East Lothian Council

REPORT TO: Audit and Governance Committee

MEETING DATE: 29 November 2016

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, 6 High risks, 26 Medium risks and 11 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 Paolo Vestri
DESIGNATION	Emergency Planning and Risk Officer Service Manager - Corporate Policy and Improvement
CONTACT INFO	skennedy@eastlothian.gov.uk 01620 827900 pvestri@eastlothian.gov.uk 01620 827320
DATE	17 November 2016

Council Resources Risk Register

Date reviewed: 17 November 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 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 • UC claimants need to make/maintain their claim online & make full-use their "journal". • The built in 7 day waiting period for the majority new UC claims • Extended processing times for UC claims, (min 32 days but potentially 42 days to 1st payment) • Additional demand for (SWF) Crisis Grants. (Risk of overspend) • The payment of UC Housing Costs direct to the claimant Increasing rent arrears for UC Claimants, (82% of ELC tenants claiming UC now in arrears), • The interruption of the established link between Housing Benefits and Council Tax Reduction, (previously claimed jointly) An increased risk of take up of Council Tax Reduction, (CTR), (7.6% reduction in CTR expenditure during 1st 2 quarters of 2016/17) • Risk of HB Admin' Subsidy reduction due to falling caseload. • Increased reliance on automated data transfer between DWP/JCP and the Council	The Council has received several update reports and will continue to be updated. The Council has established a Welfare Reform Task Group to plan for the changes to the welfare system. The Task Group has a detailed action plan to ensure that the Council takes the necessary measures to prepare for the changes to the welfare system. The Task Group and its work stream sub groups are continuing to meet regularly and will continue to report back to the Council Management Team and to the Council. The Benefit Service is continuing to make full use of additional Discretionary Housing Payment, (DHP) funding to mitigate for the impact of the removal of the spare room subsidy & other forms of housing related hardship wherever possible. DHP is now also the main potential source of mitigation for detriment caused by either the introduction of the Benefit Cap and/or in Temporary Accommodation cases which no longer receive the "management fees" element via UC housing costs. An impact analysis report (UC on rent collection) has been produced and has been considered by Senior Management. The ELC Chief Executive has written to the UC Project to highlight the impacts of the UCFS rollout of EL residents and Council Services. The ELC Chief Executive and Service Managers have met with the Universal Credit Director General to discuss ongoing concerns with the UCFS rollout The Benefit Service is monitoring it's SWF & DHP expenditure. Whilst the goal is to contain expenditure within the confines of the existing budgets the Service regularly reports on the risk of any potential overspend to the CMT & Elected Members. Revenues & Benefits Services engage in meetings between other colleagues, CoSLA and DWP/Job Centre Plus staff to ensure a managed transition to Universal Credit is achieved. Castle Rock HA providing personal budgeting support for East Lothian UC claimants.	5	4	20	A further update report to Council is being drafted. A report about the impact of UC on HB/CTR and Rent Income Performance will be submitted to PPRC. The ELC Chief Executive has agreed to send further correspondence to the UC Director General to highlight the continuing impacts of the UCFS rollout of EL residents and Council Services. The Revenues and Benefits Services stand ready to co-operate with a planned engagement with the DWP's Operational Excellence Group, (OEG). The Revenues and Benefits Services will continue monitor the development of the Scottish Social Security Agency and all potential forms of mitigation which may be deployed to tackle welfare detriment in Scotland. ELC Management & staff will continue to engage with JCP/DWP, CoSLA and Scottish Governments at a range of levels to ensure that all lessons are learned from the rollout of UC Full Service in East Lothian and are incorporated into future plans for welfare. Regular Budget Planning Meetings will be held with ELC Budget Advisor in order to factor in all known funding information to service budgets.	4	4	16	Depute Chief Executive – Resources and People Services	20 December 2016 11 January 2017 TBC TBC Review Report due by 31 March 2017 Initial Scottish Flexibilities April 2018, (TBC) Next CoSLA Welfare Advisors Group Meeting 18 November 2016 Next UC Full Service Workshop January 2017 Next Budget Planning meeting 17 November 2016 Scottish Government and DWP Funding announcements expected in December 2016 Natural Migration of Working Age HB Claims to UC due to be completed by 31 July 2019	9	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 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				
	• Previously agreed data sharing protocols no longer apply under UC “Full Service” (curtailing Council Officer’s ability to make telephone enquiries about UC claimant’s entitlement) • Temporary Accommodation management charges not being covered by UC Housing Costs • Increased demand for Discretionary Housing Payments, (DHP).risk of funding gap. • Insufficient Housing Costs information to facilitate DHP decisions, (increasing the burden of proof on the DHP claimant) • Concerns raised by Council Services over Job Centre Plus’ ability to support vulnerable claimants through the migration to UC • Early indications of UC becoming an increasing factor associated in instances of petty crime Other reforms which continue to pose significant risks include: • The removal of the spare room subsidy from those claiming housing benefit and under occupying their homes. This reform is also known as the 'bedroom tax'. • The introduction of a further Benefit Cap by the DWP, (from 7th November 2016) • Temporary Accommodation funding uncertainties. Efficient Workforce Management, restructures, budget restrictions and DWP/Scottish Government cuts could result in both the Revenues and Benefits services not being able to maintain levels of staff to allow the services currently provided to continue in their present form.	Approval was given in December 2015 for additional staffing resource within the Rent Income team to help manage the impact of UC on rent collection. 0.5FTE with immediate effect and provision made to increase establishment by 1 additional FTE in 2016/17 and 1 additional FTE in 2017/18, subject to management review. Recruitment has been ongoing to maintain current benefits establishment. 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). Promotion of ELC ‘Right Benefit Campaign’ objectives to maximise opportunity to qualify for FERIS incentive payments (to offset HB admin subsidy reductions). The Benefits & Financial Assessments Service Manager has joined the CoSLA Welfare Reform Advisor’s Group. Council Officers have engaged in the Scottish Government’s consultation process being carried out to inform plans for the devolved administration of up to 15% of the UK Welfare State. To-date this has included: • A substantial response to the SG’s consultation exercise. • Council Officers giving evidence to the Scottish Parliament’s Social Security Committee. The Revenues and Benefits Service Managers have attended PPRC to answer questions relating to the impact of the UC rollout on HB/CTR and Rent Collection performance.										

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 2017 and all employees will be expected to re-sign.	3	5	15	Head of Council Resources Service Managers - IT Infrastructure and IT Business Services	March 2017		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 2017 and all employees will be expected to re-sign.	3	4	12	Head of Council Resources Service Managers - IT Infrastructure and IT Business Services	March 2017	N/A	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: Capital funding bid not successful in 2016/17.	1	5	5	Head of Council Resources Service Manager - IT Infrastructure	Review November 2016 to make another bid for funding	N/A	Risk reviewed and updated by IT, October 2016.
CR 5	Loss/Theft of I.T. 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 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	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.	3	3	9	Head of Council Resources Service Managers - IT Infrastructure and IT Business Services	March 2017		Risk reviewed and updated by IT, Management October 2016. New risk created by Team Leader – Infrastructure & Security November 2015.

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				
		correct procedures for lost/stolen devices can take place. For shared/pool devices a responsible person in the business unit should be indentified and should then ensure devices are signed out and back in when used. A count of devices must be taken regularly.											
CR 6	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 Compliance Officer carrying out a programme of data protection health checks and the Data Protection Policy has been approved. 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 2017 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 2017 March 2017		Risk refreshed October 2016. Risk refreshed December 2015 with current score increased from 9 to 12 due to recent breach and involvement of Information Commissioner.
CR 7	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. 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.	3	4	12	Recruiting additional procurement staff to enable increased staff training and more focus on contract management and the improved contract management procedures.	2	4	8	Service Manager – Legal & Procurement All ELC Service Managers	January 2017	N/A	Risk Refreshed October 2016 by Service Manager - Legal and Procurement with no change to score and new planned measure added.

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 8	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.	2	5	10	Constant monitoring of code of connection and how we align with it. Keeping security and other devices up to date - patching etc.	1	5	5	Head of Council Resources Service Managers - IT Infrastructure and IT Business Services	March 2017	N/A	Risk reviewed and updated by IT, October 2016.
CR 9	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. 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 Managers - IT Infrastructure and IT Business Services	March 2017	N/A	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	All risks reviewed and refreshed.

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				
Likelihood	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