Appendix 1b

MOPAC | MAYOR OF LONDON
OFFICE FOR POLICING AND CRIME

DIRECTORATE OF AUDIT, RISK AND ASSURANCE
Internal Audit Service to the GLA

REVIEW OF DESKTOP MANAGEMENT

Audit Team

David Esling, Head of Audit Assurance, Risk Management | Mayor's Office for Policing and Crime
Steven Snaith, Baker Tilly Business Services Ltd
Kevin Hickman Senior Consultant, Baker Tilly Business Services Ltd

Report Distribution List

David Munn, Head of Information Technology
Jawaid Bhatti, Technology Operations Manager

CONTENTS

EXECUTIVE SUMMARY

1. Background

1.1 This review of the GLA's desktop management control framework was carried out as part of our 2013/14 plan.

1.2 The objective is to ensure an effective framework, following the Desktop Refresh Project, is in place to manage desktop computers, and mitigate the risk of a loss of integrity or unauthorised access to systems and data.

1.3 We are looking to provide assurance that the following key risks are being effectively managed;

- Failure to set and comply with agreed policies and procedures relating to the recording and disposal of desktop assets may result in loss or misappropriation of assets, inaccurate IT asset valuation and possible breaches of data security legislative requirements.
- Job roles do not provide the appropriate segregation for the use of privilege accounts, resulting in compromised systems activity.
- A lack of adequate data cleansing controls, resulting in a loss of data confidentiality with regard desktop computers equipment that are sent for repair or disposal.
- Failure to define and operate effective software patching controls, increasing the risk of vulnerabilities that can be exploited to gain unauthorised access to systems and data.
- Inadequate security control framework for desktop computers, increasing the risk of a loss to data security, confidentiality, integrity and availability.
- The activity of local privileged accounts is not managed, captured and monitored, increasing the risk that unauthorised activity will not be detected on a timely basis, resulting in systems loss.

1.4 The GLA's desktop management services for GLA staff, and for MOPAC staff using GLA PCs based at City Hall, Southwark are provided by the GLA's Technology Group. The GLA's desktop machines are run on a Windows 7 operating system platform, with office administration services provided via Microsoft Office's 2010 software. Both systems were rolled out to GLA desktop users during 2012.

2. Audit Assurance

Substantial Assurance

There is a sound framework of control operating effectively to mitigate key risks, which is contributing to the achievement of business objectives.

3. Areas of Effective Control

3.1 There are a range of clearly defined policies and procedures which include guidance on the secure use and management of desktop machines that have been produced and

made available to Technology Group (TG) staff and non-technical staff via the intranet and within shared network folders.

3.2 There are effective desktop asset management processes and documented procedures, that ensure an adequate audit trail for desktop machine roll out. These cover the lifecycle of an asset through to its decommissioning and disposal.

3.3 The GLA's Information Security Policy clearly sets out that 'Ironkey' memory sticks are used to ensure security. These are only obtainable from and issued by the TG and are configured with robust encryption so that if the maximum number of unsuccessful logins to the device is reached, all data on them is destroyed.

3.4 Desktop machines are set to 'lock out' if inactive for 10 minutes or more to reduce access by unauthorised individuals. Audit logging is in place and has been enabled desktops to reduce unauthorised activity and provide an effective process for monitoring access.

3.5 Group Policies have been configured on desktops across the GLA network which prevents the installation of software on the machines by users unless they log on with authorised Administration rights. This ensures that unapproved software is not downloaded onto desktop machines that may lead to attacks by viruses or other malware leading to threats to data security, confidentiality and availability.

3.6 Local administration rights have not been removed for desktop machines as the Local Administration facilities need to be available to technicians to enable them to carry out fixes to the machines when local system problems occur. Access to Local Admin accounts is, therefore, adequately controlled by the use of:

- Membership of the Local Admin Group. authorised by the GLA Change Board
- Complex passwords issued to authorised Group Members

3.7 Appropriate automated build scripts have been configured for GLA's desktop machines in TG's Microsoft SCCM (System Centre Configuration Manager) software deployment tool, based on standard, approved images.

3.8 The GLA has developed documented software patching procedures for desktop machines and made them available to appropriate TG staff via network folders and the intranet to help prevent failure or delay in the patching process that may lead to vulnerabilities that could be exploited to gain unauthorised access to systems and data.

3.9 The activity of local privileged user accounts such as system administration accounts is logged, and reported to the TG Live team, who monitor such activity on a daily basis as one of the tasks on the Morning checklist.

4. Key Risk Issues for Management Action

4.1 In relation to the review objectives set out in the scope of this audit, we did not identify any areas for management attention.

5. Review Objectives

5.1 We reviewed the effectiveness of the control framework in place designed to ensure that workstations (excluding laptops) are properly managed. In particular, we were looking to provide assurance that:

- Up to date and properly approved information governance and security policies and procedures are available to staff that define controls to manage risks regarding desktop use, management, data cleansing or data disposal.
- Effective desktop asset management processes have been developed and implemented that cover the lifecycle of an asset through to decommissioning and disposal, including IT PO's, asset registers, ID tagging, physical audits and disposal processes.
- Adequate technical and procedural security controls have been implemented to support the confidentiality and validity of desktop processing.

6 . Scope of Review

6.1 The review included an assessment of controls designed to ensure the design, use and management of desktop computers, including asset management, prevention of data loss and management of vulnerabilities. In particular, we considered desktop management policies and procedures, operational asset management controls and security controls focusing on endpoint security controls over removable media (USB control), screen savers/machine lockout controls, controls to prevent unauthorised software installation, restriction of local administration rights for desktops, desktop image build, desktop patch management and desktop audit logging controls.

6.2 As well as their desktops which connect to the GLA network, MOPAC staff based at City Hall have a separate set of terminals which connect directly to the Metropolitan Police Service (MPS) network over a dedicated leased BT line. Management of latter machines is the responsibility of the MPS IT department and was excluded from this review.

7. Information Governance and Security Policies and Procedures

7.1 We found that a range of clearly defined policies and procedures, that include guidance on the secure use and management of desktop machines, has been produced and made available to Technology Group (TG) staff and non-technical staff via the intranet and within shared network folders. These include the Technology Group's Security Policies and general IT Policies and Procedures and the corporate Information Security Policy and Records Management Policy.

7.2 The TG's Security Policies, to prevent the loss to desktop based systems and data confidentiality, integrity and availability, were found to be clearly defined and covered a number of issues relating to the security of the desktop control environment, including:

- Policy on the disposal of equipment.
- Local Administrator Accounts for PCs
- Process for authorising information processing - access to systems policy
- Cryptographic control policy
- Procedures on Information leakage

- Guidance on the use of Authentication
- Procedure for Incident Management
- Reporting security concerns
- Collection and Preservation of Evidence

8. Operational Asset Management Control over Desktops

8.1 We found that adequate desktop asset management processes and documented procedures are clearly defined and implemented by the GLA to cover the lifecycle of an asset through to decommissioning and disposal. These include:

- How to Asset (Manage) GLA ICT Equipment
- Delivery and Deployment of New Equipment
- Movement of equipment.
- Equipment recycling procedure

8.2 We reviewed the disposal records of a sample batch of computer equipment disposed of in July 2013 and confirmed that:

- The identity of the items disposed of, including desktop machines, had been recorded on the TG's configuration management database.
- The disposal service providers had provided the TG with a detailed list of the items disposed of for reconciliation with the Group's own asset management records. We reperformed the reconciliation of the desktops and agreed the two sets of records.
- The disposal service providers certified that the hard drives of all items listed on the copy of their disposal records had been wiped securely.

9. Technical and Procedural Controls

Endpoint Security over Removable Media (USB)

9.1 Staff who request memory devices to enable them to extract data via GLA desktops are required under the GLA's: Information Security policy to use the organisation's approved 'Ironkey' memory devices, which are obtainable from and issued by the TG. These devices have been configured with strong encryption and if the maximum number of unsuccessful logins to the device (10) is reached, all data on it is destroyed this ensures that confidential or sensitive data being extracted from GLA networked systems via a desktop port is not accessed/misused by unauthorised persons.

9.2 We obtained one of the TG's Ironkey devices issued to GLA staff and confirmed that it was encrypted to government standards (AES 256 K) and required that any data downloaded onto it is automatically encrypted and would require the use of a valid user id and password to allow decryption.

Screen Savers/machine Lockout Controls

9.3 Desktop machines are set to lock out, if inactive for 10 minutes or more to prevent individuals who may be present within GLA premises gaining unauthorised access to

GLA and MOPAC systems and data, which could lead to breaches of security and confidentiality and system misuse.

9.4 We observed online and obtained the Windows Group Policy setting covering network desktop machines at the GLA and found that they had been set in accordance with the Windows Group Policy, to time out and 'lock' after 10 minutes and also required a valid user id and password to unlock them.

Software Installation

9.5 Group Policies have been configured on desktops across the GLA network to prevent the installation of software on the machines by users unless they log on with authorised Administration rights. These policies are clearly documented in the Desktop Upgrade Project Group Policy Design document, which has been made available to all TG staff.

9.6 We viewed the Group Policy online and found that the downloading of software was prohibited on desktop machines by users other than those logging in with Administration rights. We also observed and obtained a screenshot demonstrating that an attempt to download software onto a desktop using a non-Admin user account resulted in failure and an error report on screen.

Restriction of Local Administration Rights

9.7 Local administration rights have not been removed for desktop machines, however, we found that the Technology Operations Manager requires Local Administration facilities need to be available to enable technicians to carry out fixes to the machines if local system problems occur. Access to Local Admin accounts is therefore controlled by the use of:

- Membership of the Local Admin Group, authorised by the GLA Change Board
- Complex passwords issued to authorised Group Members

Desktop Image Build

9.8 To ensure that desktop machines are built consistently and efficiently automated build scripts have been configured for GLA's desktop machines in TG's Microsoft SCCM software deployment tool, based on standard, approved images.

9.9 We obtained an example of an automated build script in use by the TG team and found that this is currently adequately deployed on GLA's desktop machines.

Desktop Patch Management

9.10 The organisation has developed and clearly documented software patching procedures, which include software loaded onto desktop machines. It has made them available to appropriate TG staff via network folders and the intranet. The TG's patching procedures are contained in the AQAP document Microsoft Desktop PC & Laptop Patching, which includes clear guidance on patching methods, authorisation of patch deployment and a checklist for staff to follow to ensure completion of the process. The role of the GLA's Change Management Board in approving patch release is clearly documented in the Change Control process document.

9.11 We reviewed a sample of software patches and found that they had been clearly recorded in the TG's Change log in line with approved patching procedures.

Desktop Audit Logging

9.13 Audit logging is in place and has been enabled on desktops to reduce unauthorised activity on GLA systems and which assist management in tracking and investigating transactions when required.

Activity of Privileged User Accounts

9.14 The activity of local privileged user accounts such as system administration accounts is logged, and reported to the TG Live team, who monitor such activity on a daily basis as one of the tasks on the Morning checklist, reducing the risk that unauthorised activity will not be detected on a timely basis, resulting in significant system or data losses or security/confidentiality breaches.

9.15 We found that the activity of local privileged user accounts such as system administration accounts is logged, and reported to the TG Live team, who monitor such activity on a daily basis as one of the tasks on the Morning checklist.

Overall Rating	Criteria	Impact
Substantial	There is a sound framework of control operating effectively to mitigate key risks, which is contributing to the achievement of business objectives.	There is particularly effective management of key risks contributing to the achievement of business objectives.
Adequate	The control framework is adequate and controls to mitigate key risks are generally operating effectively, although a number of controls need to improve to ensure business objectives are met.	Key risks are being managed effectively, however, a number of controls need to be improved to ensure business objectives are met.
Limited	The control framework is not operating effectively to mitigate key risks. A number of key controls are absent or are not being applied to meet business objectives.	Some improvement is required to address key risks before business objectives can be met.
No Assurance	A control framework is not in place to mitigate key risks. The business area is open to abuse, significant error or loss and/or misappropriation.	Significant improvement is required to address key risks before business objectives can be achieved.

RISK RATINGS

Priority	Categorisation of recommendations according to their level of priority.
1	Critical risk issues for the attention of senior management to address control weakness that could have significant impact upon not only the system, function or process objectives, but also the achievement of the organisation's objectives in relation to: • The efficient and effective use of resources • The safeguarding of assets • The preparation of reliable financial and operational information • Compliance with laws and regulations.
2	Major risk issues for the attention of senior management to address control weaknesses that has or is likely to have a significant impact upon the achievement of key system, function or process objectives. This weakness, whilst high impact for the system, function or process does not have a significant impact on the achievement of the overall organisational objectives.
3	Other recommendations for local management action to address risk and control weakness that has a low impact on the achievement of the key system, function or process objectives ; or this weakness has exposed the system, function or process to a key risk, however the likelihood is this risk occurring is low.
4	Minor matters need to address risk and control weakness that does not impact upon the achievement of key system, function or process or process objectives; however implementation of the recommendation would improve overall control.