MAYOR OF LONDON

OFFICE FOR POLICING AND CRIME

Appendix 1c

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

REVIEW OF THE GLA BUSINESS CONTINUITY CONTROL FRAMEWORK

DISTRIBUTION LIST

Audit Team

Prakash Gohil, Audit Manager
Steven Snaith, Associate Director, RSM Tenon
Charlotte Lang, Information Systems Assurance Consultant, RSM Tenon

Report Distribution List

David Munn, Head of Information Technology
David Gallie, Assistant Director of Finance
Jawaid Bhatti, Technology Operations Manager

CONTENTS

Page

EXECUTIVE SUMMARY

FINDINGS AND AGREED ACTIONS

ACTION PLAN

EXECUTIVE SUMMARY

1. Background

1.1 This review of the Business Continuity Control Framework was carried out as part of the 2011/12 internal audit plan.

1.2 The Greater London Authority (GLA) has recently updated business continuity plans to reflect the changes made to its IT Infrastructure. In particular, data backups were originally written to tape and transferred off-site by a third party. Related data recovery took between from one to five days, which was considered too long for the Authority's key services. As part of the decision to share IT services with TfL, a rack was provisioned in the TfL's Data Centre based in Woking.

1.3 The Woking site is used to host a secondary virtualised environment to manage the creation and management of 'snapshots' from the City Hall site. New hardware including a new NexSAN storage Area Network device have been installed to ensure the Woking site is capable of supporting the services normally run at City Hall. The GLA use FalconStor to carry out snapshots and replications of the City Hall environment and store them at Woking. The GLA have also implemented FalconStor RecoverTrac which enables a system to run a script to build the servers and their associated data onto the Woking virtualised environment. As a result of the new solution, the GLA estimates a recovery time following a loss of systems of eight hours.

1.4 In this report we set out our findings and comments on the key controls operated by the GLA to manage the Business Continuity control framework.

2. Audit Assurance

Substantial Assurance

Our overall opinion is that the Business Continuity and IT Disaster Recovery control framework is adequately controlled, with the exception that some minor control measures need improving to further reduce the risk of disruption from internal or external events.

3. Areas of Effective Control

3.1 A business continuity framework for building resilience and the capability for an effective response that safeguards the interests of key stakeholders, reputation and value creating activities is in place, reducing the risk of a loss of primary GLA operations.

3.2 A Systems Recovery Dependency Plan has been documented to outline the recovery sequence of services and estimated recovery times, reducing the risk the recovery process is uncoordinated and does not consider key dependencies of systems which could lead to further disruption to services in a contingency event.

3.3 Clear roles and responsibilities including who invokes the business continuity plan and the Technology Group Business Continuity Plan have been documented, reducing the risk that key individuals are unaware of their role in a disaster situation, leading to an uncoordinated response to incidents that impact the availability of IT and wider business services.

3.4 Distribution lists for the Business Continuity Plan and the Technology Group Business Continuity Plan vhave been included in the respective plans, reducing the risk that planning documentation is not available in a disaster event, leading to an uncoordinated response adversely impacting the organisation.

3.5 Responsibility for the maintenance of the Corporate Business Continuity Plan has been assigned to the London Resilience Manager, required to communicate changes to directorates so their plans can be updated. Changes made to directorate plans are communicated to the London Resilience Manager to ensure the corporate plan is updated appropriately, supporting the validity and currency of related planning arrangements.

3.6 The London Resilience Manager and the Facilities Management Team are responsible for carrying out tests on the Corporate Business Continuity Plan. Assigning responsibility for testing the plan reduces the risk that recovery planning will not be effective in practice.

3.7 Clear links between the Corporate Business Continuity Plan and the Technology Group Business Continuity Plan exists, including guidance on the format of the plans, inclusion of the Technology Operations Manager on the Business Continuity Group and the integration of key stakeholders from other directorates in the provision of the new business continuity solution, to ensure it is in line with the requirements of the business. Overall, there is a reduced risk that GLA’s objectives are not consistently considered when dealing with a disaster, resulting in an ineffective response to incidents and increased disruption to critical business functions.

3.8 A recovery site at Selbie House is available to provide backup facilities and limited office accommodation, and a server rack has been provisioned at the TfL data centre in Woking, reducing the risk that the GLA will not be able to adequately restore IT services in a timely manner to support business operations should City Hall become unavailable.

3.9 Two 10 GB links and two 1 GB internet links from City Hall to the Woking site have been installed to build redundancy into the network and reduce the risk that key aspects of the network become unavailable due to hardware failure.

3.10 The GLA has incorporated virtualisation within the network infrastructure and has enabled DRS, High Availability and VMotion solutions to allow services to load balance over 7 physical hosts at City Hall and to automatically move virtual machines to another host should one become unavailable, reducing the risk of key corporate systems not being available due to server hardware failure.

3.11 The Storage Area Network (SAN) located at Woking has the capacity to support the volume of data stored on the four SANs located at City Hall and has been configured to replicate changes to data detected on the City Hall SAN, supporting the continuity of operations in the event of failure at the primary location.

3.12 Data replication from City Hall to Woking has been implemented using the FalconStor Management Console, reducing the risk that key data is not available in the event of a disaster, leading to further disruption to services and prolonged recovery times.

3.13 Snapshots of data are taken at least twice daily depending on the system and held at the Woking site; supporting the continuity and availability of business critical information. A backup up process using snapshot technology to backup systems and data and store it at Woking, and carrying out backups to tape for legacy systems has been designed and documented, reducing the risk that critical data will not be available to support the continuity of GLA operations.

3.14 The requirement to carry out regular testing of the Technology Groups Business Continuity Plan has been determined reducing the risk the BCP plan is not fit for purpose and unworkable in a contingency event.

4. Key Risk Issues for Management Action

4.1 The Corporate Business Continuity Plan and the Technology Business Continuity Plan does not fully reflect current business operations. Out-dated information regarding business impact assessment and recovery times are included within the plans, increasing the risk that related recovery responses will not be effective in practice. The Technology Group Business Continuity Plan states that the Business Impact Assessment should be “quickly reviewed” when the business continuity plans have been invoked to ensure they are still current. However, this is not practical in practice and related planning needs to be amended.

5. Review Objectives

5.1 We reviewed the adequacy of control measures in place for mitigating the risks relating to the business continuity of GLA IT services. We sought to provide assurance that there is an effective corporate documented business continuity management framework in place and an adequate IT disaster recovery control environment has been designed and tested.

6 Scope of Review

6.1 The review covered the effectiveness of the procedures and controls established by the GLA to support business continuity. This included reviewing plans, roles and responsibilities, back up facilities, off-site recovery and GLA testing of the effectiveness of plans and arrangements as defined in the terms of reference for the review.

7. Business Impact Analysis

7.1 The Technology Group Business Continuity Plan, dated June 2012, identifies the requirement to carry out a business impact assessment to identify priorities within each directorate to determine areas essential for the continuity of the organisation. The Business Impact Assessment is divided into three categories:

- Mission Critical Functions, Process and Projects
- Critical Posts and Staff
- Mission Critical Equipment, including software, documents and records

However, the process documented in the plan does not fully reflect the revised technology platform. With regards to the new solution, the process results that once the infrastructure has been restored in a contingency event, then all servers can be brought back at the same time. This is not reflected in the plan.

7.2 In addition, the Technology Group Business Continuity Plan documents that the Business Impact Assessment should be "quickly reviewed" when the business continuity plans have been invoked to ensure they the priority of systems still reflects current requirements.

Risk
The documented Business Continuity Plans do not reflect the current situation leading to an uncoordinated response in a contingency event.

Recommendation
A formal process for carrying out periodic Business Impact Assessments should be defined and necessary adjustments made to the Business Continuity Plan with regard to the new technology solution.

7.3 An Excel spread-sheet documents the Critical Business Functions identified within different areas of the business, including the Mayor's Office, the Assembly and Secretariat, Chief Executive, Corporate Services, Finance and Performance, Media & Marketing, and Policy and Partnerships. A rating has been allocated to each service based on the damage/impact regarding each area. The exercise was carried out before the implementation of the new solution and included other directorates. However, not all services are restored in a contingency event. We were informed that the services accessible when accessing the network remotely will be restored instead of all services.

We reviewed the list of software provided on the remote access desktop; the document includes standard and non-standard software to be installed on remote desktops in line with continuity priorities.

8. Prioritisation of Tasks

8.1 The Technology Group Business Continuity Plan documents the requirement to conduct a business impact assessment quarterly to identify critical systems within GLA. The assessment identifies which systems are considered to belong to category 1 whose loss could cause a major impact to the GLA within 24 hours of outage, and category 2 whose loss could have a major impact after 24 hours.

8.2 The business impact assessment assigned seventeen systems to restore category 1 (Infrastructure Systems) and nine systems to restore category 2 (business systems).

8.3 Work has been on-going to fine tune the system following implementation of the new solution, including the recent virtualisation of Active Directory. As a result, a new set of improved system recovery times has been produced and presented to the GLA Business Continuity Board and now appear in the latest version of the plan.

9. Business Continuity Plan

9.1 The Corporate Business Continuity Plan dated June 2012 is in the form of two editions. Edition 1 contains personal contact details and is distributed to the members of the Emergency Management Team (EMT). Edition 2 does not contain personal contact details and distribution is limited to Assistant Directors, Heads of Units and their nominated business continuity deputies. The plan details three possible scenarios which could result in the invocation of the Plan and the responsibilities of teams and individuals involved in responding to an incident. The Plan was found to be adequate and reduce the risk plans may not be effective in the event of a business disruption, which could lead to a delay in returning the GLA to business as usual.

9.2 The Technology Group Business Continuity Plan dated June 2012 documents roles and responsibilities of the Strategic Response Team and the Operational Response Team, and contains comprehensive and detailed procedures. We found the scope and coverage of the business continuity plan to be adequate and reduce the risk continuity planning is insufficient to support wider business continuity requirements, resulting in a loss to business operations.

10. Roles and Responsibilities

10.1 The GLA utilises the emergency services Bronze, Silver, Gold structure for incidents. For incidents that affect City Hall, Bronze, Silver and Gold will be provided by the Facilities Management Team who will manage the emergency phase of the incident. The Facilities Management Team will be responsible for finding longer term accommodation should an incident occur that results in City Hall being unavailable for extended periods of time.

10.2 The Business Continuity Plan assigns responsibility to the Directors to ensure that their directorates have their own appropriate Business Continuity Plans (BCPs). The Technology Group Operations Manager has been assigned responsibility for the

Technology Group Business Continuity Plan and the Senior Systems Engineer is the Business Continuity Deputy. These responsibilities have been documented in their job descriptions.

10.3 Once the Emergency Management Team (EMT) has declared a major incident, the Strategic Recovery Team (SRT) has a remit to initiate and maintain control of the Technology Group Major Incident Recovery Plan (Technology Group Business Continuity Plan) and to provide resources and direction to the Operational Recovery Team. The roles and responsibilities have been documented in the Technology Group Business Continuity Plan.

10.4 Organisational recovery is designed to be led by the Emergency Management Team (EMT). The EMT is responsible for ensuring the continuity of GLA business operations and for deciding the priorities of the organisation and the allocation of resources. They are primarily responsible for maintaining communication with key stakeholders such as the Mayor, Recovery site, Assembly Members and GLA staff.

10.5 The presence of clearly defined roles and responsibilities in relation to Business Continuity and IT Disaster Recovery reduces the risk that key individuals are unaware of their role in a disaster leading to an uncoordinated response to incidents that impacts the availability of IT and wider business services.

11. GLA Business Continuity Planning Team

11.1 The GLA Business Continuity Planning Team holds overall responsibility for business continuity for the GLA. The Team consists of the following members:

- Head of Facilities Services
- Building Infrastructure Manager
- Head of Paid Services
- Director of Resources
- Director of D and E
- Director of C and I
- Head of Executive Office
- Support Services Manager
- Building Amenities Manager
- Head of Technology Group

11.2 Membership of the group and the role of each individual is documented in the Technology Group Business Continuity Plan, reducing the risk staff on the Incident Team may not be clear on what they are expected to do. In addition, the scope of membership clearly correlates to the principal GLA business functions, providing an adequate scope of critical operations coverage.

12. Distribution of the Plan

12.1 A distribution list for the Technology Group Business Continuity Plan is documented in the Plan. The Plan is distributed to the EMT, SRT and ORT electronically. It is also distributed to the Mayor’s Management Team, directors and managers. A copy of the Technology Group’s Plan is also available on the Technology Group area of the GLA Intranet.

12.2 We also confirmed the presence of the Technology Group Business Continuity Plan on the GLA Intranet page, overall reducing the risk the Plan is not available in a disaster event, leading to an uncoordinated response to a contingency event adversely impacting the organisation.

13. Maintenance of the Plan

13.1 The London Resilience Manager is responsible for maintaining the Corporate Business Continuity Plans and communicating them to relevant staff. Changes made to the corporate plan or decisions made at a senior level are communicated to the directorates with the objective that they can update their plans appropriately.

13.2 The Technology Group Business Continuity Plan states the directorates should review and update their Business Continuity Plans every six months. It is also recommended in the Plan that team meetings are used to discuss and review the Business Continuity Plans within directorates to provide an opportunity for staff to input. Plans need to be approved and signed off by the Head of Unit and Director. The compilation and maintenance of appropriate Business Continuity Plans is a performance measure for the GLA. Directorate plans are required to be formally reviewed as part of the quarterly performance monitoring at the end of quarters 2 and 4 (as documented in the BCP).

13.3 The Technology Group Operations Manager is responsible for maintaining the Technology Group Business Continuity Plan. The Plan contains version control at the front of the document. The last review was May 2012, in order to add changes in relation to servers and to update the risk register. The plan is currently in version 3.2. Changes made to the Technology Group Business Continuity Plan follow the documented Technology Group Change Control Process. The process is dated August 2008 and is version 2.2. A form is required to be completed outlining the main details, impact, external contractors, testing, and preparation for the change. The change is reviewed by the Change Advisory Board (CAB) who approves or rejects the change. The change is implemented and reviewed again by the CAB before it is closed.

13.4 Any changes made by the Technology Group are communicated to all customers affected by the change and an article is included in the weekly newsletter. The Technology Operations Manager also informs the London Resilience Manager of any changes to the Technology Group Business Continuity Plans that need to be reflected in the Corporate Plans.

13.6 We found the overall design of the business continuity plan maintenance framework to be adequate and effective to support the validity and currency of related planning arrangements.

14. Initiation of the Plan

14.1 The Facilities Management (FM) Team is responsible for invoking the business continuity plans in a contingency event. The FM Team includes a 24-hour duty manager system to ensure an incident is identified at the earliest possible stage so the plan can be invoked if necessary. This responsibility has been documented in the Corporate Business Continuity Plan and the Technology Group Business Continuity Plan. The FM Team form part of the Emergency Management Team (EMT) and are responsible for invoking the EMT to ensure the incident can be communicated to directorates to invoke their plans.

14.2 The Technology Group Operations Manager is a member of the EMT and is responsible for invoking the Technology Group Business Continuity Plan, his responsibility is documented in the Technology Group Business Continuity Plan, reducing the risk staff are unaware who to contact to invoke the plan should a disaster occur.

14.3 We found the control framework to invoke a business continuity response to be adequate helping to ensure that the correct level of continuity response is initiated at the right time.

15. Battle Box

15.1 Specialist items that are considered to be critical physical equipment are placed in the Recovery Site “Battle Box”. Requests to store items in the Battle Box are required be made to the Facilities Management Team. The Technology Group hold copies of software, licences and maintenance agreements in black sealed boxes at City Hall and the Recovery Site located at Selbie House. They contain the necessary documentation and procedures to support the establishment of required systems in the event of a critical incident. Keeping Battle Boxes at each site in external stores reduces the risk that essential equipment needed to coordinate an effective disaster recovery response is unavailable.

15.2 In addition, Disaster Recovery packs are provided to all members of the IT Technology Group, containing instructions needed for the recovery procedures. We confirmed the packs contain key documentation in relation to business continuity and disaster recovery and are stored electronically, reducing the risk that critical guidance is unavailable to staff in a contingency event, delaying the recovery of the GLA.

16. Testing of the Plan

16.1 The London Resilience Manager and the Facilities Management Team are responsible for the management of Business Continuity Plan testing. Tests of the plan are required to be carried out on a monthly basis and are documented in the Recovery Site Testing Record. The Recovery Site Testing Record documents the site the test occurred and includes details such as test location (Selbie House, City Hall, the Mayor’s briefing room); the item to be tested, the date tested and the RAG rating.

16.2 We confirmed that testing has been conducted as planned by review of the Recovery Site Testing records and related documentation. We identified that a RAG rating and date had been documented and related tests carried out at. The most recent tests were completed on 01/11/11, 09/12/11, 06/01/12, 10/01/12, 04/02/12, 06/03/12 and 03/04/12. A green rated test of the Mayor’s Briefing room was also carried out on 09/02/12 and an amber rated test carried out 09/03/12.

16.3 Carrying out regular testing of the Business Continuity Plan reduces the risk that related planning will not reflect the current organisation structure and business processes, leading to a recovery response that is not effective in practice.

17. IT DR Links to Business Continuity Plan

17.1 The Corporate Business Continuity Plan documents the responsibility of each directorate to compile and maintain their own Plans. The directorate Business Continuity Plans are required to be based on the corporate template and must “interlock” with the Corporate Plan. The Corporate plan details the areas that each directorate should reference when developing their plans including communications, key staff, mission critical process and working from home.

17.2 Key members of staff from each directorate, including the Technology Group, are included in the Emergency Management Team to ensure the Technology Group are aware of an incident in a timely manner so the Technology Group Business Continuity Plan can be invoked if necessary.

17.3 Key stakeholders and individuals from other directorates were also included in the project to implement the new IT Infrastructure to support a new business continuity solution, reducing the risk that GLA’s objectives are not consistently considered when dealing with a disaster, resulting in an ineffective response to incidents and increased disruption to critical business functions.

18. Alternative Facilities

18.1 A recovery site is available and located at Selbie House near Baker Street. The recovery site is designed to provide back-up ICT services and limited office accommodation. The primary recovery site will be invoked if City Hall is not available. The site is a short term solution and the Facilities Management Team will be responsible for finding alternative accommodation should the incident become long term. The site has 65 workstations and the initial allocation of these is set out in the Corporate Business Continuity Plan.

18.2 The Authority has an agreement with Transport for London (TfL) to provide a server rack in a designated Disaster Recovery datacentre located in Woking. The site allows the GLA to host IT hardware and software available for use as a disaster recovery solution. We reviewed the “Provision of IT Hosting space at TfL datacentre” to confirm it had been signed by the Mayor of London and dated December 2010 to approve the new solution.

18.3 The presence of alternative facilities reduces the risk that the GLA will not be able to adequately restore IT services in a timely manner to support business operations should City Hall become unavailable.

19. Network Resilience – Physical Bandwidth

19.1 City Hall is linked to the Woking disaster recovery site by two dark fibre 10 GB links. The links are used for the replication process. Two internet links are also connected from City Hall to the Woking site, each are 1 GB. These fibre links had been tested to confirm the bandwidth is appropriate for the GLA’s needs. Building redundancy into the physical infrastructure reduces the risk key aspects of the network become unavailable due to hardware failure.

20. Virtualised Storage Framework

20.1 The Authority has two virtualised server farms in place; one is located at the City Hall site and the other is located at the Disaster Recovery site in Woking. The City Hall server farm has 161 virtual machines across 7 physical ESX 4.0 hosts. The physical servers have been divided into two clusters. An external cluster for the GLA's websites contains 2 ESX hosts. An internal cluster for the GLAs servers and data has 5 ESX hosts. DRS and High Availability (HA) have been enabled as well as VMotion to provide added resilience should an ESX host becomes unavailable. We found the design of virtualisation platform to be adequate and based in the GLA's processing requirements, reducing the risk of corporate systems not being available due to server hardware faults.

20.2 The Woking site has 4 ESX hosts separated across two clusters. 2 hosts are within the Internal Cluster and 2 within the External cluster. The virtualised environment at Woking does not currently have any servers created on the hosts. It is a skeleton designed for use in a contingency event. A script configured on the FalconStor console will create the virtualised environment currently in place at City Hall in a contingency event. New 'blade servers' have been installed at the Woking site with greater capacity than the servers at City Hall. This enables the 4 hosts located at the Woking site to have the same capacity as the 7 ESX hosts at City Hall. The initiative to ensure the infrastructure at the Woking site has the same capacity as City Hall and reduces the risk that key services cannot be restored due to insufficient capacity on the disaster recovery site.

20.3 Replication of the virtualised environment is carried out by FalconStor. Recovery of the virtualised environment is managed through the FalconStor console. FalconStor RecoverTrac is based on scripts. A script can be run which takes the data located on the SAN at Woking to create the servers and environment in a contingency event.

20.4 We concluded the overall design of the virtualisation infrastructure, with regards to business continuity capacity and recovery facilitates, was adequate to support the continued critical operations of the GLA.

21. SAN Control Environment

21.1 Four Storage Area Networks (SAN) are located at City Hall and a further SAN located at the Disaster Recovery site in Woking. Any changes to the data at City Hall are detected by FalconStor which informs the FalconStor managing the SAN at Woking that changes have been made that need to be made at Woking. This process ensures the completeness and accuracy of replicated data between each location. As with the virtualised environment, the SAN at Woking has greater capacity and is able to handle the volume amount of data as City Hall's four SANs.

21.2 The design of the SAN environment with regards capacity arrangements was found to be adequate, based on typical data volumes managed and processed by the GLA and also the multiple physical location provision, supporting the continuity of operations in the event of failure at the primary location.

22. Data Replication

22.1 Replication has been configured to carry out “Block level” replication from City Hall to Woking. The FalconStor Management Console has been configured to carry out continuous replication set at “Delta” mode meaning that FalconStor will try and carry out continuous replication but if for some reason this cannot be carried out, then replications will be taken in the form of snapshots at specified time intervals.

22.2 Data replication is an important control with regards GLA managed data and we found that the replication configuration was suitably designed to support the continuity of GLA processed data.

23. Data Snapshot Capacity Planning

23.1 Snapshot data is required to be retained for 90 days. A capacity assessment was carried out to determine the space requirements to hold 90 days of data snapshots.

23.2 The Live Systems Team monitor the capacity as part of the daily checks they are required to carry out. A checklist is maintained to allow individuals within the Team to inform colleagues of the results of checks and any issues identified. Alerts are sent to the Live Systems Team to inform them if services are reaching full capacity so any remedial action can be taken. In addition, a spread-sheet of the IT infrastructure is maintained by the Technology Group and documents the capacity of each service, where it is stored, the capacity, estimated growth, free space and how many days left until full capacity is reached reducing the risk of loss of services or data due in insufficient capacity.

23.3 Capacity planning arrangement with regards server capacities linked to data volumes and thresholds were working efficiently to facilitate the maintenance of GLA processing requirements.

24. Data Backup Control Framework

24.1 The backup process implemented within the GLA has been documented in the Backup Configuration Assured Quality Action Procedure (AQAP) dated June 2012, reducing the risk that backups are carried out in an inconsistent manner which could lead to insufficient data being unavailable.

24.2 City Hall has installed two physical Falconstor Appliances to manage data back-up requirements and the GLA data has been load balanced across the two appliances with the Microsoft Exchange server, Oracle Server and GLA websites on one appliance and all other services on the other appliance. The appliances have been configured to fail-over if one becomes unavailable. Each appliance has the capacity to host all services in case of fail-over.

24.3 Backups are taken using FalconStor snapshotting technology. The resources within the appliance are grouped together and backup policies are applied to each group. “Time views” (snapshots) are taken and replicated over to the Woking site. Time views are taken at least twice a day depending on the server and maintained for 90 days. We reviewed the snapshots available on the FalconStor Management Console. We were able to confirm that snapshots are being taken as documented and 90 days of snapshots were available at Woking. We did note two servers did not have 90 days of snapshots, but were informed by the Senior Systems Engineer that this is was due to the servers not being in place for 90 days.

24.4 Unix systems and some other legacy systems are also backed up to tape. The process involves a full back up on Friday and differential backups Monday – Thursday using Symantec Netbackup onto Ultrium 5 tape. Tapes are removed from the site daily and stored on a secured site. A third party (Data Protect) collects the tapes and removes them to the off site location. An email is sent as confirmation to GLA that the tapes have arrived at the offsite location in Greenwich safely.

24.5 The Live Systems team is responsible for verifying the status of the snapshots as part of their daily checks. The process of checking the FalconStor replication and the daily checks to be carried out has been documented in Assured Quality Action Procedures dated May 2012. The individual within the live systems team who has completed the checks emails the teams with the checks and results each morning. Email alerts are also received from FalconStor to alert the Live Systems Team of any issues. We reviewed the Outlook email of the Senior Systems Engineer to confirm that daily checks have been sent and received by the Senior Systems Engineer. We were able to confirm the Senior System Engineer had daily checks emails from 30/03/2012 to 14/06/2012.

24.6 Overall, the design and operation of the data back-up control framework was found to be satisfactory, reducing the risk that critical data will not be available to support the continuity of GLA operations.

25. IT Disaster Recovery Testing

25.1 The Technology Group Business Continuity Plan documents that partial tests of individual components and recovery arrangements will be carried out on a regular basis using the Test Laboratory. The plan also documents a full recovery exercise should be carried out every 6 months, reducing the risk the Business Continuity Plan may not be fit for purpose and unworkable in a contingency event.

25.2 The test scenario, individuals involved, times and dates, the test plan, event log and the findings of the test are required to be documented and used to update and refine the business continuity and major incident recovery plan (Corporate Plans). Moreover, the Christie Tender Response documents that as part of the professional services provided to GLA, a yearly health check and DR test will be included. The implementation process includes a test of the DR fail-over including the RecoverTrac scripts.

25.3 We confirmed that related IT DR testing had been undertaken. The related test plan documents the name of the server, a description, the services tested and the result of the test, including if the Technology Group tested the service or if the users tested the service. In addition, the Senior Systems Engineer (External Systems and Security) documented the process carried out during the first Disaster Recovery test and any problems encountered, further demonstrating the application of DR testing.

RISK AND AUDIT ASSURANCE STATEMENT - DEFINITIONS

RISK AND AUDIT ASSURANCE STATEMENT - DEFINITIONS

Assurance Level	Assurance	Criteria
1	**Full** There is particularly effective management of key risks and business objectives are being achieved.	There is a sound framework of control operating effectively to achieve business objectives.
2	**Substantial** Key risks are being managed effectively, however some controls need to be improved to ensure business objectives are met.	The framework of control is adequate and controls to mitigate key risks are generally operating effectively.
3	**Limited** Some improvement is required to address key risks before business objectives can be met.	A number of controls to mitigate key risks are not operating effectively.
4	**No** Significant improvement is required to address key risks before business objectives can be met.	The control framework is inadequate and controls in place are not operating effectively to mitigate key risks. The business area is open to abuse, significant error or loss and/or misappropriation.

Definitions of Risk Ratings

Priority	Categories 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.

ACTION PLAN

Ref.	Risk	Rating and Category	Recommendation	Agreed	Responsibility	Target Date
7.2	The documented Business Continuity Plans do not reflect the current situation leading to an uncoordinated response in a contingency event.	3	A formal process for carrying out periodic Business Impact Assessments should be defined and necessary adjustments made to the Business Continuity Plans.	Yes	Technology Operations Manager	July 2012

Terminology	Definition
DRS	Virtualisation Distributed Resource Scheduler allocates available resources among virtual machines according to business needs
VMotion	Software to move running virtual machines from one physical server to another with no impact to end users.
Snapshot	A point in time copy of a data resource (disk, database, file, etc.).
BCP	Business Continuity Plan
Bandwidth	Capacity of a link between two devices.
SAN	Storage Area Network A virtualised disk storage device.
Gold, Silver & Bronze team	Business Recovery Teams Gold – Senior Management Silver – Extended Management Team Bronze – Disaster Recovery Implementation teams.
Battle Box	Secure store of essential items located at Disaster Recover site.
Dark Fibre	Privately operated optical fibre network
ESX	Enterprise-level computer virtualization software
Flaconstor	Data virtualisation software
Blade Servers	Modular designed computer optimized to minimize the use of physical space and energy.
Block Level Replication	Disk configuration offering the ability to relocate and replicate servers without any service interruption to the source workload.
Differential Backup	Backup of files that have changed since the last Full backup. Also known as an “incremental backup”.
Full Backup	Backup of all files on a system.
Delta Mode Replication	Transfers changes made to the secondary data store at defined intervals. The remote copy of the data will never be as current as the main copy; however this method can replicate data with reduced bandwidth requirements and a lower impact on host performance.
High Availability	Provides a facility to monitor and restart virtual machines on alternative physical server resources when a server failure is detected