Appendix 1 – Details of Red and Amber Assurance Internal Audit Reviews:

These include reviews where an overall red or amber assurance opinion has been provided and management responses have been received and therefore the report is considered to be finalised, however the list excludes 'spot check' reviews.

Both the police reviews have been reported to the Police Performance and Resource Management Sub Committee in March 2015.

Audit Title: **City Police – IT PBX Resilience (Red Assurance)** Recommendations: Red – 3 Amber – 1
Audit Scope and Background: A PBX is often referred to as the switchboard, although its complexity and functions go beyond this. The PBX is a multi-user, multi-application, fault tolerant and real time computer being a private telephone network used within an enterprise for users to share a certain number of outside lines. The audit objectives were concerned with PBX fraud, which received a green assurance opinion, but during the course of the review a serious issue emerged regarding the PBX resilience. As such a second report was produced relating to PBX resilience.
Audit Findings: There is only one member of staff responsible for this area and while audit have been informed there is documentation to assist when that member of staff is not present this represents a 'single point of failure'. In addition, there is no 'out of hours' support covering the Force's personnel and that of third party support/maintenance provider. Further, there is no remote access facility at any time regarding both staff and third parties. These issues are known to the IT team and this has been the accepted position for many years. This could leave the Force in an exposed position (e.g. unable to take public telephone calls) should the PBX system fail. It is understood there are contingency measures including the Metropolitan Police facility at Croydon via Computer Aided Dispatch (CAD) messages, however, it is not believed this position has been formally considered and signed off at the highest level. These issues have been discussed with the Force and an Agilysis representative and it is hoped an appropriate resilience level can be achieved. It needs to be recognised, however, that the overall City Police/AgilIsys transition is planned over at least a six months period. The urgency of the situation needs to be determined and prioritised within that planned transition. Risk: The Force may be unable to take calls and deal with emergencies.
Management Response: All recommendations were agreed to be implemented by December 2015. At the signing of the change control to extend the managed service in December 2014 this position significantly improved, with the Police able to access the broader support resources available from Agilisys. There are, however, resources gaps to be filled and this situation will continue to improve as we implement the (Information Technology Infrastructure Library (ITIL) and Infrastructure as a Service (IAAS) projects during 2015.

Audit Title: **City Police – IT Disaster Recovery (Red Assurance)**

Recommendations:
Red - 1

Audit Scope and Background:

For clarity the definition of BCMS within this review is taken from the Business Continuity Management System (BCMS) international standard (ISO 22301) which reads 'being part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity'. The management system includes organisational structure, polices, planning activities, responsibilities, procedures and resources.

It was agreed that two reports would be produced one for overall BCMS and a specific review of the IT Disaster Recovery Plan, this report is concerned with the latter. The BCMS review received a green assurance opinion.

The IT Disaster Recovery Plan was to be benchmarked against several criteria including ISO 22301.

Audit Findings:

Planned audit work was limited due to the lack of available Force staff resource to provide information, documentation and answer questions. Discussions with the Force Chief Information Officer (CIO) have confirmed that limited formal DR procedures or facilities are in place.

This report therefore offers conclusions based on the limited information available. These would indicate that there are absences or significant deficiencies across the 8 objectives of this review.

The Force does have a number of solid structures, processes and procedures regarding their BCMS which accord generally with ISO 22301, ACPO and other requirements. However, with regard to ICT DR limited evidence was available to assess the position and what evidence was gathered was not reassuring.

Risk:
The Force may not be operational in the event of a disaster as officers and staff are unaware of what the recovery process should be.

Management Response:

The findings of this report and the need to urgently improve the position are agreed. Work has been underway during 2014 to implement a managed service for the Police which will address these deficiencies.

The Police transition process started on the 1st of Dec and will be complete by December 2015. Incremental improvements will occur throughout this project and will be reported to the Police Governance structure

Consequently, an interim follow up review has been requested for July 2015 to independently assess and report on the progress made.

Audit Title: **Market and Consumer Protection - Trading Standards (Amber Assurance)**

Recommendations:
Amber – 2
Green – 5

Audit Scope and Background:

The City of London Corporation (CoL) has a statutory duty to enforce a wide range of regulations that ensure a fair and safe trading environment. Trading Standards are responsible for enforcing and advising business and consumers regarding legislation relating to trading practices. The team investigates scams and fraud in conjunction with the Tri-Regional Scambusters Team, which is funded by the National Trading Standards Board.

The review sought to evaluate the arrangements in place to ensure that the City of London fulfils its statutory responsibilities regarding Trading Standards, ensuring a fair and safe trading environment for consumers and business alike.

Audit Findings:

A number of opportunities were identified to improve control in respect of complaint and case management, some of which surround the system used by the team. Full audit testing of complaints management could not be performed due to missing information and poor quality management information generated from the Northgate M3 system, which partly results from issues with automatic notifications from the Citizens Advice Bureau. Management also conceded that there are occasionally 'glitches' in report generation whereby records appear incomplete. In addition, we noted that some system functions which might be of value (e.g. time recording) had not been enabled. We understand that the use of additional software (Crimson Investigation Management) is being considered to further facilitate case management.

Performance monitoring arrangements are not adequate at present. There is currently a single KPI for the service which, whilst it relates to critical work, could be more accurately described as an objective for which delivery is not entirely within the team's control. We understand that management have consulted with regulators and local authorities in order to determine meaningful performance indicators focused on outcomes rather than outputs but that nothing suitable has been identified. Whilst we acknowledge the rationale behind an outcome-based approach, the importance of outputs should not be ignored; target setting, monitoring and measuring of team activities are essential as they enable the service to demonstrate that resources are being used in an appropriate and efficient manner. We note that the Corporate Performance and Development Team has agreed to provide support to Trading Standards to assist in developing performance measures for 2015/16.

High level regulation of Trading Standards is facilitated via the Port Health and Public Protection Enforcement Policy and we found this to be generally compliant with the key content of the Regulators Code. However, policies and procedures in respect of day to day complaint management activities were not evident. We are informed that some progress has been made in this regard following the completion of the audit.

Audit testing of enforcement action cases concluded that work is being undertaken in compliance with the Enforcement Policy.

Risk:

Performance cannot be adequately monitored to ensure that resources are being used effectively.

Management Response:

All recommendations were agreed, with the delivery of training to address many of the areas of weakness, including one amber recommendation. The second amber recommendation is being addressed by reviewing and adopting best practice key performance indicators.