Chief Executive's Office Risk Register
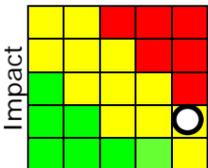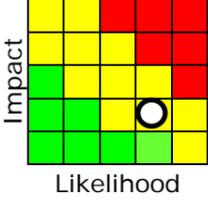
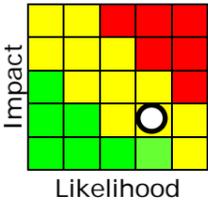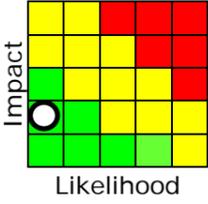| CXO Risk Register Governance	
Accountable	Chief Executive
Responsible	ICT Services Manager, Democratic Services Manager, HR Manager and Asset Manager
Consulted	All CXO Teams
Informed	Finance & Audit Scrutiny Committee
Review Date	31st Jan 2020

The Chief Executive's Office has adopted a layered approach to risk management which ensures risks are managed at an appropriated level.
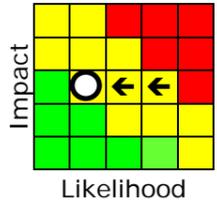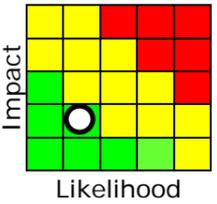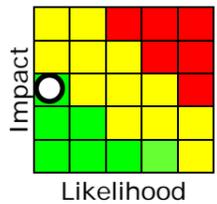
- The **Significant Business Risk Register** contains the CXO risks which have the potential to have a **significant** adverse impact on the Council. It is the responsibility of CXO team managers to advise, through their head of service, SMT of these risks so that SMT can decide whether to update the 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.
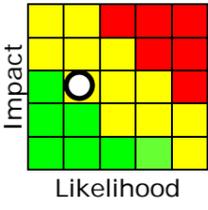
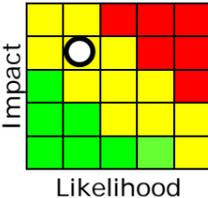| Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation/Control	Required Action(s)	Responsible Officer	Residual Risk Rating
1. Unauthorised Disclosure.	i. Hacking ii. Spyware iii. Emailing the wrong recipient iv. Stolen equipment; laptops, USB devices v. Lost devices vi. Poor hardware 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. Intentional disclosure by Councillor/Officer. xi. Unintentional disclosure 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. xiv. Information Governance Manager (DPO). xv. Staff training xvi. Register of Processing Activities & Data Retention Schedules in place and reviewed quarterly	i. Staff training (on-going)	CMT SMTplus SIRO IGM/DPO	 Evidence of multiple unauthorised disclosures due to not following existing policies. To date minimum impact. Follow up training provided as appropriate.

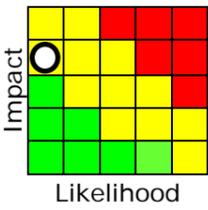| Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation/Control	Required Action(s)	Responsible Officer	Residual Risk Rating
2. Non-Availability of Staff.	i. Failure to identify gaps in staff skills & capacity that could lead to poor service delivery. ii. Poor planning to cover holidays, sickness, training, elections, etc. iii. Poor project management. iv. Epidemic v. Strike Action	i. Additional costs for specialist advice. ii. Increased service outages. iii. Increased duration of service outages. iv. Inability to deliver Council objectives. v. Failure to meet statutory or contractual obligations vi. Increased stress on residual staff. vii. Reduced level of service viii. Reduced level of resilience ix. Reputational damage	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 x. Long Term Sickness and Ill Health Capability Policy	i. Completion of Assets Team redesign	DMO HRM AM ICTSM DMT CMT	
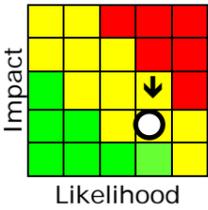
3. Inability to retain and subsequently recruit staff.	i. Staff turnover due to:
	  a. Salary
	  b. Training
	  c. T&C
	  d. Working Environment
	  e. Career Progression
	  f. Morale
	  g. Age profile
	  h. Service redesign
	ii. Uncertainty of employment prospects with WDC and Local Government
	iii. Poor recruitment processes
		i. Additional costs for specialist advice.
		ii. Increased service outages.
		iii. Increased duration of service outages.
		iv. Inability to deliver Council objectives.
		v. Failure to meet statutory or contractual obligations
		vi. Increased stress on residual staff.
		vii. Reduced level of service
		viii. Reduced level of resilience
		ix. Reputational damage
			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. Performance management framework including one to ones/appraisals/staff development.
			ix. Redeployment Policy
			x. Development paths linked to PDP's
			xi. Publicise the benefits of working for the Council
			xii. Market Forces Supplement Policy
			xiii. Recruitment branding e.g. refer a friend & social media
				i. Vacancies – Assets & Democratic	DMO
					HRM
					AM
					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.	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.	i. Loss of service to the customer. ii. Processing backlogs. iii. Potential loss of income. iv. Reputational damage. v. Fraud. vi. Cost of recovery	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. xv. Information Governance Group xvi. <mark>Register of Processing Activities & Data Retention Schedules in place and reviewed quarterly</mark>	i. ~~Implement Intrusion detection.~~	SMT ICTSM HRM DMO AM DMT SO	

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation/Control	Required Action(s)	Responsible Officer	Residual Risk Rating
5. Loss of Council computer facilities (*Servers, Storage, Network, Voice*).	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	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	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	i. Review business continuity arrangements for voice due to the repatriation of the contact centre (Ongoing)	CMT SMT ICTSM HRM DMO AM DMT SO FM	
6. Failure of Service Providers or Contractors to deliver services.	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). vi. Poor procurement or contract management procedures	i. Non-supported system. ii. Impact on resources of system/contractor 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. Potential inability to deliver statutory obligations vii. Potential damage to Council property assets viii. Hosted Systems; No access to system or data.	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. vi. Contract management training and processes		ICTSM DMO HRM AM SO Proc	

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: i. Government Connect Mail i.e. (gcsx.gov.uk) ii. DWP Customer Information System (Revs & Bens) iii. Data Transfer Appliance (Revs and Bens) iv. Tell Us Once Appliance (Revs and Bens) v. National Resilience Extranet (Civil Contingencies) vi. Individual Electoral Registration vii. 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.	i. Complete PSN action plan	SMT SIRO ICTSM DMO SO	Impact / Likelihood
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. Intranet. v. Circulation of minutes from meetings. vi. Corporate communication strategy / Media Team. vii. Staff training. viii. Qualified/experienced staff ix. Quality standards x. Good IT/Information Systems xi. Web improvement plan	i. Review of Intranet content ii. Emergency information portal on O365	ICTSM DMO HRM AM	Impact / Likelihood
9. Breaches of financial controls as they relate to the service	i. Lack of awareness ii. Lack of training iii. Malicious intent iv. Unsuitable controls driving inappropriate behaviour	i. Fraud ii. Poor value for money iii. Contractual issues, inc performance iv. Reputational damage	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 (AJ) ICTSM DMO HRM AM Proc HoF Audit	Impact / Likelihood

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation/Control	Required Action(s)	Responsible Officer	Residual Risk Rating
10. Insufficient budget to deliver the service	i. Council budget constraints. ii. Poor budget management iii. Change to software licensing models by vendors; MS, Cisco, VMWare. iv. Dollar exchange rate v. Major uninsured/uninsurable incident vi. Increase in organisational demand which impacts support services; growth in staff, users, cllrs, assets	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	i. Annual budget setting process ii. Creation of an ICT Services Equipment Reserve iii. Rigorous Software Asset Management (SAM)		Council CMT ICTSM DMO HRM AM	

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation/Control	Required Action(s)	Responsible Officer	Residual Risk Rating
11. Failure to protect staff, Councillors, contractors and customers from physical Health and Safety Risks	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. Agile 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 adaptions for individual needs. xiv. Inadequate risk assessments or method statements xv. Failure to survey, monitor or manage asbestos containing materials in accordance with CAR 2012 xvi. Failure of contractor to check the Asbestos Register xvii. Poor contractor training xviii. Tenants or leaseholders not informed of the presence of asbestos containing materials in HRA homes or leased assets xix. Inadequate safety compliance regime xx. Inadequate gas appliance maintenance and certification xxi. Inadequate electrical testing of HRA and corporate assets xxii. Inadequate fire safety measures in HRA blocks or corporate assets xxiii. Failure to adequately maintain the building fabric of assets, paths, structures, rural street and footway lighting etc.	i. Actual physical injury ii. Exposure to asbestos or legionella iii. Health and safety investigation iv. Traumatised staff v. Stress vi. Increase in sickness absence vii. Death viii. Reduced staff morale ix. Legal action including imprisonment x. Penalties/Fines/Compensation xi. Reputational damage	i. Health and Safety Policy and reporting/monitoring procedures ii. Partnership links with MAPPA, Police and Social Services iii. Robust Risk Assessments, iv. Regular DSE Assessments v. Accident/incident reporting and investigation vi. Tunstall lone working procedure. vii. Joint consultative safety Panel. viii. Asset Compliance Group ix. Asset Steering Group x. Training/induction xi. Manual Handling Procedures xii. Door access controls xiii. Portable Appliance Testing (PAT) xiv. Corporate health and safety policy including Home working and Driving at work. xv. Eye tests. xvi. Health and safety risk assessments (AssessNET). xvii. Training and training logs. xviii. Insurance cover. xix. Health & safety on team meeting agendas. xx. Home working policy. xxi. Procedures for public meetings and monitoring of staff alert list to see if the public known to be attending meetings requires additional staffing/security to be deployed xxii. Liaison with the Town Hall for meetings anticipated to have significant (greater than 35) levels of public present. xxiii. Asbestos Management Plan, Asbestos Register, Asbestos removal programme, issue of information at letting/lease signing xxiv. Appropriate testing, repair and improvement contracts in place. xxv. Provision of PPE to appropriate staff xxvi. Accident reporting and investigation xxvii. COSSH, safe systems at work and permits to work	i. Risk assessments need reviewing for public meetings ii. Corporate review of Lone Working arrangements iii. Complete Asset Compliance Group baseline mapping to enable Asset Steering Group to review need for revised procedures or allocation of responsibilities iv. Review adequacy of ActiveH to store compliance information v. Procure new FRAs for multi-storey blocks when programme of works completed vi. Refresh Home Working Policy (Agile)	CMT SMT DCE (BH) ACG ICTSM DMO AM HRM Health & Safety Officer Theatre and Town Hall Manager Building Managers	Impact / Likelihood

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation/Control	Required Action(s)	Responsible Officer	Residual Risk Rating
			xxviii. Gas servicing, electrical programme xix. Legal procedures for gaining access to properties to undertake gas services xx. Storage of compliance and testing records on assets database xxi. Appropriate building insurance xxii. Programme of updating Fire Risk Assessments xxiii. Post-Grenfell programme of works to HRA multi-storey blocks xxiv. Liaison with WFRS xxv. Stock Condition survey information and cyclical updating programme xxvi. Inspection regimes xxvii. Tenancy and lease agreements			
12. Failure to adhere to the Constitution, legislative requirements and guidance by the Council.	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. Failure to comply with policies or procedures v. Lack of concentration; vi. Poor chairing of meeting; vii. Human error. viii. Lack of awareness ix. Incorrect legal advice x. Incorrect interpretation xi. Lack of training xii. Inadequate supervision or management procedures xiii. Fraud/corruption by staff or contractors	i. Ultra vires decision ii. Failure to deliver statutory or contractual obligations iii. Potential legal action iv. Potential costs to the Council following successful legal decision v. Bad publicity vi. Decisions delayed vii. Financial loss. viii. Project delays	i. Training / MetaCompliance 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. viii. Effective supervision and management controls in place including; one to ones, team meetings, appraisals, training, recruitment & selection, capability etc. ix. Corporate audit programme x. Separation of duties xi. Declarations of interest and gifts & hospitality xii. Budgetary control regime xiii. Ability to deactivate stolen electronic devices	i. ~~Complete delivery of the new cllr induction programme~~	DCE (AJ) DCE (BH) DMO ICTSM HRM AM	

Risk Description	Possible Triggers	Possible Consequences	Risk Mitigation/Control	Required Action(s)	Responsible Officer	Residual Risk Rating
13. Failing to respond to requests for information under DP/FOI/EIR appropriately and within timescales	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	i. Loss of public confidence. ii. Referrals of the Council to the Information Commissioner by dissatisfied members of the public. iii. Intervention & Sanctions	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 IGM/DPO	Impact / Likelihood grid
14. The complaints process is not adhered to when considering a complaint.	i. Lack of available resources due to demands of other projects and work on the team. ii. Inexperienced officers iii. Officers not aware of relevant process to be followed iv. Complaints policy does not reflect the current operating environment.	i. 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.	i. Training ii. CST monitoring iii. HoS/CE sign-off complaints as appropriate iv. Referral to appropriate LGO material.	i. Review of complaints process is in SA Plan 2020	CE DMO	Impact / Likelihood grid
15. Failure to deliver corporate strategies / initiatives	i. Insufficient resources ii. Poor planning iii. Lack of engagement with customers iv. Change in scope v. Politics	i. Financial or opportunity loss ii. Failure to meet statutory responsibilities iii. Loss of staff/public confidence iv. Impact on health and wellbeing v. Reputational damage vi. Morale	i. Programme prioritisation ii. Robust project planning iii. Staff/Union/Member engagement / Communication iv. SMT support		SMT ICTSM HRM DMO AM	Impact / Likelihood grid Limited progress on Digital Strategy Office Move

Key:
New narrative
Narrative transferred from former H&PS Risk Register
Deleted narrative
O = Current risk score
→ ← ↑ ↓ ↙ = Previous risk score (and direction)

Personnel Key:
CMT – Corporate Management Team
SMT – Senior Management Team
CE – Chief Executive
DCE (AJ) – Deputy Chief Executive & Monitoring Officer
DCE (BH) – Deputy Chief Executive

DMO –   Deputy Monitoring Officer and Democratic Services Manager
DMT –   Departmental Management Team
ICTSM –   ICT Services Manager
SIRO –   Senior Information Risk Owner (DCE AJ)
DPO –   Data Protection Officer (DMO)
SO –   System Owners
FM –   Facilities Manager
AM –   Asset Manager
EM –   Elections Manager & Deputy Returning Officer
HRM –   Human Resources Manager
Proc –   Procurement Manager
HoF –   Head of Finance
ACG –   Asset Compliance Group
IGM/DPO -   Information Governance Manager/Data Protection Officer