Risk reviewed and updated by IT, October 2016.
CR 5	Risk of losing PSN accreditation which gives us connection to systems such as Blue Badge, Registrars of Scotland, DWP, Police etc. which could be caused by failure to comply with PSN Code of Connection and would seriously impact upon the business of the Council.	Complying with mandatory controls set by HMG to ensure we are able to meet government PSN Code of Connection.	3	5	15	Constant monitoring of code of connection and how we align with it. Keeping security and other devices up to date - patching etc. Successful completion of key Transformation Program Projects.	1	5	5	Head of Council Resources Service Manager - IT	March 2018 August 2018	N/A	Risk reviewed and updated by IT management, October 2017 with Likelihood raised in October 2017from 2 to 3 (15) reflecting results of 2017/18 health check. Risk reviewed and updated by IT, October 2016.

Risk ID	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	Impact	Risk Rating		Likelihood	Impact	Residual Risk Rating				
			L	I	L x I		L	I	L x I				
CR 6	Loss/Theft of IT Hardware covering mobile devices (laptops, mobile phones and blackberries), memory sticks, external drives etc. This risk creates potential compromise of our infrastructure, data loss and disclosure and is also a cost to ELC as mobile devices can be very expensive.	Mobile computing devices are encrypted which significantly reduces the risk of data stored on a stolen device being accessed. Mobile devices above a specified value are asset tagged and recorded on the IT asset database and allocated to a user. Responsibility for the safety of the device lies with the user/s. Business Units must keep a record or each mobile device they are allocated and ensure regularly that the device is still with the allocated user. If device cannot be found then this must be reported immediately to IT Service Desk so correct procedures for lost/stolen devices can take place. For shared/pool devices a responsible person in the business unit should be identified and should then ensure devices are signed out and back in when used. A count of devices must be taken regularly.	4	3	12	IT to communicate to all business units the need to maintain a record of each device, ensure each is with the allocated user, signed in and out if a shared device and regularly carry out a full check on all devices. This will be communicated via e-mail and ELNet initially and then repeated annually. Introduce Airwatch Mobile Device Management system to manage non Windows devices such as Tablets to enable them to be remotely wiped should they be reported as stolen	2	3	9	Head of Council Resources Service Manager - IT	March 2018 March 2018		Risk reviewed and updated by IT, Management October 2017 with no change to scores. Risk reviewed and updated by IT, Management October 2016. New risk created by Team Leader – Infrastructure & Security November 2015.
CR 7	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 and fines; - requirement to pay compensation; - adverse publicity; - damage to the Council's reputation. The Council's increased participation in shared services poses a risk for information security/data protection, as the council's network boundaries are being opened up to enable data sharing with other agencies. Any breaches could result in loss of PSN connection or fines from the Information Commissioner.	Arrangements for secure filing and storage of confidential papers. 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 Protection Policy in place. Revenues Information Security Procedure in place. Continual reviewing of arrangements. Maintaining staff awareness through team meetings, briefing sessions and health checks. Online Data Protection Training rolled out to all employees and repeated every 2 years. All known proposals to share information are scrutinised by the IT Security Officer and Information Governance Compliance Officer. Procurement Initiation documents check whether IT issues have been considered by new procurements. The Council has carried out a full programme of Information Security Awareness sessions within all schools.	3	4	12	Acceptable use policy for all ELC employees is to be refreshed by March 2018 and all employees will be expected to re-sign. Monitoring of take up of compulsory Data Protection training with service managers being alerted to those members of staff who have not completed up to date training.	3	3	9	Service Manager - Licensing, Admin & Democratic Services All managers.	March 2018 March 2018		Risk refreshed October 2017 by Service Manager with no change to assessment of score. Risk refreshed December 2015 with current score increased from 9 to 12 due to recent breach and involvement of Information Commissioner.

Risk ID	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	Impact	Risk Rating		Likelihood	Impact	Residual Risk Rating				
			L	I	L x I		L	I	L x I				
		Signed consent forms must be received before responding to complaints made by third parties. Security measures in place on CRM restricting access to complaints information. Regular contact with FOI/Data Protection Compliance Officer.											
CR 8	Failure of client services to comply with our procurement processes through lack of knowledge/experience 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 in place but require refresh. Purchase Card Procedures Procurement Improvement Panel (PIP) in place. Regular reporting to PIP and CMT. Procurement Skills Training carried out. Controls in place over New Suppliers. Supplier Finder on Intranet. Close working with internal audit and departments (Audited regularly). CMT ensuring improved compliance with existing Procurement Procedures by championing them and taking action when breaches are found. Contracts Register is now available and shall be made accessible for all Services. This should allow more effective work planning. Additional staff have been recruited (2.5 FTE posts). This will assist towards providing a centralised procurement service although in terms of recommended staffing the minimum recommended amount of staff for the spend of the Council should be 10 FTE.	3	4	12	Updated Procurement Strategy is to be put forward to Procurement Improvement Panel on 1st November and subsequently to Cabinet. Further work is required to ensure that more processes are in place and that those who are carrying out procurements without coming through the procurement team are identified. Utilising the Contracts Register together with monitoring processes adopted between finance and procurement team should allow clearer information coupled with a clear no purchase order no pay policy should reduce risks (the last matter may require new system investment but in the first instance training on current systems to adapt will be investigated). While Service Managers have accountability for budget allocation measures should be adopted to ensure that spend is in line with the original estimated spend (i.e. 10% increase as a limit). If this is to be approved authorisation from Service Manager (or Head of Service) together with either Service Manager for Legal & Procurement or Head of Council Resources to ensure there is a further check on the processes being properly followed, reliable pre tender data/estimates are obtained and that value for money is achieved. A review of standing orders relating to procurement may be necessary.	2	4	8	Service Manager – Legal & Procurement All ELC Service Managers	November 2017 October 2018 June 2018	N/A	Risk Refreshed October 2017 by Service Manager - Legal and Procurement with no change to score and new planned measure added.
CR 9	Committee meetings inquorate and cannot take place. Resulting in meetings being cancelled resulting in impact on Council reputation and failure to comply with statute. There is an increased likelihood of this scenario as the Council is operating with a minority administration and there has been a failure by the SNP group to nominate for some committees.	Employees carry out a double check on members' availability where necessary. Council approved an amendment to the Standing Orders for the quorum for Audit & Governance and Policy & Performance Review Committees to be amended, as a temporary measure, to state 'half + 1 of the places filled', rather than 'half + 1' to reduce the risk of meetings being inquorate and ensure the proper governance of the Council.	3	4	12	In response to the risk identified within the External Auditor's 2016/17 Audit Report, the Service Manager (LADS) has undertaken to review the current Scheme of Administration.	2	4	8	Service Manager Licensing, Administration & Democratic Services	February 2018		Risk Refreshed October 2017 by Service Manager - LADS with Current score increased from 8 to 12. Risk refreshed October 2016 with no change to scores.

Risk ID	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	Impact	Risk Rating		Likelihood	Impact	Residual Risk Rating				
			L	I	L x I		L	I	L x I				
CR 10	Council wide Catastrophic failure of central IT systems (incl. 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. The Council's increased participation in shared services escalates this risk as the council's network boundaries are being opened up to enable data sharing with other agencies.	Disaster Recovery Plan in place for major systems. Business Continuity plan in place - backup site for systems identified and core system backup plan created. All known proposals to share information are scrutinised by the IT Security Officer and Information Governance Compliance Officer.	2	5	10	Continual development of IT disaster recovery plan based on lessons learned from regular testing of existing plan.	1	4	4	Head of Council Resources Service Manager - IT	March 2018	N/A	Risk reviewed and updated by IT, October 2017 with no change to scores. Risk reviewed and updated by IT, October 2016.

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**
		1-4	**Low**

Version	Date	Author(s)	Notes on Revisions
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.
7	September 2013	S Kennedy	Slight alterations to risks by Head of Council Resources
8	October 2013	S Kennedy	Welfare Reform Risk updated by Task Group and Internal Audit Risk updated (no changes to risk rating).
9	December 2014/January 2015	S Kennedy	Legal and Procurement, Licensing, Administration & Democratic Services, I.T, HR/Payroll, Finance and Revenues & Benefits risks refreshed.
10	February 2015	S Kennedy	Finance Risks reviewed and refreshed and Benefits risks further refreshed.
11	December 2015	S Kennedy	Legal & Procurement, Revenues & Benefits, I.T. and HR & Payroll Risks refreshed.
12	February 2016	S Kennedy	Finance Risks reviewed and refreshed.
13	October 2016	S Kennedy	Revenues & Benefits, Legal & Procurement and I.T. Risks reviewed and refreshed
14	December 2016	S Kennedy	Customer Feedback Team Risks moved from Communities & Partnerships Register
15	September/October 2017	S Kennedy	Welfare Reform risk update from Corporate Risk Register and updates received from I.T., HR and Licensing, Admin & Democratic Services, Legal & Procurement, Revenue & Benefits

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	Legal
Catastrophic	5	Unable to function, inability to fulfil obligations.	Severe impacts on budgets (emergency Corporate measures to be taken to stabilise Council Finances)	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.	Significant disruption to building, facilities or equipment (Loss of building, rebuilding required, temporary accommodation required).	Complete inability to provide service/system, prolonged downtime with no back-up in place.	Catastrophic legal, regulatory, or contractual breach likely to result in substantial fines or other sanctions.
Major	4	Significant impact on service provision.	Major impact on budgets (need for Corporate solution to be identified to resolve funding difficulty)	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.	Major disruption to building, facilities or equipment (Significant part of building unusable for prolonged period of time, alternative accommodation required).	Significant impact on service provision or loss of service.	Legal, regulatory, or contractual breach, severe impact to Council.
Moderate	3	Service objectives partially achievable.	Significant impact on budgets (can be contained within overall directorate 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.	Moderate disruption to building, facilities or equipment (loss of use of building for medium period).	Security support and performance of service/system borderline.	Legal, regulatory, or contractual breach, moderate impact to Council.
Minor	2	Minor impact on service objectives.	Moderate impact on budgets (can be contained within service head's 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.	Minor disruption to building, facilities or equipment (alternative arrangements in place and covered by insurance).	Reasonable back-up arrangements, minor downtime of service/system.	Legal, regulatory, or contractual breach, minor impact to Council.
Minimal	1	Minimal impact, no service disruption.	Minimal impact on budgets (can be contained within unit's 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 media (Internal).	Minimal disruption to building, facilities or equipment (alternative arrangements in place).	No operational difficulties, back-up support in place and security level acceptable.	Legal, regulatory, or contractual breach, negligible impact to Council

Risk	Impact				
Likelihood	Minimal (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