East Lothian Council

REPORT TO: Audit and Governance Committee

MEETING DATE: 24 November 2020

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 is 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 (Appendix 2) producing 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 1 Very High, 6 High risks, 23 Medium risks and 8 Low Risk. As per the Council's Risk Strategy only the Very High and High risks are being reported to the Committee.

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 LRWG 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 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 None.

Appendix 1 – Council Resources Risk Register 2020/21

Appendix 2 – Risk Matrix 2020

AUTHOR'S NAME	Scott Kennedy
DESIGNATION	Emergency Planning, Risk and Resilience Officer
CONTACT INFO	skennedy@eastlothian.gov.uk 01620 827900
DATE	12 November 2020

Council Resources Risk Register 2020/21

Date reviewed 12 November 2020

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	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	External IT Security Threats 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.	Firewalls in place External facing systems are vulnerability tested at least once a year Security logs are reviewed daily Comprehensive change control and IT security measures also in place to ensure confidentiality, integrity and availability of systems. Information security awareness training of employees provided council wide and awareness sessions carried out in schools. Regular software and data backups are taken. Work with National Cyber Security Centre to 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 Security systems under continuous review and patching to ensure they are still capable of controlling new and emerging threats.	4	5	20	Acceptable use policy for all ELC employees is to be refreshed by March 2021 and all employees will be expected to re-sign. This will include suitable rationale / guidance / training on the need for good practices and what they look like.	3	5	15	Team Manager – Infrastructure & Security	March 2021	Risk reviewed and updated by IT management September 2020 with no change to risk scores. 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	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	Internal IT Security Threats 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. Security logs are reviewed daily Comprehensive change control and IT security measures also in place to ensure confidentiality, integrity and availability of systems. Information security awareness training of employees provided council wide and awareness sessions held in schools. Regular software and data backups. Work with National Cyber Security Centre to 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 Continual vulnerability testing. Security systems under continuous review and patching to ensure they are capable of controlling new and emerging threats.	4	4	16	Acceptable use policy for all ELC employees is to be refreshed by March 2021 and all employees will be expected to re-sign. This will include suitable rationale / guidance / training on the need for good practices and what they look like.	3	4	12	Team Manager – Infrastructure & Security	March 2021	Risk reviewed and updated by IT management September 2020 with no change to risk scores. Risk reviewed and updated by IT management August 2019 with current score reduced from 20 to 16. 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.
CR 3	Data Breach Breach of Data Protection or other confidentiality requirements through the loss or wrongful transmission of information through for example: - private committee reports, minutes or correspondence being stored or disposed of inappropriately; - loss or misdirection of material during transit; - members of staff being unaware of their responsibilities in respect of confidential material and/or personal data; - intentional or malicious misuse of personal data; - lack of appropriate facilities for storage or disposal of material; Risks 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 shift to remote and home working in response to the COVID-19 crisis has	Secure filing and storage of confidential papers and 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. Checks on documents are made by a second clerk when relevant documents are uploaded to internet. Data Protection Policy 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. A record of all breaches and near misses is being maintained to inform learning and identify areas of concern	4	4	16	Acceptable use policy for all ELC employees is to be refreshed by March 2021 and all employees will be expected to re-sign. This will include suitable rationale / guidance / training on the need for good practices and what they look like. 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. Information Asset Register to be developed that links all Data Protection Impact Assessments, Data Sharing Agreements and Data Processing Agreements templates to be revised to make them more flexible and user-friendly. Re-assessment of records management arrangements to be completed in line with the requirements of the Public Records (Scotland) Act 2011, including assessment and recommendations for Dunbar Road records store.	3	3	9	Team Manager – Information Governance Team Manager – Infrastructure and Security	March 2021 June 2021 June 2021 June 2021 June 2021	Risk refreshed October 2020 by Team Manager-Information Governance in October 2020 with increase in Current Score from 12 to 16 based on COVID-19 impact. 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	Evidence held of Regular Review
			Likelihood	Impact	Risk Rating		Likelihood	Impact	Residual Risk Rating			
			L	I	L x I		L	I	L x I			
	increased the risk of data breaches due to rapid deployment of new procedures, changing existing paper-based processes to digital ones, and shifting almost entirely to digital communications. This fundamentally increases the amount of personal information being captured in recorded form, increases the risk that personal data may be lost or misdirected and increases the Council's reliance on digital information security measures to protect data. The COVID-19 crisis itself has increased the risk of data breaches, as staff must respond rapidly to continuously changing circumstances and they have less time and capacity to perform routine checks e.g. when sending personal data externally. Since March 2020, the Council has recorded a marked increase of data breaches of varying level of severity, the majority of which have involved the misdirection of personal data under new processes/procedures. Some of these have involved delays to reporting incidents internally to the DPO/Data Breach Team. 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. Paper records storage facilities (excluding the Council Archives) do not currently have sufficient access, file tracking or disaster management controls to prevent unauthorised access or accidental loss of personal data. Paper records storage procedures are not consistently applied across the Council. Any breaches could result in loss of PSN connection or fines from the Information Commissioner. Failure to improve records management arrangements could result in non-compliance with the Public Records (Scotland) Act 2011.	Data Protection Impact Assessments being completed for all business processes that involve personal information. Data Sharing Agreements being put in place for all personal information being shared. Data Processing Agreements being put in place with bodies that are processing personal information on ELC behalf. Data Protection/Information Security awareness campaign under development jointly by Information Governance, Information Security and Communications teams. All known proposals to share information are scrutinised by the IT Team Manager – Infrastructure and Security and Team Manager-Information Governance. Procurement Initiation documents check whether IT issues have been considered by new procurements. Report under draft addressing risks at Dunbar Road records store and identifying options for improvements.				Revise our disciplinary policy and procedures to ensure that a deliberate data breach is a clear disciplinary matter attracting major sanctions as gross misconduct. Data Protection Impact Assessment template to be revised to make it more flexible and user-friendly and encourage increased use by staff.					June 2021	
CR 4	Loss of Internet Connectivity 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 in Haddington. Introduce a third link to Internet from network outwith Haddington.	1	5	5	Team Manager – Infrastructure & Security	December 2020 March 2021	Risk reviewed and updated by IT management September 2020 with no change to risk 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	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 5	Client services & procurement processes 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. Loss of further functionality to contract register due to upgrades to the main platform would lead to non-compliance and disproportionately increased administrative workload as well as failure to provide efficient procurement services.	Corporate Procurement Strategy for period 2017 to 2022 adopted and in place along with Procedures. This is reviewed on an annual basis and updated as required. Purchase Card Procedures and 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. Additional approval within procurement for single source applications is in place. 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 manually managed and distribution of up to date contract list is done quarterly. Measures are adopted to ensure appropriate budget is in place for procurement project initiated by Services through Finance budget approval of PID documents before the initiation of a project	3	4	12	There is a plan to link Purchase orders and payments to contract reference number to allow traceability, transparency and benefit tracking. This will also reduce risk maverick spend. The 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). In the event that the tender price following a procurement exercise is greater than 10% of the original estimate spend then authorisation for the award of the tender will be required from the relevant Service Manager or Head of Service together with Service Manager for Finance. Further measures are required to be implemented by the contracting Service following the award of the contract in which the Service will report back to Procurement to ensure further checks that the terms of the contract continue to be followed and best value is achieved. Research and plan implementation of a suitable contract register with at least basic procurement service support functions.	2	4	8	Commercial Programme Manager	October 2021 March 2022 December 2020 October 2021	Risk Refreshed September 2020 by Commercial Programme Manager with no change to score and new planned measure added.
CR 6	Loss of PSN Accreditation 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.	Continual monitoring of code of connection. Complying with mandatory controls set by HMG. Patching regime in place.	2	5	10	Successful completion of Online Customer Platform to replace CRM system.	1	5	5	Team Manager – Infrastructure & Security	December 2021	Risk reviewed and updated by IT management September 2020 with no change to risk scores. Risk reviewed and updated September 2019 - current score reduced from 15 to 10 due to patching regime now in place.
CR 7	Catastrophic failure of central IT systems 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.	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	2	5	10	Review of IT disaster recovery plan based on lessons learned from regular testing of existing plan.	1	4	4	Team Manager – Infrastructure & Security	March 2021	Risk reviewed and updated by IT management September 2020 with no change to risk scores. Risk refreshed by Team Manager

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	Evidence held of Regular Review
			Likelihood	Impact	Risk Rating		Likelihood	Impact	Residual Risk Rating			
			L	I	L x I		L	I	L x I			
	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.	and Information Governance Compliance Officer.										August 2019 with no change to assessment of current scores.

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