APPENDIX 1 –Amber (Moderate Assurance) Audit Review Outcomes

Audit: Corporate Wide - Payment Card Industry Data Security Standards Review - (3 Amber and 2 Green priority recommendations)
Audit Scope and Background: A number of City of London (CoL) departments accept manual payments using handheld credit and debit card payment devices. The review performed an assurance function on the level of Payment Card Industry Data Security Standards (PCIDSS) compliance for these payments. At present the City of London processes approximately 19,000 payment device transactions per annum to a value of approximately three million pounds. The PCI council expects all merchants (CoL is regarded as a merchant) to be compliant and it provides pre-defined Self-Assessment Questionnaires (SAQ) to assist in validating compliance. Failure to comply to PCIDSS can result in significant penalties of up to tens of thousand pounds, along with substantial reputational damage if personal financial information is not secure due to inadequate safeguards being in place.
Audit Findings: The areas reviewed within the PCIDSS comprise of the Network Configuration, Card Holder Data Protection, Vulnerability Management Program, Access Control Measures, System Monitoring and Testing and the Information Security Policy. Many of these areas already have some standards in place as part of normal industry practice. The level of compliance was assessed from a selection of criteria against each main PCIDSS area. All departments except the Police and Institutional departments were sent brief questionnaires and of these, the following five departments confirmed using payment devices; Built Environment; Community & Children's Services; Culture, Heritage & Libraries; Markets & Consumer Protection; and Open Spaces. The findings from these 5 departments form the basis of the report. A moderate level of compliance exists, however, some weaknesses are present and a full PCIDSS assessment exercise is recommended to expose and manage all vulnerabilities. The amber recommendations arose from lack of a PCIDSS policy and the associated procedures and processes. When the Payment Card Industry standards were first introduced they were not as extensive as they are today thus previously an official policy was not required at the City of London. It was agreed to put these in place by the end of November 2014 which has been achieved.

A great degree of cross-departmental co-operation is required to perform and complete a PCIDSS assessment and therefore the recommendations are expected to take some time, especially during the first time of assessment. PCIDSS compliance must be an annual exercise. A full PCI compliance exercise will be designed by the end of December 2014, with assessments undertaken across all Departments by the end of March 2015. Management have confirmed that they have implemented corrections to known vulnerabilities at the earliest opportunity.
Management Response: Urgent action has been taken to address higher priority non-compliant areas, all recommendations from this review are agreed to be implemented by the end of April 2015.

Audit: Chamberlains Department – Assisted Purchasing – (3 Amber and 5 Green priority recommendations)

Audit Scope and Background: The purpose of the audit was to obtain reasonable assurance that an effective control environment is in place to enable City Procurement's 'Assisted Purchasing' service to deliver value for money. This service was formerly delivered by the Transactional Buying team; responsibility for the service now falls to the Procurement Operations Team under the new City Procurement structure.

Audit Findings: The audit was unable to provide assurance that all members of the Transactional Buying Team have the required skills, qualifications and experience to deliver an effective Assisted Purchasing service. It is anticipated that these issues should be resolved by the recent City Procurement restructure, which looks to ensure that Transactional Buying staff have greater 'category focus' by aligning all roles to specific procurement categories. Despite significant investment of time in providing training and opportunities to develop staff skillsets, a number of staff did not meet the required standard.

The service delivery framework currently in place is adequately designed to enable the Assisted Purchasing Service to deliver value for money. The audit identified some areas where the control environment could be enhanced, those that relate to amber recommendations are as follows;

- Through regularly analysing spend of purchases dealt with by the service. Such analysis may help identify where the City may benefit from having a corporate contract in place in the future.
- Through improved monitoring and escalation of non-compliance on retrospective purchase orders; retrospective purchase orders effectively erode the contribution that the service can make to procurement decision making.

City Procurement has devised a set of performance metrics as a means of measuring, assessing and improving team performance in delivering the Assisted Purchasing Service. A review of the July 2014 City Procurement Service Performance Report, identified a number of areas in the presentation of performance metrics and corresponding targets where improvements could be made so that these provide a more effective means of measuring, assessing and improving performance. An amber recommendation has been agreed accordingly.

There are satisfactory arrangements in place for monitoring 'customer' satisfaction with the Assisted Purchasing Service.

Management Response: All recommendations were agreed by management and are due to be implemented by May 2015.