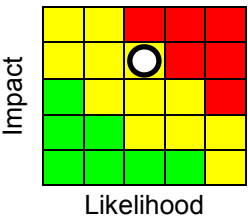
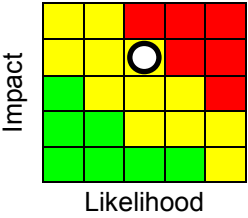
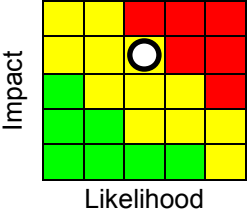
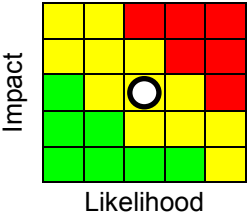
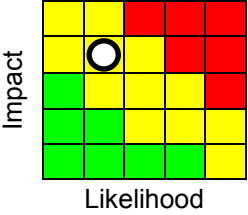


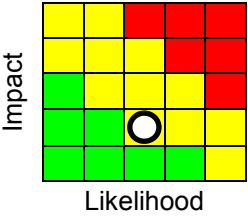
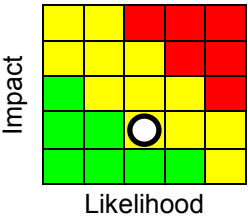
## Corporate and Community Services Risk Register

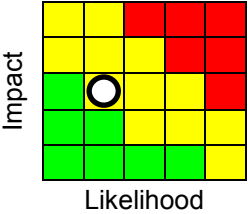
Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
<b>WDC Generic Risks</b>				
<p>1. Failure to meet "Fit for the Future" Objectives.</p>	<ul style="list-style-type: none"> <li>i. Legislative changes.</li> <li>ii. Policy changes.</li> <li>iii. Financial changes.</li> <li>iv. Service changes.</li> <li>v. Organisational changes.</li> <li>vi. Key people changes.</li> </ul>	<ul style="list-style-type: none"> <li>i. Overspending on Medium Term Financial Strategy.</li> <li>ii. Reduction in service levels for customers.</li> </ul>	<ul style="list-style-type: none"> <li>i. Specific focus on statutory compliance and statutory consultation requirements.</li> <li>ii. Early engagement with recognised Trade Unions and staff.</li> <li>iii. Supportive / good Member relationships with Executive and PF Holders.</li> <li>iv. Comprehensive redundancy &amp; redeployment policies</li> <li>v. Review of C&amp;CS – Project managers, prioritisation of FFF project work, SMT as programme board</li> <li>vi. Clear budget monitoring process.</li> </ul>	<p style="font-size: small; margin-top: 5px;">Impact</p> <p style="font-size: small; margin-top: 5px;">Likelihood</p>

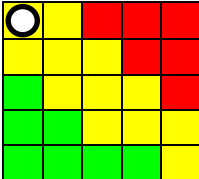
Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
<p>2. Growth within Warwick District outstrips the ability for the Council to deliver services.</p>	<ul style="list-style-type: none"> <li>i. Increased customer numbers above expectations.</li> <li>ii. Changes in legislation resulting in changes in customer behaviour.</li> </ul>	<ul style="list-style-type: none"> <li>i. Insufficient resource within Council.</li> <li>ii. Increased costs</li> <li>iii. Dissatisfaction of residents.</li> <li>iv. Reputation.</li> </ul>	<ul style="list-style-type: none"> <li>i. Channel strategy implementing additional channels &amp; self-service options.</li> <li>ii. Local Plan.</li> <li>iii. Joint planning and delivery arrangements with partners.</li> </ul>	
<p>3. Impact of climate change on service delivery.</p>	<ul style="list-style-type: none"> <li>i. Changes in weather as a result of climate change. Prolonged spells of inclement weather.</li> </ul>	<ul style="list-style-type: none"> <li>i. Long periods of cold weather could reduce service availability through staff sickness or disrupted travel.</li> </ul>	<ul style="list-style-type: none"> <li>i. Inclement weather policy in place.</li> <li>ii. Sickness absence management in place.</li> <li>iii. Documented processes &amp; staff training.</li> <li>iv. Contingency plans in place.</li> <li>v. Agile working policy in place &amp; key staff have access to systems remotely.</li> </ul>	

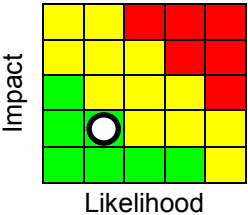
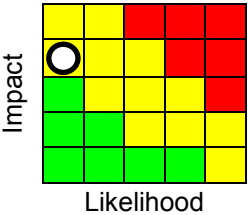
Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
<p>4. Accidents / health &amp; safety of staff in office.</p>	<ul style="list-style-type: none"> <li>i. Lack of health &amp; safety good practice.</li> <li>ii. Genuine accidents.</li> </ul>	<ul style="list-style-type: none"> <li>i. Injuries to staff.</li> <li>ii. Financial.</li> <li>iii. Loss of staff morale</li> <li>iv. Adverse publicity, reputation.</li> <li>v. Difficulty in service delivery.</li> <li>vi. Increase in sickness absence.</li> </ul>	<ul style="list-style-type: none"> <li>i. Lone Worker (Tunstall system)</li> <li>ii. H&amp;S Policy and Procedures in place.</li> <li>iii. Joint Consultative Group (management and unions).</li> <li>iv. Operation of robust risk assessments, safe working practices.</li> <li>v. Accident/incident reporting and investigation.</li> <li>vi. Safety Advisors inspection of workplace.</li> <li>vii. DSE assessments.</li> </ul>	

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
<p>5. Recruitment and retention of staff.</p>	<ul style="list-style-type: none"> <li>i. Failure to maintain a workforce that can provide good service delivery.</li> <li>ii. Failure to identify gaps in staff skills &amp; capacity that could lead to poor service delivery.</li> <li>iii. Age profile of staff.</li> <li>iv. Competitive salary levels.</li> <li>v. Failure to conclude appointments quickly leading to loss of candidates.</li> <li>vi. Competitive terms and Conditions.</li> </ul>	<ul style="list-style-type: none"> <li>i. Loss of key staff.</li> <li>ii. Inability to recruit.</li> <li>iii. Additional costs for specialist advice.</li> <li>iv. Loss of technical staff to private sector for more competitive job offers</li> <li>v. Reduction in service to customers.</li> </ul>	<ul style="list-style-type: none"> <li>i. Shared Services.</li> <li>ii. Succession planning.</li> <li>iii. Training on roles to build resilience.</li> <li>iv. Generic Roles where possible.</li> <li>v. Clear recruitment process.</li> <li>vi. Managers trained in recruitment and management of staff.</li> <li>vii. Redeployment policy.</li> </ul>	
<p>6. The impact of a business continuity incident.</p>	<ul style="list-style-type: none"> <li>i. Loss of building or office space.</li> <li>ii. Loss or lack of key staff.</li> <li>iii. Loss of key equipment or systems.</li> </ul>	<ul style="list-style-type: none"> <li>i. Poor/lack of service delivery.</li> <li>ii. Reputation.</li> </ul>	<ul style="list-style-type: none"> <li>i. Service Area Crisis Plans – current and communicated.</li> <li>ii. WDC Major Emergency Plan in place.</li> <li>iii. ICT Business Continuity contract in place.</li> </ul>	

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
7. Giving incorrect information and advice.	i. Untrained staff. ii. Poor communication. iii. Re-organisations. iv. Loss of key staff. v. Inaccurate data on systems or website.	i. Negligence and liability claims. ii. Adverse publicity. iii. Loss of reputation. iv. Waste of resources v. Poor service to customers.	i. Training in place ii. Qualified staff. iii. Risk assessments. iv. Quality standards. v. Supportive management environment. vi. Good IT/Information Systems/Accurate data. vii. Clear processes. viii. Web Improvement Plan.	
8. High or increasing levels of sickness.	i. Individual workloads increase resulting in higher stress levels. ii. Pandemic. iii. Poor working environment. iv. Poor management. v. Key staff are off sick. vi. Prolonged periods of sickness by key staff.	i. Some services not delivered. ii. Increase in stress/pressure on remaining staff. iii. Reputational risk. iv. Additional costs to cover key staff. v. Low resilience of service.	i. Detailed monitoring ii. Management information provided to SMT. iii. New HRMS will allow faster access to information. iv. Documented processes & staff training. v. Succession plans for critical posts and staff.	

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
9. Strike Action.	<ul style="list-style-type: none"> <li>i. Unhappy staff</li> <li>ii. Union actions</li> <li>iii. National movements.</li> </ul>	<ul style="list-style-type: none"> <li>i. Breakdown of employment relationships.</li> <li>ii. Council reputation through disruption to service delivery.</li> </ul>	<ul style="list-style-type: none"> <li>i. Strong formal and informal communication forums and mechanisms at a local level.</li> </ul>	 <p>The risk matrix is a 5x5 grid. The vertical axis is labeled 'Impact' and the horizontal axis is labeled 'Likelihood'. The grid is color-coded as follows:</p> <ul style="list-style-type: none"> <li>Row 1 (High Impact): Yellow, Yellow, Red, Red, Red</li> <li>Row 2 (Medium-High Impact): Yellow, Yellow, Red, Red, Red</li> <li>Row 3 (Medium Impact): Green, Yellow, Yellow, Yellow, Red</li> <li>Row 4 (Medium-Low Impact): Green, Green, Yellow, Yellow, Yellow</li> <li>Row 5 (Low Impact): Green, Green, Green, Green, Yellow</li> </ul> <p>A white circle with a black outline is positioned in the cell at the intersection of the second row from the bottom (Medium-Low Impact) and the first column from the right (Low Likelihood).</p>

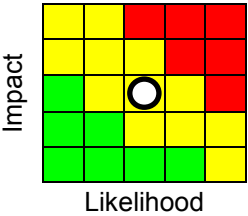
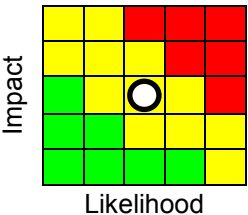
Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
<p>10. ICT systems not able to support current service delivery and future improvements.</p>	<ul style="list-style-type: none"> <li>i. Failure of the current ICT infrastructure being unable to meet demand.</li> <li>ii. Interruption of power supply.</li> <li>iii. Physical damage.</li> <li>iv. Systems failure of hardware and software.</li> <li>v. Cyber attack.</li> <li>vi. Use of third party systems.</li> </ul>	<ul style="list-style-type: none"> <li>i. Prolonged loss of systems.</li> <li>ii. Additional cost to operate systems</li> <li>iii. Corrupted information and/or databases.</li> <li>iv. Provision of data unavailable.</li> <li>v. Reduction in service delivery to customers.</li> </ul>	<ul style="list-style-type: none"> <li>i. Third party support and maintenance contracts.</li> <li>ii. WDC Data centre protected by UPS.</li> <li>iii. WDC backup generator</li> <li>iv. Hardware resilience; dual power suppliers, RAID, virtualisation, etc.</li> <li>v. Critical business devices protected by UPS.</li> <li>vi. Backup and recovery strategy</li> <li>vii. Disaster recovery in place and ongoing testing</li> <li>viii. Backup and recovery systems in place.</li> <li>ix. ICT Services Service Area Continuity Plan.</li> <li>x. Third Party Disaster Recovery Contract.</li> <li>xi. ICT Business Continuity Plan.</li> </ul>	<div style="text-align: center;">  <p>Impact</p> <p>Likelihood</p> </div>

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
<p>11. Insufficient money resulting in an inability to provide normal services.</p>	<ul style="list-style-type: none"> <li>i. Poor financial planning</li> <li>ii. Unexpected loss of income / increase in expenditure.</li> <li>iii. Fit for the future projects do not achieve sufficient savings.</li> <li>iv. Changes to Government Policy.</li> <li>v. Reduced Government grants.</li> <li>vi. Budgets exceeded.</li> <li>vii. Insufficient money to provide services as specified.</li> </ul>	<ul style="list-style-type: none"> <li>i. Loss-making services</li> <li>ii. Problems delivering key services.</li> <li>iii. Reduced quality of service.</li> <li>iv. Budget exceeded and therefore subsequent budgets reduced.</li> <li>v. Forced to make large scale redundancies.</li> </ul>	<ul style="list-style-type: none"> <li>i. Effective management of Fit for the Future Programme &amp; prioritisation of projects.</li> <li>ii. Effective audit of financial accounts.</li> <li>iii. Effective fees and charges schemes.</li> <li>iv. Delivery plans and overall project plans have been completed.</li> <li>v. Effective internal audit function.</li> <li>vi. Codes of Financial and Procurement practice adhered to and understood by relevant officers.</li> </ul>	
<p>12. Failure to:-</p> <ul style="list-style-type: none"> <li>(a) Respond to new legislation.</li> <li>(b) Comply with new/existing legislation.</li> <li>(c) Take into account legal implications of decisions.</li> </ul>	<ul style="list-style-type: none"> <li>i. Failure to respond to new legislation, comply with new or existing legislation or to take into account legal implications of decisions.</li> <li>ii. Change in Government policy.</li> <li>iii. Poor decision making.</li> <li>iv. Inexperienced staff.</li> </ul>	<ul style="list-style-type: none"> <li>i. WDC unprepared for changes resulting in additional costs/workloads for staff.</li> <li>ii. Damage to reputation.</li> <li>iii. Judicial reviews.</li> <li>iv. Financial impact.</li> <li>v. Legal action against the Council.</li> </ul>	<ul style="list-style-type: none"> <li>i. Legal advice available to staff.</li> <li>ii. Communication with professional bodies and organisations to seek assistance and advice.</li> <li>iii. Staff suitably trained and qualified to give advice and guidance.</li> </ul>	



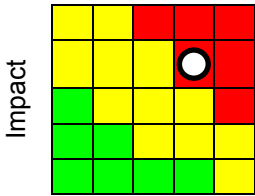
Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
------------------	-------------------	-----------------------	---------------------------	----------------------

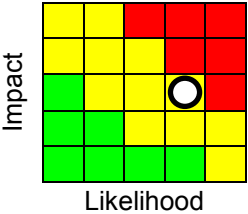
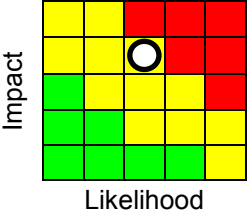
**Service Area Specific Risks**

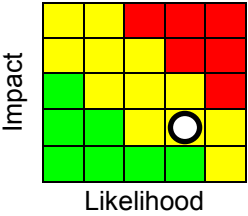
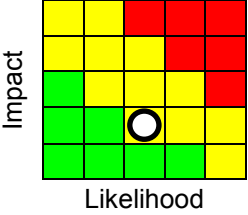
<p>13. Cultural Change not progressing fast enough.</p>	<ul style="list-style-type: none"> <li>i. Work on People Strategy not achieved.</li> <li>ii. Change in focus.</li> <li>iii. Failure to communicate what is required and why.</li> <li>iv. Failure of leaders to role model what is require.</li> <li>v. Failure to engage and gain buy in from staff and Members.</li> </ul>	<ul style="list-style-type: none"> <li>i. High turnover</li> <li>ii. Redundancies more frequent.</li> <li>iii. More disciplinaries and grievances.</li> <li>iv. Reduction in staff motivation.</li> <li>v. Reduction in performance.</li> </ul>	<ul style="list-style-type: none"> <li>i. Monitoring of People Strategy by Members, unions &amp; Senior Management.</li> <li>ii. SMT agree what culture change they want and why.</li> <li>iii. SMT agree a plan for delivering culture, including agreeing roles&amp; responsibilities.</li> <li>iv. SMT to review and monitor delivery of the plan.</li> </ul>	
<p>14. Partnership working fails.</p>	<ul style="list-style-type: none"> <li>i. Changes in funding or priorities of partners.</li> <li>ii. Relationship breakdown.</li> <li>iii. Changing partnership landscape (abolition of area committees &amp; future grant management arrangements).</li> <li>iv. Possible changes to LSP.</li> </ul>	<ul style="list-style-type: none"> <li>i. Loss of or reduction in service</li> <li>ii. Increased complaints</li> <li>iii. Increased demand on resources.</li> <li>iv. Reduction in available resources.</li> <li>v. Reputation.</li> </ul>	<ul style="list-style-type: none"> <li>i. SLA to be signed for CSC &amp; OSS.</li> <li>ii. Legal agreements for OSS signed.</li> <li>iii. Frequent communication at all levels.</li> <li>iv. Consultation on Partnership Landscapes&amp; other Localities work.</li> </ul>	

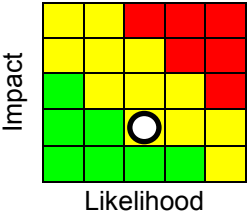
Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
------------------	-------------------	-----------------------	---------------------------	----------------------

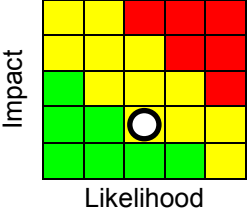
**Service Specific – Human Resources & Organisational Development**

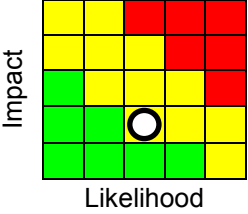
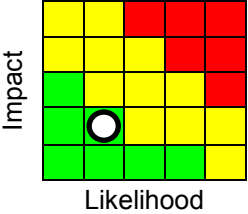
<p>15. Staff morale is low: staff are unhappy and unengaged.</p>	<ul style="list-style-type: none"> <li>i. High levels of change in the Council.</li> <li>ii. Risk of redundancy or Job changes.</li> <li>iii. Concerns raised in exit interviews.</li> <li>iv. Increase in staff &amp; managers coming to talk to HR about work.</li> <li>v. High levels of stress indicated by 'Hotfrog' survey.</li> </ul>	<ul style="list-style-type: none"> <li>i. High numbers of leavers.</li> <li>ii. Higher number of disciplinaries and grievances.</li> <li>iii. More case work for HR</li> <li>iv. Increase disputes with Unions.</li> <li>v. Increased escalation of management involvement for case work.</li> </ul>	<ul style="list-style-type: none"> <li>i. Good levels of communication at all levels of the organisation.</li> <li>ii. Use of ESOs, union and HR for advice and support as well as managers.</li> <li>iii. Consultation is used at every opportunity to keep staff informed.</li> <li>iv. Managers are supported by their managers and HR.</li> </ul>	 <p align="center">Likelihood</p>
--	--	--	---	--

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
<p>16. Employment Tribunal claims.</p>	<ul style="list-style-type: none"> <li>i. Disgruntled employees.</li> <li>ii. Union actions.</li> </ul>	<ul style="list-style-type: none"> <li>i. Poor HR practices identified.</li> <li>ii. Financial cost.</li> <li>iii. Break down of employee relationships.</li> <li>iv. Bad press / poor reputation as an employer.</li> </ul>	<ul style="list-style-type: none"> <li>i. Clear policies and procedures</li> <li>ii. Good HR practice</li> <li>iii. HR staff maintain Professional qualification (CIPD)</li> <li>iv. Trained management via courses, mentoring and coaching.</li> <li>v. Constructive relationships with Unions.</li> </ul>	
<p>17. The council has difficulty in getting the right people in post or retaining people in post</p>	<ul style="list-style-type: none"> <li>i. High turnover of staff</li> <li>ii. Internal staff do not apply for internal roles</li> <li>iii. Low update on training offered</li> <li>iv. Cost is higher as need to recruit frequently</li> </ul>	<ul style="list-style-type: none"> <li>i. Poor choice of candidates for roles internally</li> <li>ii. Council not seen as a place people want to work so reputation is poor externally</li> <li>iii. Staff morale is low as staff have to cope with more work if recruitment not working or staff leave their team</li> </ul>	<ul style="list-style-type: none"> <li>iv. Clear training and development opportunities.</li> <li>v. Clear development paths for staff linked to Personal Development Plan.</li> <li>vi. Publicise the benefits of working with the council in recruitment.</li> <li>vii. Ensure recruiters are well trained.</li> <li>viii. Ensure managers can manage their team's development.</li> </ul>	

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
<p>18. The council's workforce profile does not represent the community profile</p>	<ul style="list-style-type: none"> <li>i. Low visibility of female, disabled, ethnic staff amongst the management levels.</li> <li>ii. Service delivery is challenged as discriminatory.</li> <li>iii. Consultation is not undertaken with service changes or delivery.</li> </ul>	<ul style="list-style-type: none"> <li>i. Views on how services are shaped and delivered are narrow .</li> <li>ii. Communities feel isolated and not involved in what services they receive.</li> <li>iii. Customer complaints increase regarding diversity or discrimination.</li> <li>iv. Reputational damage</li> <li>v. Financial loss.</li> </ul>	<ul style="list-style-type: none"> <li>i. Understanding of Equalities is embedded across the council.</li> <li>ii. HR lead on Equality work to support managers.</li> <li>iii. Staff value diversity and welcome consultation.</li> <li>iv. Recruitment and selection is not biased against diversity.</li> </ul>	
<p>19. Loss or Corruption of Personal Data.</p>	<ul style="list-style-type: none"> <li>i. Human error.</li> <li>ii. Systems failure.</li> <li>iii. Loss of information during transactions.</li> <li>iv. Hardware/Software corruption.</li> <li>v. Poor training.</li> <li>vi. Malicious intent.</li> </ul>	<ul style="list-style-type: none"> <li>i. Unhappy staff.</li> <li>ii. Reputation of Council.</li> <li>iii. Possible Financial cost</li> <li>iv. Loss of service to the customer.</li> <li>v. Processing backlogs.</li> </ul>	<ul style="list-style-type: none"> <li>i. Clear policies for holding personal data e.g. retention.</li> <li>ii. Training for staff .</li> <li>iii. Audit logs.</li> <li>iv. Quality checking of data.</li> </ul>	

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
20. Training – not evaluated as adding value.	<ul style="list-style-type: none"> <li>i. No training needs analysis and training delivered to meet this.</li> <li>ii. No training plans (as above).</li> <li>iii. Appraisals not carried out at all or in time.</li> <li>iv. Attendees do not attend or cancel last minute when booked on a course.</li> <li>v. Spend not analysed.</li> <li>vi. Impact of training on performance not analysed.</li> </ul>	<ul style="list-style-type: none"> <li>i. Service delivery impeded.</li> <li>ii. Recruitment and retention affected.</li> <li>iii. Corporate objectives not achieved.</li> <li>iv. Motivation is low from staff without the right skills to do the job.</li> <li>v. Equality may be impacted as it may have an adverse affect.</li> <li>vi. Cost is low but effectiveness not measured.</li> <li>vii. Members not given right skills/support.</li> <li>viii. Poor decisions as staff do not have the skills.</li> <li>ix. Reputation damage.</li> </ul>	<ul style="list-style-type: none"> <li>i. Investors In People (IIP) accreditation Process&amp; action plan.</li> <li>ii. Performance Management Framework</li> <li>iii. Course evaluation.</li> <li>iv. Tendering/ selection of providers.</li> <li>v. Review of budget.</li> <li>vi. Managers review the effect of training on staff performance.</li> <li>vii. ICT Steering Group reviewing ICT training needs.</li> </ul>	

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
<p>21. Failure to achieve the statutory Equality Framework.</p>	<ul style="list-style-type: none"> <li>i. Lack of commitment at all levels.</li> <li>ii. Lack of understanding of how to achieve it and what it means to the services..</li> <li>iii. Inability to do the work required (lack of understanding/capacity).</li> </ul>	<ul style="list-style-type: none"> <li>i. Poor audits.</li> <li>ii. Possible Cost in tribunal cases e.g. discrimination.</li> <li>iii. Service delivery could be causing discrimination thus impacting customers.</li> <li>iv. Not able to retain Investors In People. Reputation damage.</li> <li>v. Affects ability to recruit and retain staff.</li> </ul>	<ul style="list-style-type: none"> <li>i. Educate and support services through training and coaching.</li> <li>ii. Focus HR resource on achieving Framework. Use of best practice and examples of success.</li> <li>iii. Involve customers in decisions, via engagement groups.</li> <li>iv. Embedded in service planning cycle/service area plans. Equality Impact Assessment (EIA) training completed.</li> <li>v. EIA required for all policy/service changes.</li> </ul>	

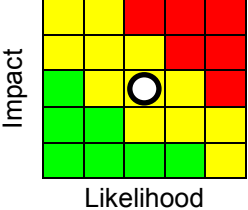
Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
<p>22. The council does not retain Investors in People (IIP) status</p>	<ul style="list-style-type: none"> <li>i. Fail assessment.</li> <li>ii. Failure to deliver IIP Action Plan.</li> <li>iii. Staff morale is low at time of next assessment.</li> </ul>	<ul style="list-style-type: none"> <li>i. Staff engagement decreases as staff feel under-valued.</li> <li>ii. Council reputation could be decreased as could be seen as slipping in standards.</li> </ul>	<ul style="list-style-type: none"> <li>i. Commitment at all levels to IIP attainment.</li> <li>ii. Communication across the council about IIP and how it affects everyone.</li> <li>iii. HR &amp; OD resource focus on delivery of Actin Plan.</li> <li>iv. SMT quarterly review of action plan and People Strategy.</li> </ul>	
<p>23. Job Evaluations appear to staff to be poorly carried out and / or inconsistent grading carried out.</p>	<ul style="list-style-type: none"> <li>i. Managers and staff resubmit evaluations if they don't get the 'right' score.</li> <li>ii. Staff unhappy with changes to job descriptions.</li> <li>iii. Hay panel loss of integrity / reputation.</li> </ul>	<ul style="list-style-type: none"> <li>i. Unhappy staff who appeal their scores.</li> <li>ii. Managers, Unions and staff do not trust the decisions.</li> <li>iii. Managers don't want to join the Hay panel so struggle to do evaluations.</li> <li>iv. High numbers of appeals by staff.</li> </ul>	<ul style="list-style-type: none"> <li>i. Well trained Hay panel who are competent and experienced.</li> <li>ii. Managers, Unions and staff work together to build trust in the Hay panel decisions.</li> <li>iii. Fair process and appeal process in place.</li> </ul>	

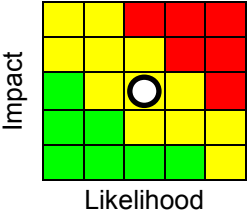
Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
------------------	-------------------	-----------------------	---------------------------	----------------------

**Service Specific – Information & Communication Technology**

<p>24. Unauthorised Disclosure.</p>	<ul style="list-style-type: none"> <li>i. Hacking</li> <li>ii. Spyware</li> <li>iii. Emailing the wrong recipient</li> <li>iv. Stolen equipment; laptops, USB devices</li> <li>v. Lost devices</li> <li>vi. Poor hardware disposal practices</li> <li>vii. Poor password management</li> <li>viii. Allowing unauthorised third parties, including family &amp; friends, to utilise Council equipment.</li> </ul>	<ul style="list-style-type: none"> <li>i. Potential fines; ICO, DP.</li> <li>ii. Reputational damage.</li> </ul>	<ul style="list-style-type: none"> <li>i. Information Security Policy.</li> <li>ii. Penetration testing</li> <li>iii. Perimeter protection; Firewall, 2 Factor Authentication</li> <li>iv. Disk encryption</li> <li>v. USB device restriction and encryption.</li> <li>vi. Virtual Desktops</li> <li>vii. Adoption of the ISO 27001 security standard.</li> <li>viii. Formation of the ICT Steering Group’s Governance sub-group.</li> <li>ix. Third Party Network Access Agreement</li> <li>x. Non-Disclosure Agreements</li> <li>xi. Destruction certificates for equipment disposal.</li> </ul>	
-------------------------------------	--	--	--	--



Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
25. Non-Availability of Key Technical & Support Staff.	<ul style="list-style-type: none"> <li>i. Failure to maintain a workforce that can provide good service delivery.</li> <li>ii. Salary</li> <li>iii. Training</li> <li>iv. T&amp;C</li> <li>v. Working Environment</li> <li>vi. Career Progression</li> <li>vii. Failure to identify gaps in staff skills &amp; capacity that could lead to poor service delivery.</li> <li>viii. Poor planning to cover holidays, sickness, etc.</li> <li>ix. Poor project management.</li> <li>x. Epidemic.</li> </ul>	<ul style="list-style-type: none"> <li>i. Additional costs for specialist advice.</li> <li>ii. Increased service outages.</li> <li>iii. Increased duration of service outages.</li> <li>iv. Inability to deliver Council objectives.</li> <li>v. Increased stress on residual staff.</li> </ul>	<ul style="list-style-type: none"> <li>i. Shared Services.</li> <li>ii. Succession planning.</li> <li>iii. Generic Roles where ever possible.</li> <li>iv. Third party Support &amp; Maintenance Contracts.</li> <li>v. Business Continuity – Staff Absence Strategy.</li> <li>vi. Documentation.</li> <li>vii. Training budget.</li> </ul>	

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
<p>26. Loss of Data or Data Integrity.</p>	<ul style="list-style-type: none"> <li>iv. Hacking.</li> <li>v. Human error.</li> <li>vi. Poor change management.</li> <li>vii. Little or no testing of new software releases.</li> <li>viii. Viruses.</li> <li>ix. Poor password management.</li> <li>x. Insecure web applications.</li> <li>xi. Software bugs.</li> <li>xii. Inappropriate access rights.</li> <li>xiii. Hardware corruption.</li> <li>xiv. Poor training.</li> <li>xv. Malicious intent.</li> </ul>	<ul style="list-style-type: none"> <li>i. Loss of service to the customer.</li> <li>ii. Processing backlogs.</li> <li>iii. Potential loss of income.</li> <li>iv. Reputational damage.</li> <li>v. Fraud.</li> </ul>	<ul style="list-style-type: none"> <li>i. Perimeter protection; Firewall, 2 Factor Authentication, Spam filter, Antivirus, etc.</li> <li>ii. Test plans.</li> <li>iii. Penetration testing (Ethical Hacking).</li> <li>iv. Antivirus strategy.</li> <li>v. Audits (Internal, 3rd Party ICT Auditors, Communications-Electronics Security Group (CESG), PCI DSS)</li> <li>vi. Activity logs.</li> <li>vii. Staff Training.</li> <li>viii. Code of Connection.</li> <li>ix. Information Security Policy.</li> <li>x. Adoption of ISO 27001 standard.</li> <li>xi. Formation of Info. Governance Sub-Group (ICT Steering Group)</li> <li>xii. Recruitment using the Baseline Personnel Security Standard.</li> <li>xiii. Supplier support contracts.</li> <li>xiv. GovCertUK notifications of threats and vulnerabilities.</li> <li>xv. Nominated system owners.</li> </ul>	

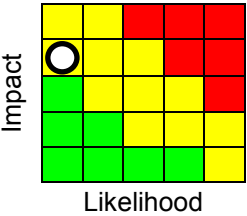
Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
------------------	-------------------	-----------------------	---------------------------	----------------------

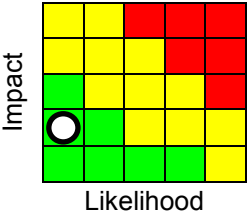
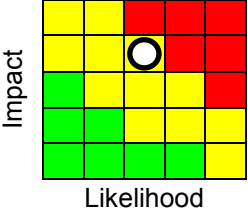
27. Loss of Council computer facilities (*Servers, Storage, Network, Voice*).

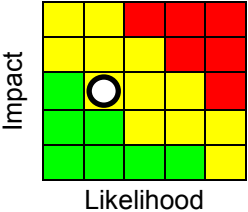
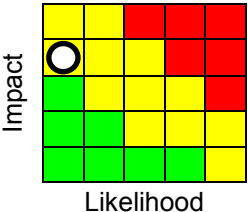
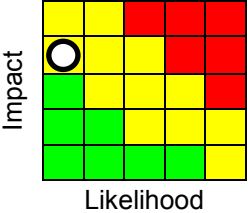
- i. Human error.
- ii. Hardware/software failure (OS).
- iii. Poor change management
- iv. Fire/Flood
- v. Loss of power
- vi. Theft
- vii. Malicious damage
- viii. Environmental (Too hot, too cold)
- ix. Telecoms failure.
- x. Firmware bug.
- xi. Lack of funding.

- i. Loss of service to the customer.
- ii. Processing backlogs
- iii. Potential loss of income.
- iv. Reputational damage
- v. Loss of data.

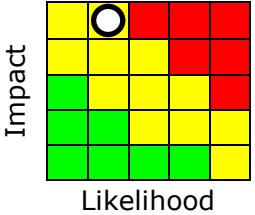
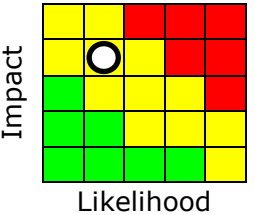
- i. Staff training.
- ii. Technical documentation.
- iii. Hardware resilience.
- iv. Backup generator/Uninterruptible Power Supply (UPS).
- v. Offsite backup tapes.
- vi. Business continuity contract.
- vii. Change Management Policy / Back-out Plans.
- viii. Audits.
- ix. Fire/Flood detection.
- x. Fire suppression
- xi. Air conditioning
- xii. Proactive monitoring (System Centre Operations Manager)
- xiii. Redundant Array of Independent Disks – RAID 5.
- xiv. VMware High Availability.
- xv. Third party support & Maintenance contracts.
- xvi. Environmental security policy.
- xvii. Insurance.
- xviii. Code of Connection.
- xix. Investment planning via the Equipment Renewal Reserve.

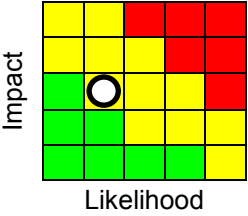
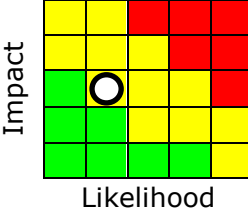
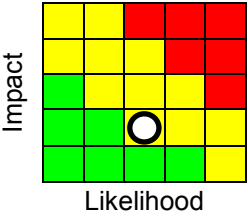


Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
28. Failure of Service Providers.	<ul style="list-style-type: none"> <li>i. Bankruptcy.</li> <li>ii. Natural disaster.</li> <li>iii. Takeover.</li> <li>iv. Legal (Intellectual property infringement).</li> <li>v. Change of strategy (no longer wish to supply the product).</li> </ul>	<ul style="list-style-type: none"> <li>i. Non-supported system.</li> <li>ii. System replacement costs.</li> <li>iii. Potential loss of service to the customer.</li> <li>iv. Potential loss of income.</li> <li>vi. Potential inability to deliver Council objectives.</li> </ul>	<ul style="list-style-type: none"> <li>i. Change freeze.</li> <li>ii. Shared service.</li> <li>iii. Emergency procurement.</li> <li>iv. Business Continuity - Business Application Supplier Strategy.</li> <li>v. Financial vetting of suppliers as part of the procurement process.</li> </ul>	
<b>Service Specific – Community Partnership Team</b>				
29. Partnership working with WCC fails.	<ul style="list-style-type: none"> <li>i. Staff integration</li> <li>ii. Reduced funding or support</li> <li>iii. Policy change at WCC or WDC.</li> </ul>	<ul style="list-style-type: none"> <li>i. Reduced resources available</li> <li>ii. Reduced service level and/or quality</li> <li>iii. Reduced support for communities</li> </ul>	<ul style="list-style-type: none"> <li>i. Regular dialogue &amp; monitoring.</li> <li>ii. Create joint team objectives.</li> <li>iii. Regular review of policy changes at WDC &amp; WCC.</li> </ul>	

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
30. Insufficient staff to provide services.	<ul style="list-style-type: none"> <li>i. Failure to identify gaps in staff skills &amp; capacity that could lead to poor service delivery.</li> <li>ii. Staff illness/leave.</li> <li>iii. Increasing workload and community expectations.</li> </ul>	<ul style="list-style-type: none"> <li>i. Reduction in level and/or quality of service to communities.</li> <li>ii. Poor perception of service.</li> <li>iii. Increased complaints.</li> </ul>	<ul style="list-style-type: none"> <li>i. Team operational plan.</li> <li>ii. Working with Service areas to ensure delivery by experts.</li> <li>iii. Generic Roles where possible.</li> <li>iv. Supportive management.</li> </ul>	
31. Scope for violence/abuse of staff.	<ul style="list-style-type: none"> <li>i. Dissatisfied customers at public meetings.</li> <li>ii. Dissatisfied customers in Voluntary &amp; Community Sector.</li> </ul>	<ul style="list-style-type: none"> <li>i. Injured/traumatised staff.</li> <li>ii. Reduced service.</li> <li>iii. Financial.</li> </ul>	<ul style="list-style-type: none"> <li>i. Staff training &amp; policies including lone worker policies.</li> </ul>	
32. Failure to /delay in payment to grant recipients; incorrect amounts paid.	<ul style="list-style-type: none"> <li>i. Untrained staff.</li> <li>ii. Loss of key staff.</li> <li>iii. Inaccurate data.</li> <li>iv. Lack of planning.</li> </ul>	<ul style="list-style-type: none"> <li>i. Grant recipients distressed.</li> <li>ii. Community activities .stopped/delayed due to financial shortfall.</li> <li>iii. Negative publicity.</li> </ul>	<ul style="list-style-type: none"> <li>i. Monthly monitoring of budgets. against SLAs</li> <li>ii. Trained staff.</li> <li>iii. Forward planning.</li> </ul>	

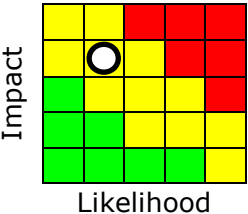
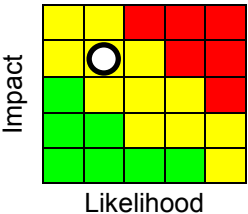
Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
------------------	-------------------	-----------------------	---------------------------	----------------------

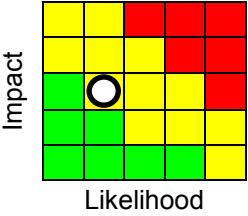
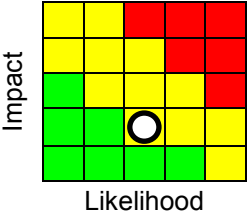
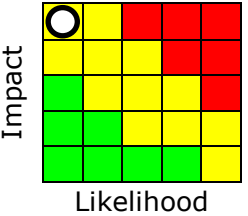
<b>Service Specific – Warwickshire Direct (Customer Service Centre)</b>				
<p>33. Loss of telephony platform.</p>	<ul style="list-style-type: none"> <li>i. Automated Call Distributer (ACD) server loss.</li> <li>ii. Loss of Shire Hall telephone switch.</li> <li>iii. Lack of skilled resource to rectify issues.</li> </ul>	<ul style="list-style-type: none"> <li>i. Service delivery compromised and resultant customer dissatisfaction.</li> <li>ii. Potential for individuals to be put at risk.</li> <li>iii. Inability to take payments affects income.</li> <li>iv. Reputational damage.</li> </ul>	<ul style="list-style-type: none"> <li>i. Switch capability at Kings House.</li> <li>ii. Utilise switch only functionality if ACD is lost (limited).</li> <li>iii. Business continuity plan supports prioritisation of service delivery.</li> <li>iv. Procurement of new system in Cloud avoids traditional infrastructure dependency.</li> <li>v. Plan in place to train second responsible officer on ACD.</li> </ul>	 <p>Impact</p> <p>Likelihood</p>
<p>34. Insufficient staffing levels to deliver services.</p>	<ul style="list-style-type: none"> <li>i. Staff shortfall against establishment.</li> <li>ii. Staff attrition.</li> <li>iii. Sickness and leave.</li> <li>iv. Recruitment freeze or failure.</li> </ul>	<ul style="list-style-type: none"> <li>i. Customer dissatisfaction.</li> <li>ii. Reputational damage.</li> <li>iii. Closure of OSS outlets.</li> </ul>	<ul style="list-style-type: none"> <li>i. On-going scheduled recruitment activity.</li> <li>ii. Absence management policies and training.</li> <li>iii. Review of exit interviews.</li> <li>iv. Team leaders trained to deliver service.</li> </ul>	 <p>Impact</p> <p>Likelihood</p>

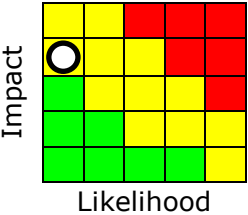
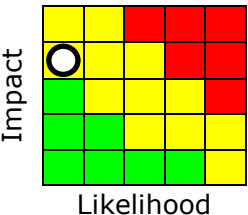
Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
35. Harm to staff.	<ul style="list-style-type: none"> <li>i. Exposure to abusive customer contact.</li> <li>ii. Exchange of information of an upsetting nature.</li> </ul>	<ul style="list-style-type: none"> <li>i. Temporary loss of capacity.</li> <li>ii. Service disruption.</li> <li>iii. Reputational damage.</li> <li>iv. Liability/negligence claims.</li> </ul>	<ul style="list-style-type: none"> <li>i. Risk assessments in place.</li> <li>ii. Abusive call process in place.</li> <li>iii. Training completed.</li> </ul>	
36. ICT failure.	<ul style="list-style-type: none"> <li>i. Network issues</li> <li>ii. Service related ICT system issues.</li> </ul>	<ul style="list-style-type: none"> <li>i. Disruption of core activities/services offered to customers.</li> <li>ii. Reputational damage.</li> </ul>	<ul style="list-style-type: none"> <li>i. Reporting routines established.</li> <li>ii. Procedures to deal with enquiries manually.</li> </ul>	
37. Provision of incorrect information and advice.	<ul style="list-style-type: none"> <li>i. Lack of training provision.</li> <li>ii. Individuals failing to follow procedures.</li> <li>iii. Inaccurate information stored within the system.</li> <li>iv. Poor performance management routines.</li> </ul>	<ul style="list-style-type: none"> <li>i. Reputational damage.</li> <li>ii. Liability/negligence claims.</li> <li>iii. Service degradation.</li> </ul>	<ul style="list-style-type: none"> <li>i. Training undertaken.</li> <li>ii. Robust recruitment procedures.</li> <li>iii. Quality framework and feedback routines established.</li> <li>iv. Regular engagement with services to maintain accurate information.</li> </ul>	

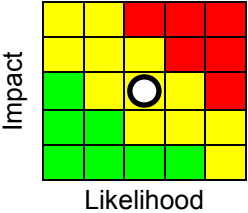
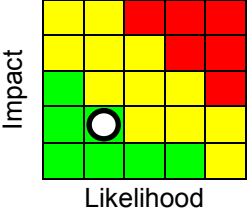
Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
<p>38. Breakdown of partnership working.</p>	<ul style="list-style-type: none"> <li>i. Differing organisational priorities.</li> <li>ii. Financial constraints.</li> <li>iii. Breakdown of relationships.</li> <li>iv. Withdrawal of political support.</li> </ul>	<ul style="list-style-type: none"> <li>i. Need to extricate from operational arrangements – would introduce cost.</li> <li>ii. Organisational withdrawal from partnership.</li> <li>iii. Non-realisation of partnership vision.</li> <li>iv. Disruption to customer service.</li> <li>v. Reputational damage</li> <li>vi. Potential closure of centres.</li> </ul>	<ul style="list-style-type: none"> <li>i. Regular engagement at all appropriate levels to confirm priorities and activities.</li> <li>ii. Staff consultations and alignment of terms and conditions at delivery level.</li> <li>iii. Retention of management on organisational contracts.</li> <li>iv. Location licenses signed.</li> </ul>	
<p>39. Loss of premises.</p>	<ul style="list-style-type: none"> <li>i. Major incident e.g. flood, loss of power, building damage.</li> </ul>	<ul style="list-style-type: none"> <li>i. Service delivery compromised and resultant customer dissatisfaction.</li> <li>ii. Reputational damage.</li> </ul>	<ul style="list-style-type: none"> <li>i. Business continuity plan</li> <li>ii. Offer service from second centre (Bedworth).</li> </ul>	

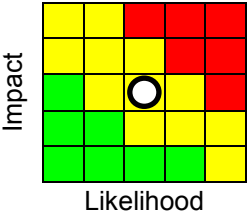
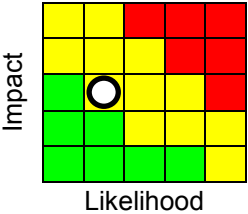


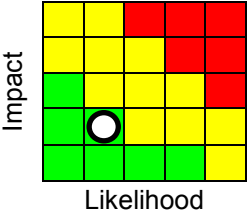
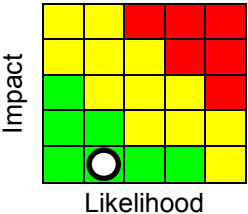
Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
<b>Service Specific – Warwickshire Direct (One Stop Shops)</b>				
40. Insufficient staffing levels to deliver services.	<ul style="list-style-type: none"> <li>i. Staff shortfall against establishment.</li> <li>ii. Staff attrition.</li> <li>iii. Sickness and leave.</li> <li>iv. Recruitment freeze or failure.</li> </ul>	<ul style="list-style-type: none"> <li>i. Customer dissatisfaction</li> <li>ii. Reputational damage.</li> <li>iii. Closure of OSS outlets.</li> </ul>	<ul style="list-style-type: none"> <li>i. Recruitment plans in place.</li> <li>ii. Absence management policies and training.</li> <li>iii. Review of exit interviews</li> <li>iv. Team leaders trained to deliver service.</li> <li>v. Opportunity to gain support from CSC.</li> <li>vi. Introduction of Hub working.</li> </ul>	
41. Harm to staff/other members of the public.	<ul style="list-style-type: none"> <li>i. Exposure to abusive customer contact.</li> <li>ii. Exchange of information of an upsetting nature.</li> </ul>	<ul style="list-style-type: none"> <li>i. Temporary loss of capacity.</li> <li>ii. Service disruption.</li> <li>iii. Reputational damage</li> <li>iv. Liability/negligence claims.</li> </ul>	<ul style="list-style-type: none"> <li>i. Risk assessments in place</li> <li>ii. Procedures documented</li> <li>iii. Training completed.</li> </ul>	

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
42. ICT failure.	<ul style="list-style-type: none"> <li>i. Network issues.</li> <li>ii. Service related ICT system issues.</li> </ul>	<ul style="list-style-type: none"> <li>i. Disruption of core activities/services offered to customers.</li> <li>ii. Reputational damage.</li> </ul>	<ul style="list-style-type: none"> <li>i. Reporting routines established.</li> <li>ii. Procedures to deal with enquiries manually.</li> </ul>	
43. Provision of incorrect information and advice.	<ul style="list-style-type: none"> <li>i. Lack of training provision.</li> <li>ii. Individuals failing to follow procedures.</li> <li>iii. Inaccurate information stored within the system.</li> </ul>	<ul style="list-style-type: none"> <li>i. Reputational damage.</li> <li>ii. Liability/negligence claims.</li> <li>iii. Service degradation.</li> </ul>	<ul style="list-style-type: none"> <li>i. Training undertaken.</li> <li>ii. Robust recruitment procedures.</li> <li>iii. Quality framework and feedback routines established.</li> <li>iv. Regular engagement with services to maintain accurate information.</li> </ul>	
44. Firearms/suspect package incidents.	<ul style="list-style-type: none"> <li>i. OSS delivering Police services – seen as appropriate place to dispose of weapons.</li> </ul>	<ul style="list-style-type: none"> <li>i. Physical harm to staff and customers</li> <li>ii. Damage to premises.</li> </ul>	<ul style="list-style-type: none"> <li>i. Procedures established</li> <li>ii. Training in place.</li> <li>iii. Risk assessments complete.</li> </ul>	

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
<p>45. Breakdown of partnership working within the face to face environment.</p>	<ul style="list-style-type: none"> <li>i. Differing organisational priorities.</li> <li>ii. Financial constraints.</li> <li>iii. Breakdown of relationships.</li> <li>iv. Withdrawal of political support.</li> </ul>	<ul style="list-style-type: none"> <li>i. Remain co-location only.</li> <li>ii. Organisational withdrawal from partnership.</li> <li>iii. Increased cost and non-realisation of partnership vision</li> <li>iv. Disruption to customer service.</li> <li>v. Reputational damage</li> <li>vi. Closure of face to face outlets.</li> </ul>	<ul style="list-style-type: none"> <li>i. Regular engagement at all appropriate levels to confirm priorities and activities.</li> <li>ii. Staff consultations and alignment of terms and conditions.</li> </ul>	
<p>46. Loss of premises.</p>	<ul style="list-style-type: none"> <li>i. Major incident e.g. flood, loss of power, building damage.</li> </ul>	<ul style="list-style-type: none"> <li>i. Service delivery compromised and resultant customer dissatisfaction.</li> <li>ii. Reputational damage.</li> </ul>	<ul style="list-style-type: none"> <li>i. Business continuity plan.</li> <li>ii. Offer service from alternative location or from CSC or Web.</li> </ul>	

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
<b>Service Specific – WEB</b>				
<p>47. Staff/customers unable to access Website or particular contents.</p>	<ul style="list-style-type: none"> <li>i. Current Content Management System (CMS) is old.</li> <li>ii. Technology failure – computers down.</li> </ul>	<ul style="list-style-type: none"> <li>i. Reduced service and / or service standard.</li> <li>ii. Increase in more expensive customer contacts via face to face visits and telephone.</li> <li>iii. Possible financial implications if customers unable to make payments online.</li> </ul>	<ul style="list-style-type: none"> <li>i. Replace CMS with new fit for purpose solution – procurement process underway.</li> <li>ii. Service Level Agreement with 3<sup>rd</sup> party supplier.</li> <li>iii. Contractual Agreement.</li> <li>iv. Agree with ICT acceptable level of downtime.</li> <li>v. Ability to set up 'dummy' website quickly for customer payments.</li> </ul>	<div style="text-align: center;">  <p>Impact</p> <p>Likelihood</p> </div>
<p>48. Content insufficient or fails to meet accessibility standards.</p>	<ul style="list-style-type: none"> <li>i. Service areas not entering information.</li> <li>ii. Service areas entering incorrect information.</li> <li>iii. Service areas not developing web solutions.</li> </ul>	<ul style="list-style-type: none"> <li>i. Increase in more expensive customer contacts via face to face visits and telephone.</li> <li>ii. Poor service to customers.</li> <li>iii. Possible financial penalties.</li> </ul>	<ul style="list-style-type: none"> <li>i. Web Implementation plan.</li> <li>ii. Service area plans.</li> <li>iii. Web Manager quality checks.</li> <li>iv. Expiry dates on pages for review</li> <li>v. External checking undertaken annually.</li> <li>vi. Annual accessibility audit.</li> </ul>	<div style="text-align: center;">  <p>Impact</p> <p>Likelihood</p> </div>

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
<b>Service Specific – Media Room</b>				
49. Inaccurate/Inappropriate Communication.	<ul style="list-style-type: none"> <li>i. Comms not co-ordinated.</li> <li>ii. Staff not using internal media team including ad agency.</li> <li>iii. Equality &amp; Diversity Guidelines are not followed.</li> <li>iv. Untrained staff.</li> </ul>	<ul style="list-style-type: none"> <li>i. Financial implications.</li> <li>ii. Incorrect or defamatory information given to media.</li> <li>iii. Customers irritated by receiving mass comms from council.</li> <li>iv. Wrong messages given to stakeholders.</li> </ul>	<ul style="list-style-type: none"> <li>i. Training given by media team through network group.</li> <li>ii. Robust signing off process.</li> <li>iii. Ensure all work passes through the media team for screening.</li> </ul>	
50. Breaching the Code of Recommended Practice on Local Authority Publicity.	<ul style="list-style-type: none"> <li>i. Staff are not aware of the publicity code.</li> </ul>	<ul style="list-style-type: none"> <li>i. Breaking legislation and possible investigation</li> <li>ii. Council reputation impacted.</li> </ul>	<ul style="list-style-type: none"> <li>i. Make all staff aware through media network group, list the simplified guide along with the full version on the media pages of the intranet, run training through network group and media drop in sessions.</li> </ul>	

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
51. Failure to meet production deadlines for print.	i. Lack of planning. ii. Machine breakdown. iii. Untrained staff.	i. Services disrupted. ii. Delayed committee meetings and decisions. iii. Customers not receiving information on time. iv. Council reputation impacted.	i. Machine Maintenance scheduled with contractor. ii. Training of staff. iii. Service areas to plan work to add contingency to deadlines.	
52. Communications not in plain English or meeting accessibility guidelines.	i. Untrained staff. ii. Use of external design agencies or partners.	i. Contravening E&D policy. ii. Customers not informed. iii. Possible financial penalty. iv. Council reputation impacted.	i. Trained staff. ii. Service areas to send work to Media room for checking.	

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
------------------	-------------------	-----------------------	---------------------------	----------------------

**Service Specific – Document Management Centre**

<p>53. WDC is not able to process payments.</p>	<ul style="list-style-type: none"> <li>i. Allpay system fails.</li> <li>ii. Capita system fails.</li> <li>iii. Failure to comply with PCI DSS.</li> <li>iv. Security breach.</li> <li>v. Technology failure.</li> </ul>	<ul style="list-style-type: none"> <li>i. Loss or reduction of service .</li> <li>ii. Loss of income.</li> <li>iii. Reputation damaged.</li> <li>iv. Possible fines imposed.</li> <li>v. Customers required to pay cash and additional costs this incurs.</li> </ul>	<ul style="list-style-type: none"> <li>i. Regular account management meetings with Allpay, Capita</li> <li>ii. Project to ensure compliance with PCI DSS.</li> <li>iii. Ability to set up 'dummy' website quickly for customer payments.</li> <li>iv. Service areas encouraging Direct Debit take up.</li> </ul>	
<p>54. Not able to handle and processing incoming and outgoing documents, including post.</p>	<ul style="list-style-type: none"> <li>i. DSA fails to collect / deliver mail.</li> <li>ii. Trained staff not available.</li> </ul>	<ul style="list-style-type: none"> <li>i. Loss or reduction of service.</li> <li>ii. Increased cost re use of Royal Mail.</li> <li>iii. Reputation damaged.</li> </ul>	<ul style="list-style-type: none"> <li>i. Regular account management meetings with provider.</li> <li>ii. Business continuity process from provider.</li> <li>iii. Staff training</li> <li>iv. Processes documented.</li> <li>v. Use of temporary staff.</li> </ul>	

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation / Control	Residual Risk Rating
55. Insufficient stock of travel tokens.	<ul style="list-style-type: none"> <li>i. Poor planning</li> <li>ii. Delivery failure.</li> <li>iii. Unanticipated demand.</li> </ul>	<ul style="list-style-type: none"> <li>i. Increased customer complaints.</li> <li>ii. Adverse publicity.</li> </ul>	<ul style="list-style-type: none"> <li>i. Regular account management meetings.</li> <li>ii. Stock management.</li> <li>iii. Monitoring of customer demand.</li> </ul>	