


Appendix A – Corporate Risks and Opportunities with changed assessments



Risk Code	TR59.006	Risk Title	Shared Procurement Opportunity
Risk Owner	Vaughan Watson	Updated By	Chloe Hipwood
Year Identified	2014	Corporate Priority	Responsive and Efficient
Risk Description	<p>There is an opportunity to share the procurement of the waste and street cleansing contract with East Herts District Council. As a result of:</p> <ul style="list-style-type: none"> - A lack of staff resources to support the project - A lack of ability to influence the design, delivery and performance of services in the future - Including too many options in the ITT - Lack of interest in the market for a NHDC only contract - Lack of interest in the market for a joint contract - The large number of options and optional services being sought from bidders to accommodate each councils requirements <p>There is a risk that:</p> <ul style="list-style-type: none"> - The future contract is not suitable for the needs of NHDC - There will be slight modifications to the service delivered to residents - One or both parties decide not to continue with a joint procurement, impacting on the timescale for the procurement - The Business Case benefits are not realised - There are very few tenders received for the contract 		
Opportunities	<ul style="list-style-type: none"> - Improving the cost effectiveness and resilience of the waste collection and street cleansing contract 		
Consequences	<p>If the risks materialise, the consequences might be:</p> <ul style="list-style-type: none"> - Loss of ability to make savings through a joint procurement - Continuing capacity problems at current transfer locations - Contract costs increase - Lack of satisfaction with the service from residents leading to an increase in complaints - Deterioration in the level of recycling and an increase in the use of landfill - Deterioration in the levels of street cleanliness and increased public complaints 		
Work Completed	<ul style="list-style-type: none"> - December 2014 Cabinet approved the development of a Business Case - Current contract extended to 8 May 2018 to align with EHDC contract - Cabinet approved Strategic Outline Case - Consultant employed to support the project - Outline Business Case approved by Cabinet in July 2016 - Full contract scope and financial implications determined - AFM funds used to fund the costs involved in joint procurement - Governance arrangements for contract agreed - Interim Inter-Authority Agreement in place to protect both authorities from financial liabilities and risks in the event of one partner unilaterally ending the partnership prior to procurement - Workshops held with Members to ensure a better understanding of jointly agreed policies 		
Ongoing Work	<ul style="list-style-type: none"> - Agree composition of a management board and determine Member involvement - Determine future contract management staffing arrangements - Determine joint policies - Develop contract documentation - Develop contract specification - Partnership working with EHDC - To determine if contract monitoring role will be client led - To finalise arrangements for the Customer Service Centre for the contract 		

	<ul style="list-style-type: none"> - Consider potential TUPE issues from combining two sets of staff on different terms and conditions - Following tender evaluation and financial review, to consider if the authorities' or the contractor are to cover the capital costs of investment in vehicles etc. 		
Current Impact Score	3	Current Likelihood Score	2
Current Risk Matrix			
Date Reviewed	09-Feb-2017	Next Review Date	01-Jun-2017
	FINANCIAL		
	OPERATIONAL		
	PEOPLE		
	REPUTATION		
	STRATEGIC		

Risk Code	TR62	Risk Title	Cyber Risks
Risk Owner	Howard Crompton	Updated By	Vic Godfrey
Year Identified	2014	Corporate Priority	Responsive and Efficient
Risk Description	<p>As a result of:</p> <ul style="list-style-type: none"> - Computer virus - Malware - Ransomware - Computer hacking - Action by Staff/member (e.g. opening a malicious link) - Malicious tampering of computer records - Information being sent to the wrong recipient - Loss or damage to server room particularly during DCO refurbishment - Failure by members to register with ICO <p>There is a risk of:</p> <ul style="list-style-type: none"> - Systems being interrupted or damaged - Data being corrupted or erased - Personal data being stolen - Breach of the Data Protection Act 		
Opportunities	<ul style="list-style-type: none"> - Safe and effective use of Information Technology 		
Consequences	<p>The consequences of these risks include:</p> <ul style="list-style-type: none"> - Loss of reputation - Ability to provide services is disrupted - Revenue streams are reduced - Additional costs to investigate and test following repair/restoration - Claims for compensation if a third party suffers a financial loss - Fines from the Information Commissioner 		
Work Completed	<ul style="list-style-type: none"> - Annual penetration test carried out in line with Cabinet Office (PSN) requirements in July 2016 and all systems passed - Annual PSN accreditation completed and awarded in October 2016 - Information Security policy in place, which applies to staff and Members use of IT systems - Email encryption software (EGress) implemented - Introduced new software (Clearswift and Bloggs) to enhance the checking of threats attempting to attack via the firewall - All data centres have fire suppressing systems and are located in secure areas - Disaster recovery in place at a remote site (Unit 3) - Basic computer insurance provides limited cover for damage to equipment and reinstatement of data (although it does not cover payment of any fines or compensation to third parties) - Business Continuity Plans in place - Ransomware attack resulting in the write-off of IT hardware and infrastructure identified as a financial risk for 2017/18 - Data Protection/FOI SIAS internal audit - Controls in place to ensure any third party providers adhere to NHDC security requirements 		
Ongoing Work	<ul style="list-style-type: none"> - Anti-virus/malware software in place and automatic updates are performed to servers and all PCs/laptops/tablets - Email Filter monitoring - Web Filter monitoring - Firewalls continually reviewed and updated - Microsoft patches kept up to date - Annual PEN Test and PSN Accreditation scheduled for 2017 - Regular advice and reminders issued to users - LMS training available (e.g. annual DPA training) - Control/security systems enable potential threats to be identified, investigated and managed accordingly 		

	<ul style="list-style-type: none"> - Review findings of penetration test and work through potential improvements (e.g. changing password requirements) - A quarterly reminder to all staff and Members is sent by the Head of Revenues Benefits & IT about the need to be vigilant about opening emails from unknown sources. 		
Current Impact Score	3	Current Likelihood Score	2
Current Risk Matrix			
Date Reviewed	16-Feb-2017	Next Review Date	30-Sep-2017
	FINANCIAL		
	INFORMATION		
	OPERATIONAL		
	PEOPLE		
	REGULATORY		
	REPUTATION		