

REPORT TO: Audit and Governance Committee

MEETING DATE: 29 November 2022

BY: Chief Executive

SUBJECT: Corporate Support Risk Register

1 PURPOSE

- 1.1 To present to the Audit and Governance Committee the Corporate Support Risk Register (Appendix 1) for discussion, comment and noting.
- 1.2 The Corporate Support 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 Corporate Support Local Risk Working Group (LRWG).

2 RECOMMENDATIONS

- 2.1 It is recommended that the Audit and Governance Committee notes the Corporate Support 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 Corporate Support risks 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 Corporate Support 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 Corporate Support 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 Corporate Support Risk Register includes 1 Very High, 4 High, 12 Medium and 13 Low risks. 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 Corporate Support 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 – Corporate Support Risk Register 2022-23

Appendix 2 – Risk Matrix

AUTHOR’S NAME	Scott Kennedy	
DESIGNATION	Emergency Planning, Risk and Resilience Officer	
CONTACT INFO	skennedy@eastlothian.gov.uk	01620 827900
DATE	17 November 2022	

Corporate Support Risk Register 2022-23

Date reviewed 17 November 2022

Risk ID	Risk Category	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]			Planned Control Target Date	Evidence held of Regular Review
				Likelihood	Impact	Risk Rating		Likelihood	Impact	Residual Risk Rating		
				L	I	L x I		L	I	L x I		
Corp 1	Reputational	<p>External IT Security Threats</p> <p>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.</p> <p>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.</p> <p>Heightened Risk Due to War in Ukraine Due to the current conflict in Ukraine there is a heightened risk of Nation State led cyberattacks on the West. These could potentially affect National Infrastructure such as data and voice networks which could have an impact on East Lothian Council.</p>	<p>Firewalls in place.</p> <p>External facing systems are vulnerability tested at least once a year.</p> <p>Security logs are reviewed daily.</p> <p>Comprehensive change control and IT security measures also in place to ensure confidentiality, integrity and availability of systems.</p> <p>Information security awareness training of employees provided council wide and awareness sessions carried out in schools.</p> <p>Regular software and data backups are taken.</p> <p>Work with National Cyber Security Centre to keep up to date with new and emerging threats.</p> <p>Ensure purchase of secure systems and maintain security through system life cycle.</p> <p>The Council complies with ISO27001 the International standard for Information Security.</p> <p>Security systems under continuous review and patching to ensure they are still capable of controlling new and emerging threats.</p> <p>Intrusion Detection System implemented.</p> <p>All Council Services advised to review and update Business Continuity Plans to allow for potential period of up to 2 weeks without IT systems.</p>	5	4	20	<p>Acceptable use policy for all ELC employees has been refreshed and is currently with Joint Trades Unions for consultation. Will be implemented in 2022 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.</p>	3	4	12	November 2022	<p>Risk reviewed and updated by Service Manager – IT, October 2022 with no change to risk scores.</p> <p>Risk reviewed and updated by IT Management in March 2022 in light of war in Ukraine with Current Impact reduced to 4 thanks to the Intrusion Detection System, however, Likelihood increased to 5 due to conflict in Ukraine. Residual score reduced from 15 to 12.</p>

Risk ID	Risk Category	Risk Description (Threat/Opportunity to achievement business objective)	of	Risk Control Measures (currently in place)	Assessment of Current Risk			Planned Risk Control Measures	Assessment of Residual Risk [With proposed control measures]			Planned Control Target Date	Evidence held of Regular Review
					Likelihood	Impact	Risk Rating		Likelihood	Impact	Residual Risk Rating		
					L	I	L x I		L	I	L x I		
Corp 2	Reputational	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. Intrusion Detection System implemented.	4	4	16	Acceptable use policy for all ELC employees has been refreshed and is currently with Joint Trades Unions for consultation. Will be implemented in 2022 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	November 2022	Risk reviewed and updated by Service Manager – IT, October 2022 with no change to risk scores. Risk reviewed and updated by IT management August 2019 with current score reduced from 20 to 16.
Corp 3	Reputational Financial Psychological impact (data subjects)	Data Breaches / Compliance Breach of personal data through: - accidental disclosure or loss of personal data in transmission; - lack of staff awareness - intentional or malicious misuse of personal data; - lack of appropriate provisions for storage or disposal of personal data; 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 risks initially posed by the COVID 19 pandemic have reduced as staff have settled into new ways of working. The Council's pandemic response has fundamentally shifted the workforce to more digital service delivery in the longer term, and changes to working practices continue to evolve, meaning approaches to information governance must remain resilient. Ongoing changes such as the Asset Review require significant information governance input to support secure destruction, transfer and digitisation of the		Data Protection Policy, IT Acceptable Use Policy and associated guidance/procedures available to all staff via ELnet; Data Breach Procedure addresses timely containment, reporting and recording of breaches; Records Management Plan / Information and Records Management Policy, including confidential waste procedures/bins; Information Security Management System (ISMS) in line with ISO27002; Mandatory e-learning for all staff in Data Protection and Information Security, refreshed every 2 years; Data Protection Impact Assessments completed and assessed by DPO/Information Security for all business processes involving personal information; Data Sharing Agreements put in place for all regular sharing of personal data; Recruitment to additional Information Officer post to support Information Governance input into corporate projects and establish digital preservation provisions. Data Protection/Information Security awareness campaign under development jointly by Information Governance, Information Security and Communications teams;	4	4	16	Acceptable use policy for all ELC employees has been refreshed and is currently with Joint Trades Unions for consultation. Will be implemented in 2022 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. Information Asset Register continues to be developed via workshops with Service Areas. Data Sharing Agreement templates to be revised to make them more flexible and user-friendly. 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 Breach Dashboard currently in development to support high-level reporting to senior managers re: trends in data breaches and contributing factors. Creation of new Team Leader – Information Governance post in progress to act as depute DPO and lead on Information Governance process development.	3	3	9	November 2022 January 2023 January 2023 January 2023	Risk reviewed and updated by Service Manager, IT and Team Manager-Information Governance in October 2022 with no change to scores. Risk refreshed October 2021 by Team Manager-Information Governance with increase in Current Score from 12 to 16 based on COVID-19 impact.

Risk ID	Risk Category	Risk Description (Threat/Opportunity to achievement business objective)	Risk Control Measures (currently in place)	Assessment of Current Risk			Planned Risk Control Measures	Assessment of Residual Risk [With proposed control measures]			Planned Control Target Date	Evidence held of Regular Review
				Likelihood	Impact	Risk Rating		Likelihood	Impact	Residual Risk Rating		
				L	I	L x I		L	I	L x I		
		<p>high volume of paper records still held by the Council and application of security and records management controls.</p> <p>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.</p> <p>Any breaches could result in loss of PSN connection or fines from the Information Commissioner.</p> <p>Failure to improve records management arrangements could result in non-compliance with the Public Records (Scotland) Act 2011.</p>	<p>Annual PUR update on Records Management arrangements submitted to the national regulator (the Keeper);</p> <p>Short-term contract in place with document management Supplier Oasis to manage storage/retrieval of high volume of records being transferred out of offices due to Asset Review.</p>				<p>Following approval of Digital Strategy c.December 2023, procurement exercise to identify best value for document management services to improve storage, security and service improvement.</p>				<p>January 2023</p> <p>April 2023</p>	
Corp 4	<p>Business Continuity</p> <p>Service Objectives</p> <p>Financial</p>	<p>Legal Service Staffing</p> <p>An unplanned loss of a key employee or employees due to resignation, long-term sickness absence etc. such as Senior Solicitors may affect the quality and scope of the legal service resulting in a failure to meet statutory objectives and provide an adequate legal service.</p> <p>The current inability (November 2022) to fill the Team Manager and the Senior Solicitor (Commercial) roles had already placed additional pressures on the team. This was compounded by the resignation of the Senior Solicitor (Litigation) who left at the end of October. Service requirements have been further reviewed and a recruitment campaign for a Principal Solicitor (Litigation) post, Senior Solicitor (Litigation), Principal Solicitor (Commercial) and Solicitor (Property) were advertised with the Principal Solicitor (Litigation) and Senior Solicitor (Litigation) posts being filled. The successful candidates were internal therefore resulting in two vacant Solicitor (Litigation) posts for which recruitment campaigns are being progressed.</p> <p>Due to this lack of resource and increased demand for Legal Services the team continue to find it difficult to fulfil service requests timeously without considering outsourcing at an additional cost to the Council.</p> <p>The increased workload falling on the remaining members of the team may result in further absence due to stress.</p> <p>Outsourcing legal work to external firms incurs unbudgeted costs for client services, which can be significant for complex matters.</p>	<p>Succession planning has been developed and rolled out to share the knowledge ensuring there are now at least two team members in each area of work with sufficient knowledge to ensure continuity of the service.</p> <p>An ability to employ temporary employees if required and an ability to outsource to acquire external legal advice. In addition if further advice/specialist advice is required there is access to the Edinburgh's Legal Services Framework to obtain appropriate external legal support.</p> <p>An expedited Service Review has been conducted to improve capacity across the team which included a new Property Solicitor to support the asset rationalisation project which will provide additional capacity to the team, if it can be filled.</p> <p>To ensure there is a clear record of transactions being carried out the legal team maintain individual work plans, which are reviewed by the Service Manager monthly.</p> <p>Standard Processes are in place which the team are able to follow. These processes are also agreed with the relevant Services to ensure that there remains consistent processes between the Legal Department and the Service and vice versa (primarily within the litigation side of the team).</p> <p>Additional capacity has been created within the legal services team with a refocus of one solicitor's post to assist with increased requirement of legal work for Commercial and Property.</p> <p>East Lothian Council is able to access legal services through the Edinburgh Legal Services Framework arrangement.</p>	4	4	16	<p>On a temporary basis consideration will be given to bringing in suitably qualified solicitors through agencies and/or outsourcing to external legal firms. While these may assist these people may require training etc. which will take some time.</p> <p>To ensure capacity within the team remains on a long-term basis the priority is to fill the current vacant posts.</p>	3	3	9	<p>December 2022</p> <p>February 2023</p>	<p>Risk Reviewed and updated by Service Manager – Governance September 2022 with Current Score increased from 9 to 16 due to loss of staff.</p> <p>Risk Reviewed and updated by Service Manager – Governance December 2021 with Current Score increased from 6 to 9 due to knowledge held by key employees.</p>

Risk ID	Risk Category	Risk Description (Threat/Opportunity to achievement business objective)	of	Risk Control Measures (currently in place)	Assessment of Current Risk			Planned Risk Control Measures	Assessment of Residual Risk [With proposed control measures]			Planned Control Target Date	Evidence held of Regular Review
					Likelihood	Impact	Risk Rating		Likelihood	Impact	Residual Risk Rating		
					L	I	L x I		L	I	L x I		
Corp 5	Legal & Regulatory	<p>Legal Advice</p> <p>Giving inaccurate or incorrect legal advice or failing to give appropriate legal advice could result in the Council failing to comply with its statutory duties and/or acting ultra vires leading to legal action and loss of reputation.</p> <p>Due to current staff shortages the team may not have the resource to comply with all of the mitigation measures at any given time which may lead to mistakes being made either in advice or in process.</p>		<p>Access to relevant on line legal sources such as Westlaw, Nexis Lexis, Practical Law Company etc.</p> <p>Regular monitoring of Scottish Government/Scottish Parliament websites together with checks on Scottish Courts, Sherriff Officer and Scottish Law Society websites for any updates on legislation or guidance.</p> <p>Participation in the Society of Local Authority Regulators (SOLAR) working groups and sub-committees.</p> <p>Retaining a full complement of qualified employees.</p> <p>An expedited Service Review has been conducted to improve capacity across the team which included a new Property Solicitor to support the asset rationalisation project which will provide additional capacity to the team, if it can be filled.</p> <p>East Lothian Council is able to access legal services through the Edinburgh Legal Services Framework arrangement. As part of this arrangement there is are seminars made available to East Lothian Council legal team and relevant services at no additional cost, which assists in continuing professional development for the legal team.</p> <p>There is standard protocol and methods in place to deal with day to day business with services to ensure consistent approach is adopted from all members of the team. There are regular team meetings (twice per week) providing a strong team awareness of what each member of the team is working on in any particular week. Also discussing approach and seeking comments from the team as necessary.</p> <p>Regular monitoring of workloads.</p> <p>Succession/Leave planning, sharing the knowledge amongst all employees.</p> <p>Outsourcing for appropriate specialist advice when applicable.</p> <p>Maximising access to free training events.</p>	3	4	12	<p>On a temporary basis consideration will be given to bringing in suitably qualified solicitors through agencies and/or outsourcing to external legal firms. While these may assist these people may require training etc. which will take some time.</p> <p>To ensure capacity within the team remains on a long-term basis the priority is to fill the current vacant posts.</p>	3	3	9	<p>December 2022</p> <p>February 2023</p>	<p>Risk Reviewed and updated by Service Manager – Governance September 2022 with current score increased from 8 to 12.</p>

East Lothian Council Risk Matrix

Likelihood Description

Likelihood of Occurrence	Score	Description
Almost Certain	5	>90% chance of occurring
Probable	4	70%-90% chance of occurrence
Possible	3	30-70% chance of occurring
Unlikely	2	10-30% chance of occurring
Rare	1	<10% chance of occurring

Impact Description

Impact of Occurrence	Score	Description							
		Impact on Service Objectives	Financial Impact	Physical and/or Psychological Impact on People	Impact on Time	Impact on Reputation	Impact on Assets	Business Continuity	Legal & Regulatory
Catastrophic	5	Catastrophic failure in service delivery and key service standards are not met, long-term catastrophic interruption to operations, several major partnerships are affected	Severe impacts on budgets (emergency Corporate measures to be taken to stabilise Council Finances. Consideration should be given as to whether this is an insured or uninsured risk and whether there may be reliance on reserves. The Council is expected to hold a reserve to budget ratio of 2%.	Single or Multiple fatality and or psychological impact, within council control, leading to 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. Prolonged regional and national condemnation.	Significant disruption to building, facilities, vehicles or equipment (Loss of building, vehicles, rebuilding required, temporary accommodation required, vital equipment lost without replacement capability available resulting in services being unable to be delivered).	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, including substantial involvement from regulators.
Major	4	Major impact to service quality, multiple service standards are not met, long-term disruption to operations, multiple partnerships affected.	Major impact on budgets (need for Corporate solution to be identified to resolve funding difficulty). Consideration should be given as to whether this is an insured or uninsured risk and whether there may be reliance on reserves.	Number of extensive injuries (major permanent harm) or major psychological impact to employees, service users or public.	Major - between 1 & 2 years to recover pre-event position.	Serious negative national or regional criticism and publicity.	Major disruption to building, facilities, vehicles or equipment (Significant part of building unusable for prolonged period of time, alternative accommodation required, equipment or vehicles unavailable to provide significant elements of service delivery and no appropriate contingency arrangements in place).	Significant impact on service provision or loss of service.	Legal, regulatory, or contractual breach, severe impact to Council, fines and regulatory action publicly enforced.
Moderate	3	Significant fall in service quality, major partnership relationships strained, serious disruption in service standards.	Moderate impact on budgets (can be contained within overall directorate budget).	Serious injury requiring medical treatment or moderate psychological impact 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.	Adverse national media public attention with elected members becoming involved.	Moderate disruption to building, facilities, vehicles or equipment (loss of use of building for medium period, loss of equipment or vehicles requires contingency arrangements to be employed and has moderate impact on overall service delivery).	Security support and performance of service/system borderline.	Legal, regulatory, or contractual breach, moderate impact to Council, regulator action and or improvement required of the Council .
Minor	2	Minor impact to service quality, minor service standards are not met, short-term disruption to operations, minor impact on a partnerships	Minor impact on budgets (can be contained within service head's budget).	Non life changing injury or psychological impact to staff or member of the public requiring treatment.	Some - between 2 and 6 months to recover.	Minor adverse local, public or media attention and complaints.	Minor disruption to building, facilities, vehicles or equipment (alternative arrangements in place and covered by insurance, equipment or vehicles unavailable for small period of time minor impact on service).	Reasonable back-up arrangements, minor downtime of service/system.	Legal, regulatory, or contractual breach, minor impact to Council, regulator advice and improvement requested of the Council.
Minimal	1	No impact to service quality, limited disruption to operations.	Minimal impact on budgets (can be contained within unit's budget).	Minor injury or minor psychological impact to employee, service user or public.	Minimal - Up to 2 months to recover.	Public concern restricted to local complaints and of no interest to the media.	Minimal disruption to building, facilities, vehicles or equipment (alternative arrangements in place, equipment or vehicles alternative quickly available to replace or substitute).	No operational difficulties, back-up support in place and security level acceptable.	Legal, regulatory, or contractual breach, negligible impact to Council, regulator suggested improvements requested.

Risk	Impact				
	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
------	-----	--------	------	-----------

