Appendix 1c

MOPAC | MAYOR OF LONDON
OFFICE FOR POLICING AND CRIME

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

REVIEW OF INTERNET- BASED NETWORK SECURITY

DISTRIBUTION LIST

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 internet-based network security control framework was carried out as part of our 2013/14 plan.

1.2 The objective is to ensure an effective framework is in place to manage Network Internet based security to support the validity and confidentiality of related access, in particular regarding the transfer of MOPAC network management to City Hall.

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

- The network topology and supporting domain structure and management is not adequately designed, increasing the risk of unauthorised network based access and activity.

- Weaknesses in the arrangements regarding the transfer of MOPAC, HCA and LDA to City Hall adversely impacting the integrity of MPS/GLA staff

1.4 The GLA's primary datacentre and network infrastructure is based at City Hall, in the London Borough of Southwark. It has been in place since 1999, when the GLA was founded, and provides networked information systems for GLA staff, encompassing about 1,000 live networked user accounts access.

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 The GLA's 'corporate' part of its network and that part of the GLA network also supported by the GLA Technology Group (TG) but used by MOPAC staff based, is separated into two logical domains. This approach prevents GLA and MOPAC staff being able to access information which they are not permitted to view or handle.

3.2 The Metropolitan Police Service (MPS) network, which is maintained and supported wholly by the Metropolitan Police's IT department and not by GLA's ICT team, is entirely physically separate from the GLA network, with gateway equipment for the network located in a secure room to which the GLA TG do not have. This ensures that the likelihood of breaches of confidentiality and security regarding, for example, sensitive crime-related personal or police business information are reduced significantly.

3.3 A range of network management and information security policies and procedures has been documented and made available to members of the GLA TG via shared network folders and on the GLA intranet. The existence of documented network

management guidance and its communication to all appropriate TG staff reduces the risk that staff will be unaware of their key network management responsibilities which could adversely impact network operational availability and the confidentiality and integrity of networked business critical systems and data.

3.4 The password and lockout settings in place at the domain level for both the corporate GLA domain and the MOPAC domain have been adequately designed to prevent any successful attempts to access networked systems and data by unauthorised persons.

3.5 The GLA has developed an adequate standard set of user account management procedures which have been made available to the TG via network folders and the intranet. These help to ensure a consistent approach to the management of user accounts at the network level.

3.6 Access by staff to different applications and data on the GLA network is controlled through the use of Group Policies on Windows Active Directory. Staff are assigned to particular Groups in accordance with their job roles and as authorised by their line management under the GLA's account management procedures. These arrangements ensure adequate separation of duties are in place to prevent unauthorised access to and activity regarding networked applications and personal and business data.

3.7 Access to the system administration account at the network level were found to have been restricted to appropriate members of the TG team, reducing the risk that the high level of access privileges associated with such accounts could be misused, resulting in significant breaches of security and confidentiality regarding GLA and MOPAC data.

3.8 A series of clearly documented plans were produced, regularly reviewed and updated regarding the migration of different elements of MOPAC systems and data to the GLA network. A controls-based approach was documented within the plans for the migration of MOPAC systems and data.

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 action.

5. Review Objectives

5.1 We reviewed the effectiveness of the control framework in place designed to ensure the security of the GLA managed network internet service. In particular, we looked to provide assurance that:

- The network topology has been designed and is operated to ensure adequate segregation between GLA and MOPAC network access.
- Adequate network domain management controls are in place and operating effectively to support the confidentiality and integrity of network internet based processing.
- A focused controls-based approach was undertaken regarding the migration of MOPAC to the GLA network to facilitate the effective management of the network going forward.

6. Scope of Review

6.1 The review included an assessment of controls covering the design and operation of the network topology, domain structure, HCA, LDC and MOPAC migration processes, logical access controls, business level separation of duty controls, administrator access and account management procedures.

6.2 As well as their PCs which connect to the GLA network MOPAC teams also have a separate set of terminals within City Hall which connect directly to the Metropolitan Police Service (MPS) network over a WAN link. The latter network is the responsibility of the MPS IT department and was excluded from this review.

7. Network Topology and Supporting Domain Structure

7.1 The GLA network at City Hall is separated into two logical domains: the 'corporate' GLA domain and the MOPAC domain, which are administered separately by GLA technical support staff in the Technology Group.

7.2 The above network and domain configuration helps to ensure that GLA's networked information resources can be managed effectively and securely, including, where appropriate, separating access rights of GLA and MOPAC staff. This reduces the risk that either group of staff will be able to use systems and access information which they are not permitted to view or handle, in line with their operational responsibilities, leading to breaches of security and confidentiality.

7.3 In addition to their GLA-maintained network facilities, MOPAC staff also have a number of terminals located on the 2nd floor of City Hall which connect to the MPS (Metropolitan Police Service) network, which is maintained and supported wholly by the Metropolitan Police's IT department and not by GLA's ICT team. This connection is physically separate from the GLA network and there are no links between the two networks. The MPS terminals used by MOPAC staff are connected by an MPS cabling system to gateway equipment located in a locked cabinet on the 2nd floor, to which the GLA TG do not have access.

7.4 These arrangements reduce the risk of unauthorised network based access to or misuse of Metropolitan Police systems and data, which could lead to breaches of

confidentiality and security regarding, for example, sensitive crime-related personal or police business information.

7.5 We reviewed the network topology and domain structure and confirmed through our testing that the controls in place demonstrated through the network infrastructure diagrams and architecture screens on 2nd floor of City Hall are adequate.

8. Network Domain Management

Policy and Procedures

8.1 A range of network management and information security policies and procedures have been documented and made available to members of the GLA TG through shared network folders and the GLA intranet. These documents include a number which are in the form of Assured Quality Action Procedures (AQAPs) are as follows:

- Live Team Morning (Network) Checks
- Change Control process
- Code of Ethics (relating to IT/network security)
- Information Security (for general users)
- Information Security (Technology Group security policies)
- Data Protection

8.2 The Live Team Morning (network) Checks document in particular provides guidance to technical staff on the daily checks on all key networked IT services to be undertaken ensure they are available and accessible. These include:

- Email servers
- Oracle servers
- Public websites
- Nagios (network monitoring application)
- Telecoms
- Internal websites
- Print servers
- Backups
- Falconstor replication (network storage)

The document clearly sets out how TG staff prioritise items to be checked and procedures for ensuring that issues are recorded in the Track-IT Service Desk tool and raised with the correct technical teams for remedial action to be taken according to the criticality of the systems concerned. It also specifies the requirement for daily reports on the results of the checks, including an overall status report on each items reported on, based on a Green, Yellow and Red notation, where Green is satisfactory, Yellow indicates a problem and Red confirms the complete loss of service. The reports are sent to the TG operations manager and the whole of the ICT Live System group.

8.3 We found that the above documented network procedures and their communication to all appropriate TG staff, are adequate and it enables TG staff to be fully aware of their key network management responsibilities that cover network operational

availability, confidentiality and the integrity of networked business critical systems and data.

8.4 We reviewed copies of a Live Morning checks document and a sample of work orders raised in the Track-IT system in respect of faults detected we were able to confirm in our test that the Morning checks and associated procedures were being complied with.

Logical Access Controls

8.5 Logical access controls for both the GLA corporate network domain and the MOPAC network domain are configured as follows:

- Enforce password history: 6 passwords remembered
- Maximum password age: 90 days
- Minimum password age: 0 days
- Minimum password length:8 characters
- Password must meet complexity requirements: enabled
- Account lockout duration: 4320 minutes
- Account lockout threshold: 5 invalid log attempts
- Reset lockout counter after: 1440 minutes

8.6 The above password and lockout settings in place at the domain level for both the corporate GLA domain and the MOPAC domain have been adequately designed to reduce the risk of successful attempts to access networked systems and data by unauthorised persons through determining and exploiting the access credentials of valid network users.

Account Management Procedures

8.7 The GLA has developed a standard set of user account management procedures which have been made available to TG staff via network folders and the intranet. They include:

- Adding a new user and moving staff at City Hall.
- Leavers Procedure (Staff Departure)
- Dealing with initial and further requests for permissions to GLA's data

As part of the leavers' process, the TG also has a documented procedure whereby the accounts of leavers who have not logged into the GLA network for 3 months are more are identified via a scheduled Windows AD (Active Directory) report, which is run once a month and queried with their line management as to whether they still require access.

8.8 The above processes help to ensure a consistent and efficient approach to the management of user accounts at the network level.

8.9 We reviewed a sample of leavers requests extracted from the Track-IT service desk system and confirmed that the accounts of the users concerned had been removed promptly from the system, as required by the Leaver Procedures. In addition, we

obtained a copy of the 3 month leavers' report for the month of October 2013 (designed to capture leavers who have not logged on to the network for 3 months or more by the end of September). We were able to confirm in a sample of user accounts that they had all been queried by the TG Group with their respective line managers and that according to the responses received, their user accounts had either been removed from AD or there was a valid, documented and approved reason for their existence.

Business Level Separation of Duties

8.10 Group Policies are clearly defined stipulating roles and responsibilities for access to different applications and data on the GLA network and are held on Windows Active Directory. Staff are assigned to particular Groups in accordance with their job roles and as authorised by their line management under the GLA's account management procedures referred to above.

8.11 The above arrangements reduce the risk that an adequate level of separation of duties cannot be implemented across the network. This could lead to staff gaining access to systems and data which are not commensurate with their responsibilities and potentially to misuse of systems and breaches of security and confidentiality regarding personal and business data.

Administrator Access

8.13 Access to the system administration account at the network level has been restricted to appropriate members of the TG team who require it to carry out their job responsibilities. We found that the controls in place, to prevent the misuse or unauthorised access by individuals which could result in significant breaches of security and confidentiality regarding GLA/ MOPAC data, are adequate.

8.14 We reviewed a screenshot of the Domain Admin Properties Members and found that all Members of the Domain Admins Group were members of the Live Service Desk Team as appropriate.

9. Migration of MOPAC System

9.1 A controls-based approach was adopted and documented for the migration of MOPAC systems and data to the GLA network. We found that a series of clearly documented plans had been produced, regularly reviewed and updated for the migration of different elements of MOPAC systems and data to the GLA network. We reviewed the following plans which had been produced:

- MOPAC transition Plan
- MOPAC Blackberry Plan
- MOPAC Changeover Days Plan
- MOPAC Email Move Plan
- MOPAC plans for moving email domain name to City Hall.

9.2 We confirmed through our testing that the planning approach adopted for the migration was in accordance with best practice and adequate controls were in place to ensure the network was secure during the migration.

RISK AND AUDIT ASSURANCE STATEMENT – DEFINITIONS

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.