Audit and Assurance Committee

Date: **8 October 2014**

Item 13: **Cyber Security**

This paper will be considered in public

1 Summary

1.1 This paper provides an update regarding data security, the allocation and tracking of IT equipment and virus definition updates.

2 A paper is included on Part 2 of the agenda which contains exempt supplemental information and documentation. Subject to the decision of the Committee, this paper is exempt and is therefore not for publication to the public or press by virtue of paragraph 7 of Schedule 12A of the Local Government Act 1972 in that it contains information relating to action which might be taken in relation to preventions, investigation or prosecution of a crime.

3 Recommendation

2.1 **The Committee note the paper.**

4 Background

4.1 This is an update on the discussion of TfL’s strategic risks and proposed mitigations as of Q4 2013/14.

4.2 A report on cyber security was requested by Members at its meeting of 8 June 2014, to include data security, the allocation and tracking of IT equipment and virus definition updates.

5 Scope

5.1 Cyber security and Information assurance is an increasingly growing challenge. Information Management (IM) introduced the role of Chief Information Security Officer (CISO) as a direct result of this changing environment to lead the effort to assess maturity in this space. The following actions were taken:

(a) an information security controls framework (ISCF) was created to assess maturity;

(b) the processes in IM were assessed against the ISCF;

(c) processes were scored against the Active Risk Manager (ARM);

(d) the ISCF considered IT inventory and tracking, data security and AV/Malware, and the results (contained in Part 2) to the Leadership Team; and

(e) following the meeting with Leadership Team:

(i) Meeting with TfL Managing Directors, and documented their near term cyber security concerns;

(ii) Created a cyber task force to address their near term concerns; and

(iii) Committed that, that on completion of (ii) above, will create a proposal for extending the gap analysis across TfL.

6 Management of Cyber Security and Information Assurance issues

6.1 TfL's risks in the area of cyber security and information assurance are aligned with guidance from the government and the management of said risks is a strategic level risk.

6.2 The ISCF maps to the controls in HMG Security Policy Framework (SPF), SANS 20, as well as unique TfL requirements. The SPF published by HMG in 2009, and last updated November 2013, requires a "holistic" approach to security policy management.

6.3 The HMG SPF applies to Critical National Infrastructure (CNI) transport assets as identified by government. The SANS 20 has been endorsed by Centre for the Protection of the National Infrastructure (CPNI) and Communication Electronics Security Group (CESG).

6.4 The Information Security Controls Framework contains 29 controls. The ISCF has been reviewed by Gartner and CPNI. (Gartner is a recognised global leader in IT research, advising in cyber security). The gap analysis for addressing cyber security risks was completed against the IM risks only. The cyber security proposal will be expanded to include all disciplines in TfL upon completion of the gap analysis across the additional TfL disciplines. The gap analysis will:

(a) utilise the information security controls framework (ISCF) to ensure a repeatable, testable and traceable analysis;

(b) focus on the areas identified by the managing directors; and

(c) be the basis for the on-going cyber security proposal to define TfL risk, identify remediation steps, governance and financial investment.

7 Summary

7.1 The cyber security and information assurance analysis across TfL will set out the risks, governance, remediation and financial investment roadmap.

List of appendices to this paper:

A paper on Part 2 of the agenda contains exempt supplemental information.

List of Background Papers:

None

Contact Officer:	Steve Townsend, Chief Information Officer
Number:	020 30544130
Email:	stevetownsend@tfl.gov.uk