APPENDIX 2

Strategic Risk Register 2016/2017

Identified Strategic Risks

Risk	Risks mitigation method	Monitoring Body
Local Plan - risk that if the Local Plan is not submitted to the Secretary of State by early 2017, that any new allocation of New Homes Bonus due to the Council in that year will be withheld.	Action Plan	Development Committee
LCC Cost Sharing- risk that changes to the LCC cost sharing agreement on waste will result in a significant negative impact on resources making it difficult to deliver the Council's other priorities.	Progress reported to Operational Management and reported in terms of financial implications through the MTFS	Operational Management & Finance Committee
Financial Challenges - medium term risk that the Council is unable to deliver key projects and services due to limited and reducing resources.	Managed via MTFS	Finance Committee
Cyber Attacks - risk that the Council's infrastructure is disabled by cyber-attack such that services cannot be delivered effectively.	Risk Action Plan	SRMG & Reports to Audit Committee

Risk Reports to the SRMG and Audit and Standards Committee will include updates on the Cyber Attack Prevention Action Plan.

Reporting on the other strategic risks will be made to the SRMG quarterly and to the Audit and Standards committee on an exception basis only.

APPENDIX 2

2016/2017 Risk Register

Cyber Attack Prevention Action Plan No: 1

Champion – Director of Resources

Issue Description	Cyber Attack Prevention
Council Objective	Value for money

EXISTING CONTROLS IN PLACE
✓ Two corporate firewalls in place, with redundancy should one be compromised or fail
✓ Separate firewall for PSN (Public Services Network secure) originated traffic
✓ Proxy server and separate web filters based on user profiles
✓ Desktop Anti-virus (McAfee)
✓ Wave safe end control (end point security for restricting/ blocking USB devices)
✓ Intrusion Protection (IPS)
✓ Application control (Deep pack inspection including SSL traffic)
✓ Appsure Backup solution
✓ Virus awareness communications
✓ Web logs (monitoring)
✓ CERT UK, networking, attending conferences
✓ Patch policy, every Tuesday from Microsoft/ application vendors for security updates
✓ Test environment for enable new patches or updates
✓ Data Leak Prevention (DLP)
✓ Anti-virus/ anti malware at the firewall level
✓ Fusemail spam and email filtering
✓ Fortimail internally hosted spam and email filtering for PSN (Public Services Network secure) originated email exchange
✓ Network address translation (NAT) across all firewalls to 'hide' our network IP ranges behind outward facing Public ones
✓ Network connection redundancy through a separate link to the outside from the Cem and Crem
✓ SSID filtering and secure authentication through Cisco wireless controller
✓ Demilitarized zone for outward facing web servers
✓ Reverse proxy for outward facing web services, that are required to be hosted internally

APPENDIX 2

Required action / control	Responsible for action	Critical success factors	Due Dates
Staff engagement and awareness programme of potential cyber threats	A.Scrivens	Review existing ICT Computer Security Policy with assistance from Blackpool Policy services.	April 2016
	A.Scrivens / R.Mckelvie	Review current ICT Security iPool module content, contact Blackpool to see if there has been any updates to their content since original version done (2011). Liaise with ICT to add wording for Fylde and make any relevant or necessary changes etc. Re-vamp and modernise content.	April 2016
	A.Scrivens	Use recent PowerPoint slides and quiz published by ICT to show what virus look like, add onto new iPool module as a quiz.	May 2016
	A.Scrivens	Relaunch ICT Security iPool Module, setup as next compulsory course for all staff to complete.	June 2016
	R.Mckelvie	IT network policy enforcement logon software	June 2016
	R.Mckelvie	ICT to attend team briefs, undertake as an action once for all team briefs	August 2016
	R.Mckelvie	Assess the impacts from team briefs via surveymonkey to analysis findings	September 2016
	R.Mckelvie	Mystery Shopping exercise with website checks by staff.	March 2017
Next Generation Threat Control	R.Mckelvie	Establish quotes for product	March 2016
	R.Mckelvie	Purchase and deploy	April 2016
	R.Mckelvie	Publicise this via the Vine & Directorate communications	April 2016

APPENDIX 2

Baseline network/ check for changes to files/ configuration.	M.Don	Re-deploy existing software to detect file / network changes	April 2016
	R.Mckelvie	Prioritise backups, the way which areas are selected first based on the Business Continuity Plan.	May 2016
Block certain high risk sites.	R.Mckelvie	Web filtering software in place, review and implement	April 2016
Review ICT Strategy / Plan	R.Mckelvie	Make sure virus controls are highlighted as high risks, ensure capacity within department is set at the appropriate level to reach maintain set standards	May 2016
CERT liaison, to implement best practice advice	R.Mckelvie	Implement any actions through network groups, lean on partners for advice where possible.	March 2017
Server consolidation excise	R.Mckelvie	Continue to reduce the amount of servers to eliminate virus, storage, backup constraints	March 2017