

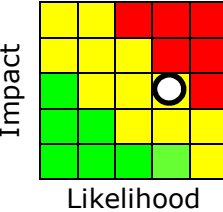
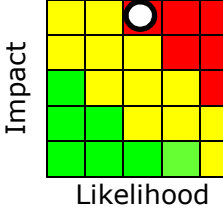
Chief Executive's Office Risk Register - October 2016

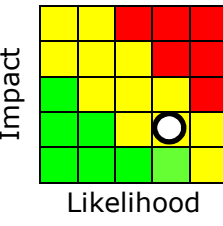
Introduction

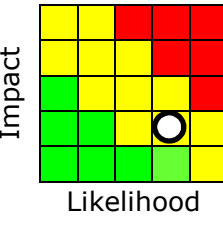
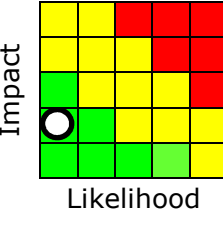
The Chief Executive's Office has adopted a layered approach to risk management which ensures risks are managed at an appropriated level.

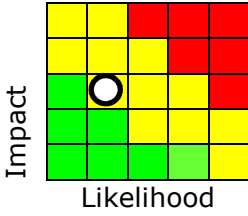
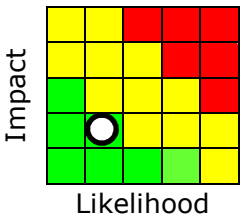
- The **Significant Business Risk Register** contains the CXO risks which have the potential to have a **significant** adverse impact on the Council. It is the responsibility of CXO team managers to advise, through their head of service, SMT of these risks so that SMT can decide whether to update the corporate risk register as appropriate.
- The **CXO Risk Register** identifies the high level Service Area risks that have the potential to adversely impact multiple Service Areas. The document uses the corporate formatting standard and uses language that is more understandable to the business. The format also supports political scrutiny.
- **Thematic Risk Registers** are used to identify risks associated with particular aspects of the CXO's service that requires additional focus and risk management. For example, ICT has a specific risk register that relates to malware.
- **Project Risk Registers** are created, when appropriate, to manage the risks associated with the introduction of new technology.
- **Individual Risks Assessments** are created when a Request for Service requires a deviation from an agreed policy.
- The **Team Operational Plan** contains the key operational service risks for the period of the plan.

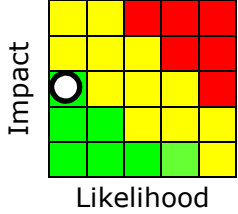
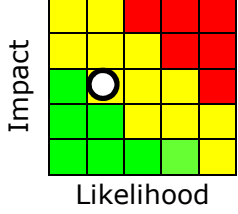
Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation/Control	Required Action(s)	Responsible Officer	Residual Risk Rating
1. Unauthorised Disclosure.	i. Hacking ii. Spyware iii. Emailing the wrong recipient iv. Stolen equipment; laptops, USB devices v. Lost devices vi. Poor hardware disposal practices vii. Poor password management viii. Allowing unauthorised third parties, including family & friends, to utilise Council equipment and/or software. ix. Forwarding council emails to unauthorised accounts/devices x. Leak by Councillor/Officer.	i. Potential fines; ICO, DP. ii. Reputational damage. iii. Legal challenge; e.g. contract disclosure iv. Lost opportunity to develop projects. v. Legal challenge vi. Compensation claim made for distress, loss of business	i. Information Security Policy ii. Penetration testing iii. Perimeter protection; Firewall, 2 Factor Authentication iv. Disk encryption v. USB device restriction and encryption. vi. Virtual Desktops vii. Sandboxed applications viii. Information governance is a standing item on the ICTSG agenda. ix. Third Party Network Access Agreement x. Non-Disclosure Agreements xi. Destruction certificates for equipment disposal. xii. Ad-hoc compliance monitoring xiii. Appropriate Codes of Conduct.	i. Corporate review and implement Data Handling Policy, Data Classification and Retention & Disposal Policy. ii. Staff training	CMT SMTplus SIRO DPO	<p>The risk rating matrix is a 4x4 grid. The vertical axis is labeled 'Impact' and the horizontal axis is labeled 'Likelihood'. The grid cells are colored as follows: (Impact 1, Likelihood 1) is Green; (Impact 1, Likelihood 2) is Yellow; (Impact 1, Likelihood 3) is Yellow; (Impact 1, Likelihood 4) is Yellow; (Impact 2, Likelihood 1) is Green; (Impact 2, Likelihood 2) is Yellow; (Impact 2, Likelihood 3) is Red; (Impact 2, Likelihood 4) is Red; (Impact 3, Likelihood 1) is Green; (Impact 3, Likelihood 2) is Yellow; (Impact 3, Likelihood 3) is Red; (Impact 3, Likelihood 4) is Red; (Impact 4, Likelihood 1) is Green; (Impact 4, Likelihood 2) is Yellow; (Impact 4, Likelihood 3) is Red; (Impact 4, Likelihood 4) is Red. A white circle with a black outline is placed in the center of the grid, specifically at the intersection of Impact 2 and Likelihood 2.</p>

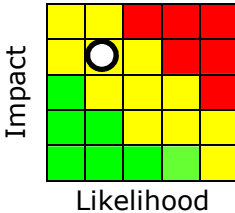
Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation/Control	Required Action(s)	Responsible Officer	Residual Risk Rating
2. Non-Availability of Staff.	<ul style="list-style-type: none"> i. Failure to identify gaps in staff skills & capacity that could lead to poor service delivery. ii. Poor planning to cover holidays, sickness, training, elections, etc. iii. Poor project management. iv. Epidemic v. Strike Action 	<ul style="list-style-type: none"> i. Additional costs for specialist advice. ii. Increased service outages. iii. Increased duration of service outages. iv. Inability to deliver Council objectives. v. Increased stress on residual staff. vi. Reduced level of service vii. Reduced level of resilience 	<ul style="list-style-type: none"> i. Shared Services. ii. Workforce planning. iii. Generic Roles where ever possible. iv. Third party Support & Maintenance Contracts. v. Business Continuity – Staff Absence Strategy. vi. Documented procedures vii. Contract staff/consultancy viii. Training on roles to build resilience ix. Managing Attendance Policy 	i. HR & DS plans need reviewing	DMO HRM ICTSM DMT CMT	
3. Inability to retain and subsequently recruit staff.	<ul style="list-style-type: none"> i. Staff turnover due to: <ul style="list-style-type: none"> a. Salary b. Training c. T&C d. Working Environment e. Career Progression f. Morale g. Age profile ii. Uncertainty of employment prospects with WDC and Local Government iii. Poor recruitment processes 	<ul style="list-style-type: none"> i. Additional costs for specialist advice. ii. Increased service outages. iii. Increased duration of service outages. iv. Inability to deliver Council objectives. v. Increased stress on residual staff. vi. Reduced level of service vii. Reduced level of resilience 	<ul style="list-style-type: none"> i. Shared Services. ii. Workforce planning. iii. Generic roles where ever possible. iv. Appropriate training budget to enable training and development opportunities. v. Contract staff/consultancy vi. Training on roles to build resilience vii. Robust recruitment process with staff training programme viii. Professional staff management including one to ones/appraisals/staff development and stress management ix. Redeployment Policy x. Development paths linked to PDP's xi. Publicise the benefits of working for the Council 	i. Salary, benefits & recruitment review 2016/17	DMO HRM ICTSM DMT CMT	

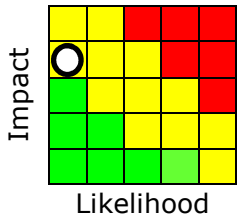
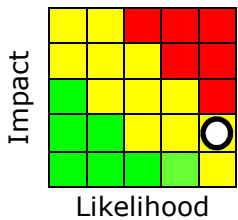
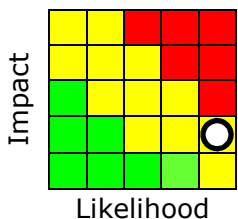
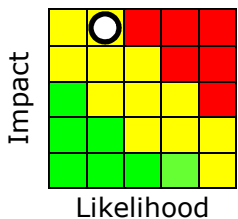
Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation/Control	Required Action(s)	Responsible Officer	Residual Risk Rating
4. Loss of Data or Data Integrity.	<ul style="list-style-type: none"> i. Hacking. ii. Human error. iii. Poor change management. iv. Little or no testing of new software releases. v. Viruses. vi. Poor password management. vii. Insecure web applications. viii. Software bugs. ix. Inappropriate access rights. x. Hardware corruption. xi. Poor training. xii. Malicious intent. xiii. Unlocked computers during absence. 	<ul style="list-style-type: none"> i. Loss of service to the customer. ii. Processing backlogs. iii. Potential loss of income. iv. Reputational damage. v. Fraud. vi. Cost of recovery 	<ul style="list-style-type: none"> i. Perimeter protection; Firewall, 2 Factor Authentication, Spam filter, Antivirus, etc. ii. Test plans. iii. Penetration testing (Ethical Hacking). iv. Antivirus strategy. v. Audits (Internal, 3rd Party ICT Auditors, Communications-Electronics Security Group (CESG), PCI DSS) vi. Activity logs. vii. Staff Training. viii. Code of Connection. ix. Information Security Policy. x. Recruitment using the Baseline Personnel Security Standard. xi. Supplier support contracts. xii. GovCertUk notifications of threats and vulnerabilities. xiii. Nominated system owners to manage systems. xiv. Information governance is a standing item on the ICTSG agenda. 	Implement Intrusion detection as part of the next firewall upgrade.	SMT ICTSM HRM DMO DMT SO	 <p style="text-align: center;">Impact</p> <p style="text-align: center;">Likelihood</p>

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation/Control	Required Action(s)	Responsible Officer	Residual Risk Rating
<p>5. Loss of Council computer facilities (Servers, Storage, Network, Voice).</p>	<ul style="list-style-type: none"> i. Human error. ii. Hardware/software failure (OS). iii. Poor change management iv. Fire/Flood (Environmental and/or internal service failure) 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 	<ul style="list-style-type: none"> i. Loss of service to the customer. ii. Processing backlogs iii. Potential loss of income. iv. Reputational damage v. Loss of data. vi. Significant stress on key personnel during recovery period. vii. Potential costs 	<ul style="list-style-type: none"> i. Staff training. ii. Technical documentation. iii. Hardware resilience. iv. Backup generator/Uninterruptible Power Supply (UPS). v. Offsite backup tapes. vi. External 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. xx. team Business Continuity plans 	<ul style="list-style-type: none"> i. Review business continuity arrangements for voice due to the repatriation of the contact centre ii. HR & DS plans need reviewing 	<p>CMT SMT ICTSM HRM DMO DMT SO FM</p>	
<p>6. Failure of Service Providers.</p>	<ul style="list-style-type: none"> i. Bankruptcy. ii. Natural disaster. iii. Takeover. iv. Legal (Intellectual property infringement). v. Change of strategy (no longer wish to supply the product or service). 	<ul style="list-style-type: none"> i. Non-supported system. ii. Impact on resources of system replacement; human, financial, etc. iii. Potential loss of service to the customer. iv. Potential loss of income. v. Potential inability to deliver Council objectives. vi. Hosted Systems; No access to system or data. 	<ul style="list-style-type: none"> i. Change freeze. ii. Shared service. iii. Emergency procurement. iv. Business Continuity - Business Application Supplier Strategy. v. Financial vetting of suppliers as part of the procurement process. 		<p>ICTSM DMO HRM SO Proc</p>	

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation/Control	Required Action(s)	Responsible Officer	Residual Risk Rating
7. Failure to achieve or maintain PSN compliance	i. Time constraints ii. Cost iii. Inconsistent assessment process. iv. Changes to the compliance regime with little or no notice.	Inability to deliver the following services: <ul style="list-style-type: none"> • Government Connect Mail i.e. (gcsx.gov.uk) • DWP Customer Information System (Revs & Bens) • Data Transfer Appliance (Revs and Bens) • Tell Us Once Appliance (Revs and Bens) • National Resilience Extranet (Civil Contingencies) • Individual Electoral Registration i. LoCTA Service (Revs & Bens)	i. Undertake regular awareness training to understand the requirements. ii. Communicate the implications to the business to ensure compliance. iii. Where possible anticipate budget implications and make provision. iv. Engage a security specialist to advise on compliance.		SMT SIRO ICTSM DMO SO	
8. Failure to communicate effectively/giving incorrect information and advice	i. Untrained staff ii. Reorganisation iii. Inaccurate data on systems or website iv. Poor communication/information v. High workload. vi. Reliance on key staff. vii. Staff absence. viii. Human error. ix. Inappropriate form of communication.	i. Incorrect information used to carry out work. ii. Negligence and liability claims iii. Adverse publicity iv. Loss of reputation v. Waste of resource vi. Poor service to customers vii. Additional workload. viii. Impact to health & wellbeing	i. Team meetings. ii. One-to-ones. iii. E-mail. iv. Core brief. v. Intranet. vi. Circulation of minutes from meetings. vii. Corporate communication strategy / Media Team. viii. Staff training. ix. Qualified/experienced staff x. Quality standards xi. Good IT/Information Systems xii. Web improvement plan		ICTSM DMO HRM	

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation/Control	Required Action(s)	Responsible Officer	Residual Risk Rating
9. Breaches of financial controls as they relate to the service	<ul style="list-style-type: none"> i. Lack of awareness ii. Lack of training iii. Malicious intent iv. Unsuitable controls driving inappropriate behaviour 	<ul style="list-style-type: none"> i. Fraud ii. Poor value for money iii. Contractual issues, inc performance iv. Reputational damage 	<ul style="list-style-type: none"> i. Code of financial practice ii. Code of procurement iii. Whistleblowing policy iv. Anti-Fraud & Corruption policy v. Audits vi. Staff training vii. Contracts register viii. Annual budget acceptance / signature by ICTSM ix. Monthly budget monitoring x. Corporate processes for managing expenditure. xi. Appropriate Codes of Conduct for Councillors/Officers 		DCE ICTSM DMO HRM Proc HoF Audit	
10. Insufficient budget to deliver the service	<ul style="list-style-type: none"> i. Council budget constraints. ii. Poor budget management iii. Change to software licensing models by vendors; MS, Cisco, VMWare. iv. Dollar exchange rate 	<ul style="list-style-type: none"> i. Inability to deliver the service. ii. Inability to deliver the Service Area Plan iii. Opportunity costs. iv. Increased service failures through lack of investment 	<ul style="list-style-type: none"> i. Annual budget setting process ii. Creation of an ICT Services Equipment Reserve iii. Rigorous Software Asset Management (SAM) 		Council CMT ICTSM DMO HRM	

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation/Control	Required Action(s)	Responsible Officer	Residual Risk Rating
<p>11. Failure to protect staff, Councillors and customers from physical Health and Safety Risks</p>	<ul style="list-style-type: none"> i. Lack of health and safety good practice ii. Customer dissatisfaction. iii. Accident. iv. Intruders in offices. v. Staff in building very early and/or very late. vi. Violence/threatening customers. vii. Home working. viii. Driving for work. ix. D.S.E. / V.D.U. usage. x. Manual handling. xi. Person falling from height. xii. Items falling from height. xiii. Failure to undertake necessary adaptations for individual needs. 	<ul style="list-style-type: none"> i. Actual physical injury ii. Health and safety investigation iii. Traumatized staff iv. Stress v. Increase in sickness absence vi. Death vii. Reduced staff morale viii. Legal action ix. Penalties/Fines/Compensation 	<ul style="list-style-type: none"> i. Health and Safety Policy ii. Robust Risk Assessments, iii. DSE Assessments iv. Accident/incident reporting and investigation v. Tunstall procedure. vi. Joint consultative safety Panel. vii. Training/induction viii. Policies. ix. Reporting/monitoring procedures. x. Manual Handling Procedures xi. Door access controls xii. Portable Appliance Testing (PAT) xiii. Corporate health and safety policy including Home working and Driving at work. xiv. Eye tests. xv. Regular DSE assessments. xvi. Health and safety risk assessments (AssessNET). xvii. Training available. xviii. Insurance cover. xix. Health & safety on team meeting agendas. xx. Home working policy. xxi. Procedures for public meetings xxii. Liaison with the Town Hall for meetings anticipated to have significant (greater than 35) levels of public present. xxiii. Monitoring of staff alert list to see if the public known to attend meeting may cause a greater risk (then enhanced staffing/security as appropriate) 		<p>CMT ICTSM DMO HRM Health & Safety Officer Theatre and Town Hall Manager</p>	 <p>The matrix is a 4x4 grid with Impact on the vertical axis and Likelihood on the horizontal axis. The colors represent risk levels: Green (1), Yellow (2), Orange (3), and Red (4). A white circle with a black outline is placed in the cell corresponding to Low Likelihood and Low Impact, indicating a risk level of 2.</p>

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation/Control	Required Action(s)	Responsible Officer	Residual Risk Rating
12. Failure to adhere to the Constitution, legislative requirements and guidance by the Council.	<ul style="list-style-type: none"> i. Misinterpret regulations or the Constitution ii. Constitution not maintained so does not reflect current legislation iii. Failure to publish agendas in line with statutory requirements iv. Lack of concentration; v. poor chairing of meeting; vi. Human error. vii. Awareness viii. Incorrect legal advice ix. Incorrect interpretation 	<ul style="list-style-type: none"> i. Ultra vires decision ii. Potential legal action iii. Potential costs to the Council following successful legal decision iv. Bad publicity v. Decisions delayed vi. Financial loss. vii. Project delays 	<ul style="list-style-type: none"> i. Training ii. Knowledge of Constitution, legislative requirements and guidance iii. Attendance of Legal Services at Planning, Licensing and Regulatory Panels iv. Comprehensive induction for Councillors v. Regular reviews of Constitution to ensure it reflects current legislation vi. Ensuring hand over of work for Committee team members when away from the office to ensure deadlines are not missed vii. Checks and procedures within team; effective Chair to ensure clarity on decision being taken. 		DCE DMO ICTSM HRM	
13. Failing to respond to requests for information under DP/FOI/EIR appropriately and within timescales	<ul style="list-style-type: none"> i. Inability to locate/access required information within time; ii. failure to monitor deadline iii. insufficient resources iv. Poor planning v. Failure to identify appropriate responder. vi. Poor or insufficient training. 	<ul style="list-style-type: none"> i. Loss of public confidence. ii. Referrals of the Council to the Information Commissioner by dissatisfied members of the public. iii. Intervention & Sanctions 	<ul style="list-style-type: none"> i. Awareness of changes in legislation/Government advice. ii. Monitoring of FOI/EIR/DP systems put in place Council wide to ensure they are working. iii. Emphasise importance of responding to these from CMT 		DMO	
14. The complaints process is not adhered to when considering a complaint.	<ul style="list-style-type: none"> i. Lack of available resources due to demands of other projects and work on the team. ii. In experienced officers iii. Officers not aware of relevant process to be followed iv. Complaints policy does not reflect the current operating environment. 	<ul style="list-style-type: none"> i. Also a lack of transparency for the public ii. Referral to LGO iii. LGO sanction iv. compromise an insurance claim which may be received after a complaint has been replied to. 	<ul style="list-style-type: none"> i. Training ii. CST monitoring iii. HoS/CE sign-off complaints as appropriate iv. Referral to appropriate LGO material. 	Report to come forward to CMT in Autumn 2016 on revised procedure.	CE DMO	
15. Failure to deliver corporate strategies / initiatives	<ul style="list-style-type: none"> i. Lack of available resources due to demands of other projects and work on the team. ii. insufficient resources iii. Poor planning iv. Change in policy v. Lack of engagement 	<ul style="list-style-type: none"> i. Financial or opportunity loss ii. Loss of staff/public confidence iii. Impact on health and wellbeing 	<ul style="list-style-type: none"> i. Robust project planning ii. Staff/Union/Member engagement / Communication iii. SMT support 		SMT ICTSM HRM DMO	

Key:

New narrative

Narrative being transferred

~~Deleted narrative~~

⊕ = Current risk score

⊖ = Previous risk score (and direction)

Personnel Key:

CMT – Corporate Management Team

SMT – Senior Management Team

CE – Chief Executive

DCE– Deputy Chief Executive & Monitoring Officer

DMO – Deputy Monitoring Officer and Democratic Services Manager

DMT – Departmental Management Team

ICTSM – ICT Services Manager

SIRO – Senior Information Risk Owner (DCE)

DPO – Data Protection Officer (DMO)

SO – System Owners

FM – Facilities Manager

EM – Elections Manager & Deputy Returning Officer

HRM – Human Resources Manager

Proc – Procurement Manager

HoF – Head of Finance