East Lothian Council

REPORT TO: Audit and Governance Committee

MEETING DATE: 22 March 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 1 Very High risk, 8 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 EQUALITIES IMPACT ASSESSMENT

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

6 RESOURCE IMPLICATIONS

6.1 Financial – It is the consideration of the Council Resources 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	10 March 2016

Council Resources Risk Register

Date reviewed: 10 March 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	Council IT systems are compromised by criminal 3rd party (e.g. hacker, terrorism) - causing the loss of a system, virus/trojan infection or loss/disclosure of data. This potentially could have a serious impact on one or more Council services. A recent breach of security (November 2015) has highlighted that we are at heightened risk at this moment in time and HMG are classing the risk as severe which could result in loss of PSN connection or fines from the Information Commissioner. At the time of this update (Dec-15) the Council's Corporate Internet pipe was under a DDOS attack and has been for 5 days. This is a Scotland wide issues which is affecting all LA's and highlights the risk faced at this time.	Systems are protected from outside world by firewall (the corporate firewall hardware was renewed in October 2014). 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. Info sec awareness training of employees to ensure they are aware of risks. Continue to take regular software and data backups to allow systems and data to be restored, following any failure. Regular awareness training of employees' council wide. Continue and constantly improve security measures. Keep up to date with new and emerging threats. Ensure we purchase secure systems and maintain security throughout the system life cycle. 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). Keep security hardware and software up to date to mitigate risk. 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.	4	5	20	Following the recent breach the Council is planning a programme of Information Security Awareness sessions within all schools. Acceptable use policy for all ELC employees is to be refreshed during 2016 and all employees will be expected to sign.	3	5	15	Head of Council Resources	December 2016 July 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 2	**Welfare reform** The UK Government is continuing to introduce a range of measures to reform the welfare system and reduce the budget for welfare benefits. It is expected that East Lothian residents will continue to experience financial detriment as a result of ongoing changes. The rollout of Universal Credit in East Lothian started in April 2015. Whilst the volumes of new cases hasn't been as high as initially expected, the workload created by this change has been significant and has so far been managed within existing resource. The current working arrangements may not be sustainable once volumes match JCP/DWP projections and it is predicted that considerable investment in additional staffing resource will be required. The DWP will introduce its Full 'Digital' Universal Credit service in East Lothian on 23rd March 2016. This will see UC payment extended to all eligible claimants/households and will increase the live UC caseload significantly. It is anticipated that new claims to legacy benefits will be closed once claimants begin their transition to UC; Migration to Universal Credit of existing HB cases is expected to follow from July 2018. When full implementation of Universal Credit has been achieved (expected to be by 2018/19), it is estimated that the Council's Rent Income team would have to collect an additional £8.3m per annum from claimants whose rent is currently paid direct to their rent account by housing benefit. A reform which continues to pose a significant risk to rent collection is 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'. Whilst this has been mitigated by funding made available by the Scottish Government there is a risk that this funding may still be inadequate for alleviating Housing related hardship and may not be sustainable in the longer term. Following the publication of the Smith Report recommendations the Scottish Government is considering how it may use its devolved powers provided for within the Scotland Bill (yet to be enacted). The outcome of these deliberations will introduce Scottish flexibilities to the delivery of UC in Scotland. Within the business areas covered by Council Resources, further changes could	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. Up until now the work of the group has been based around communications; data sharing; training; and migration to the new benefits system such as the establishment of the Scottish Welfare Fund. However, the focus of the group will change as welfare reform evolves further. 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 and other forms of housing related hardship wherever possible. An impact analysis report (UC on rent collection) has been produced and has been considered by Senior Management. The Welfare Reform Task Group, Welfare Reform Reference Group and Welfare Reform Liaison Group will all continue to implement their action plans to mitigate the impact of welfare reform. The Benefit Service will continue to monitor it's DHP expenditure and will regularly report the extent of any potential overspend to the CMT & Elected Members. Revenues & Benefits Services engage in meetings between other colleagues 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. 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	4	4	16	Both the Revenues and Benefits Services will monitor the progress of the Scotland Bill recommendations and will engage in any consultation relating to its findings on further devolution of welfare.	4	4	16	Depute Chief Executive – Resources and People Services	Under constant review.	9	Risk refreshed by Service Managers – Revenues & Benefits March 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				
	lead to: • Increase in rent arrears from reduced assistance with Housing costs and possible increase in evictions • increased pressures on rent collection teams • increase in Council Tax arrears and non-payment of Council Tax • increase in Business Rates arrears and non-payment of Business Rates • continued loss of income the Council currently receives for administering Housing Benefits • an overspend of DHP if/when the Scottish Government fail to fully reimburse the Council for its expenditure relating to mitigation of the spare room subsidy. • Increasing footfall/demand for sign-posting, help and advice from customers who are required to claim Universal Credit and confused about which agency provides assistance with housing costs. 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.	current benefits establishment. Promotion of ELC 'Right Benefit Campaign' objectives to maximise opportunity to qualify for FERIS incentive payments (to offset HB admin subsidy reductions).											
CR 3	Council IT systems are compromised by the actions of an internal employee - causing the loss of a system, virus/trojan infection or loss/disclosure of data. This potentially would have a serious impact on the business of the Council. A recent breach of security (November 2015) has highlighted that we are at heightened risk at this moment in time and HMG are classing the risk as severe which could result in loss of PSN connection or fines from the Information Commissioner.	Internal IT Systems are protected by antivirus, group policy etc. Employees sign the Acceptable Usage Policy and are party to various HR policies and legislation such as the Data Protection Act and Computer misuse act. Info security awareness, HR and Data Protection training etc is provided for employees. Continue to take regular software and data backups to allow systems and data to be restored, following any failure. Continue and constantly improve security measures. Keep up to date with new and emerging threats. Ensure we purchase secure systems and maintain security throughout the system life cycle. 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). Continuous review and upgrading of security systems to ensure they are still capable of controlling new and emerging threats.	4	4	16	Following the recent breach the Council planned a programme of Information Security Awareness training sessions within all schools as part of "in service" training. Several sessions have already been delivered by the Data Protection Compliance Officer and IT as part of a rolling programme that will be completed in May. The schools themselves are to cascade training to whoever has not been able to attend a session and are to instruct their staff to complete the compulsory online training module. Acceptable use policy for all ELC employees is to be refreshed during 2016 and all employees will be accepted to resign.	3	3	9	Head of Council Resources	May 2016 June 2016 July 2016	N/A	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.

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 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. At the time of this update (Dec-15) the Council's Corporate Internet pipe was under a DDOS attack and has been for 5 days. This is a Scotland wide issues which is affecting all LA's and highlights the risk faced at this time.	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.	1	5	5	Head of Council Resources	March 2018	N/A	Risk refreshed December 2015 with Current score increased from 10 to 15 due to current attacks.
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 certain cost are asset tagged and recorded on our asset database and allocated to a user. Some may be shared resources. Responsibility for the safety of the device lies with the user/s.	4	3	12	IT must ensure all mobile assets are tagged and entered into asset database. When handing out devices to users an allocated person in the business unit must then be documented as having responsibility for control of the asset. This person is then responsible for the asset during its lifecycle. If they pass they asset on to another user they must inform IT immediately to ensure the asset database is updated accordingly. 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 indentified and should then ensure devices are signed out and back in when used. A count of devices must be taken regularly.	3	3	9	Head of Council Resources	March 2017		New risk created by Team Leader – Infrastructure & Security November 2015
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.	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	3	4	12	Following the recent breach the Council is planning a programme of Information Security Awareness sessions within all schools. Acceptable use policy for all ELC employees is to be refreshed during 2016 and all employees will be expected to re-sign.	3	3	9	Service Manager - Licensing, Admin & Democratic Services All managers.	December 2016 July 2016		Risk refreshed December 2015 with current score increased from 9 to 12 due to recent breach and involvement of Information Commissioner. Risk refreshed by Data Protection / F.O.I Compliance Officer December 2014 and risk score reduced from 12 to 9 thanks to planned measures now implemented.

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				
	A recent breach of security (November 2015) has highlighted that we are at heightened risk at this moment in time and HMG are classing the risk as severe which could result in loss of PSN connection or fines from the Information Commissioner.	meetings, briefing sessions and health checks. Online Data Protection Training rolled out to all employees and repeated every 2 years.											
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 including pre-qualification of suppliers 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). Annual Procurement Capability Assessment in place and action plan progressed. CMT ensuring improved compliance with existing Procurement Procedures by championing them and taking action when breaches are found.	3	4	12	Improved contract management procedures to be put in place in tandem with continuing to improve procurement practices.	2	4	8	Service Manager – Legal & Procurement All ELC Service Managers	April 2016	N/A	Risk Refreshed November 2015 by Service Manager - Legal and Procurement.
CR 8	Risk of losing PSN accreditation which gives us connection to systems such as Blue Badge, Registrars of Scotland, DWP, Police etc. This would be caused by failure to comply with PSN Code of Connection and could 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	December 2016	N/A	New risk created November 2015.
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.	Business Continuity plan in place - backup site for systems identified and core system backup plan created.	2	5	10	Continual development of IT disaster recovery plan based on lessons learned from regular testing of existing plan. Ensure IT Staff know their role in event of a disaster.	1	4	4	Head of Council Resources	April 2016	N/A	Risk refreshed November 2015.

Original date produced (Version 1)	19th December 2011			**Risk Score**	**Overall Rating**
File Name	CH&PM Risk Register			**20-25**	**Very High**
Original Author(s)	Scott Kennedy, Risk Officer			**10-19**	**High**
Current Revision Author(s)	Scott Kennedy, Risk Officer			**5-9**	**Medium**
Version	**Date**	**Author(s)**	**Notes on Revisions**	**1-4**	**Low**
1	19/12/2011	S Kennedy	Original Version		
2	31/05/2012	S Kennedy	IT Risks updated by S Buczyn and Register revised following Senior Management Restructure		
3	19/11/2012	S Kennedy	Updated following update of Risk Strategy		

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				
	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.								

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